사용자 가이드

AWS Organizations

AWS Organizations: 사용자 가이드

Table of Contents

AWS Organizations란 무엇인가요?

AWS Organizations은 생성한 여러 AWS 계정을 조직에 통합하고 중앙에서 관리할 수 있는 계정 관리 서비스입니다. AWS Organizations의 계정 관리 및 통합 결제 기능을 활용하면 기업의 예산, 보안 및 규정 준수 요구 사항을 보다 잘 충족할 수 있습니다. 조직의 관리자로서 조직에서 계정을 생성하고 기존 계정을 조직에 초대할 수 있습니다.

이 사용 설명서는 AWS Organizations의 주요 개념을 정의하고 자습서를 제공하며, 조직을 생성 및 관리하는 방법을 설명합니다.

주제

AWS Organizations 기능

AWS Organizations는 다음 기능을 제공합니다.

모든 AWS 계정의 중앙 집중식 관리

기존 계정을 하나의 조직으로 결합해 중앙에서 계정을 관리할 수 있습니다. 자동으로 조직의 일부가 되는 계정을 만들고, 다른 계정을 조직에 초대할 수 있습니다. 또 계정 일부나 전체에 영향을 주는 정책을 연결할 수도 있습니다.

모든 멤버 계정에 대한 통합 결제

통합 결제는 AWS Organizations의 기능입니다. 조직의 관리 계정을 사용하여 모든 멤버 계정을 통합하고 요금을 지불할 수 있습니다. 통합 결제에서 관리 계정은 조직에 속한 멤버 계정의 결제 정보, 계정 정보 및 계정 활동에 액세스할 수도 있습니다. 이 정보는 관리 계정이 조직의 비용 성과를 향상시키는 데 도움이 되는 Cost Explorer와 같은 서비스에서 활용할 수 있습니다.

예산, 보안, 규정 준수 필요 충족을 위한 계정의 계층적 그룹화

계정을 조직 단위(OU)로 그룹화하고 OU마다 다른 액세스 정책을 연결할 수 있습니다. 예를 들어 특정 규제 요구 사항을 충족하는 AWS 서비스에만 액세스해야 하는 계정이 있는 경우 이러한 계정

을 하나의 OU에 넣을 수 있습니다. 그런 다음 해당 OU에 정책을 연결해 규제 요구 사항을 충족하지 않는 서비스에 대한 액세스를 차단합니다. OU는 5층으로 다른 OU에 중첩할 수 있어, 계정 그룹을 유연하게 구성할 수 있습니다.

각 계정이 액세스할 수 있는 AWS 서비스 및 API 작업의 제어를 중앙화하는 정책

조직 관리 계정의 관리자는 서비스 제어 정책(SCP)을 사용하여 조직의 멤버 계정에 대한 최대 권한을 지정할 수 있습니다. SCP에서 각 멤버 계정의 사용자 및 역할이 액세스할 수 있는 AWS 서비스, 리소스 및 개별 API 작업을 제한할 수 있습니다. 또한 AWS 서비스, 리소스 및 API 작업에 대한 액세스를 제한할 조건을 정의할 수도 있습니다. 이러한 제한은 조직의 멤버 계정 관리자보다도 우선합니다. AWS Organizations에서 멤버 계정의 서비스, 리소스 또는 API 작업에 대한 액세스를 차단하면 해당 계정의 사용자나 역할은 이러한 서비스, 리소스 또는 API 작업에 액세스할 수 없습니다. 이 차단은 멤버 계정의 관리자가 IAM 정책에서 이러한 권한을 명시적으로 부여하더라도 여전히 적용됩니다.

자세한 정보는 서비스 제어 정책(SCP) 섹션을 참조하세요.

조직 계정의 리소스 전반에서 태그를 표준화하는 정책

태그 정책을 사용하여 태그 키와 태그 값의 기본 대소문자 처리를 포함한 태그를 일관적으로 유지 관리할 수 있습니다.

자세한 내용은 태그 정책 섹션을 참조하세요.

AWS 인공 지능(AI) 및 기계 학습 서비스가 데이터를 수집하고 저장하는 방식을 제어하는 정책

AI 서비스 옵트아웃 정책을 사용하면 사용하지 않으려는 AWS AI 서비스에 대한 데이터 수집 및 저장을 옵트아웃할 수 있습니다.

자세한 내용은 AI 서비스 옵트아웃 정책 섹션을 참조하세요.

조직 계정의 리소스에 대해 자동 백업을 구성하는 정책

백업 정책을 사용하여 자동으로 AWS Backup 계획을 구성하고 모든 조직 계정의 리소스에 적용할 수 있습니다.

자세한 내용은 백업 정책 섹션을 참조하세요.

AWS Identity and Access Management(IAM)에 대한 통합 및 지원

IAM은 개별 계정에서 사용자와 역할에 대한 세분화된 제어를 제공합니다. AWS Organizations는 사용자가 계정이나 계정 그룹에서 사용자와 역할이 할 수 있는 일을 제어하게 함으로써 이러한 제어력을 계정 수준으로까지 확장합니다. 결국 계정 수준에서 AWS Organizations가 허용하는 권한과

해당 계정 내 사용자 또는 역할 수준에서 IAM이 명시적으로 부여하는 권한이 논리적으로 교차된 권한이 생성됩니다. 다시 말해 사용자는 AWS Organizations 정책과 IAM 정책 모두가 허용하는 것에만 액세스할 수 있습니다. 둘 중 하나가 작업을 차단한다면, 사용자는 해당 작업에 액세스할 수 없습니다.

다른 AWS 서비스와의 통합

AWS Organizations에서 사용 가능한 다중 계정 관리 서비스를 일부 AWS 서비스와 함께 사용하면 조직의 멤버인 모든 계정에서 작업을 수행할 수 있습니다. 서비스 목록 및 조직 전체 수준에서 각 서비스를 사용하는 이점은 AWS 함께 사용할 수 있는 서비스 AWS Organizations 단원을 참조하세요.

AWS 서비스가 조직의 멤버 계정 내에서 사용자를 대신하여 작업을 수행하도록 활성화하면 AWS Organizations는 각 멤버 계정에 해당 서비스용 IAM 서비스 연결 역할을 생성합니다. 서비스 연결 역할에는 다른 AWS 서비스가 조직과 해당 계정에서 특정 작업을 수행하도록 허용하는 사전 정의된 IAM 권한이 있습니다. 이렇게 하기 위해 조직의 모든 계정은 자동으로 서비스 연결 역할을 갖습니다. 이 역할을 통해 AWS Organizations 서비스는 AWS 서비스에서 신뢰할 수 있는 액세스를 활성화하는 데 필요한 서비스 연결 역할을 생성할 수 있습니다. 이러한 추가적인 서비스 연결 역할은 특정 서비스를 활성화하여 구성 선택에 필요한 작업만을 수행하도록 하는 IAM 권한 정책에 연결됩니다. 자세한 정보는 다른 AWS 서비스와 함께 AWS Organizations 사용 섹션을 참조하세요.

전역 액세스

AWS Organizations는 모든 AWS 리전에서 작동하는 하나의 엔드포인트를 가진 글로벌 서비스입니다. 작동할 리전을 명시적으로 선택할 필요가 없습니다.

최종 일관 데이터 복제

AWS Organizations는 다른 많은 AWS 서비스와 마찬가지로 최종 일관성이 있습니다. AWS Organizations에서는 리전 내에 있는 AWS 데이터 센터의 여러 서버 간에 데이터를 복제하여 고가용성을 구현합니다. 일부 데이터를 변경하겠다는 요청이 성공하면 변경이 실행되고 그 결과는 안전하게 저장됩니다. 그러나 변경 사항은 여러 서버에 걸쳐 복제되어야 합니다. 자세한 정보는 변경 사항이 매번 즉시 표시되는 것은 아닙니다. 섹션을 참조하세요.

무료 사용

AWS Organizations는 추가 비용 없이 AWS 계정에 제공되는 기능입니다. 조직의 계정에서 다른 AWS 서비스에 액세스할 때만 요금이 부과됩니다. 다른 AWS 제품 요금에 대한 자세한 내용은 Amazon Web Services 요금 페이지를 참조하세요.

AWS Organizations 요금

AWS Organizations는 추가 비용 없이 제공됩니다. 멤버 계정의 사용자와 역할이 사용한 AWS 리소스에 대한 요금만 청구됩니다. 예를 들어 멤버 계정의 사용자나 역할이 사용한 Amazon EC2 인스턴스에 대한 표준 요금이 청구됩니다. 다른 AWS 서비스 요금에 대한 자세한 내용은 AWS 요금을 참조하세요.

AWS Organizations에 액세스

다음 방법 중 하나를 사용하여 AWS Organizations에서 작업할 수 있습니다.

AWS Management Console

AWS Organizations 콘솔은 조직과 AWS 리소스를 관리하는 데 사용할 수 있는 브라우저 기반 인터페이스입니다. 콘솔을 사용하여 조직에서 모든 작업을 수행할 수 있습니다.

AWS 명령줄 도구

AWS 명령줄 도구를 사용하면 시스템 명령줄에서 명령을 실행하여 AWS Organizations 및 AWS 작업을 수행할 수 있습니다. 명령줄로 작업하는 것이 콘솔을 사용하는 것보다 더 빠르고 편리할 수 있습니다. AWS 작업을 수행하는 스크립트를 작성할 때도 명령줄 도구가 유용합니다.

AWS에서는 다음과 같은 두 가지 명령줄 도구 세트를 제공합니다.

- AWS Command Line Interface(AWS CLI). AWS CLI 설치 및 사용에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 참조하세요.
- AWS Tools for Windows PowerShell. Tools for Windows PowerShell 설치 및 사용에 대한 자세한 내용은 AWS Tools for Windows PowerShell 사용 설명서를 참조하세요.

AWS SDK

AWS SDK는 다양한 프로그래밍 언어 및 플랫폼(Java, Python, Ruby, .NET, iOS, Android 등)을 위한 라이브러리와 샘플 코드로 구성되어 있습니다. SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. AWS SDK 다운로드 및 설치 방법을 비롯한 자세한 내용은 Amazon Web Services용 도구를 참조하세요.

AWS Organizations HTTPS 쿼리 API

AWS Organizations HTTPS 쿼리 API를 사용하여 AWS Organizations 및 AWS에 프로그래밍 방식으로 액세스할 수 있습니다. HTTPS 쿼리 API를 이용하면 HTTPS 요청을 서비스에 바로 보낼 수 있습니다. HTTPS API를 사용할 때는 자격 증명을 사용하여 요청에 디지털 방식으로 서명하는 코드를 포함해야 합니다. 자세한 정보는 HTTP 쿼리 요청을 통한 API 호출 및 AWS Organizations API 참조를 참조하세요.

AWS Organizations에 대한 지원 및 의견

우리는 여러분의 의견을 환영합니다. feedback-awsorganizations@amazon.com으로 의견을 보낼 수 있습니다. 또한 AWS Organizations 지원 포럼에 의견과 질문을 올리셔도 됩니다. AWS 지원 포럼에 대한 자세한 정보는 포럼 도움말을 참조하세요.

기타 AWS 리소스

- AWS 교육 및 과정 - 역할 기반 및 특수 과정 외에도 자습형 실습과 연결하여 AWS 기술을 연마하고 실용적인 경험을 얻는 데 도움을 드립니다.
- AWS 개발자 도구 - AWS로 혁신적인 애플리케이션을 구축하는 데 도움이 될 수 있는 설명서, 코드 예제, 출시 정보 및 기타 정보를 제공하는 개발자 도구 및 리소스 링크입니다.
- AWS Support Center - AWS 지원 사례를 생성하고 관리하는 허브입니다. 또한 포럼, 기술 FAQ, 서비스 상태 및 AWS Trusted Advisor 등의 기타 유용한 자료에 대한 링크가 있습니다.
- AWS Support - 클라우드에서 1대 1로 애플리케이션을 구축 및 실행하도록 지원하는 빠른 응답 지원 채널인 AWS Support에 대한 정보가 포함된 기본 웹 페이지입니다.
- 문의처 - AWS 결제, 계정, 이벤트, 침해 및 기타 문제에 대해 문의할 수 있는 중앙 연락 창구입니다.
- AWS 사이트 약관 – 저작권 및 상표, 사용자 계정, 라이선스 및 사이트 액세스와 기타 주제에 대한 세부 정보입니다.

AWS Organizations 시작하기

다음 주제는 AWS Organizations를 배우고 사용하기 시작하는 데 도움이 되는 정보를 제공합니다.

추가 정보 ...

AWS Organizations 용어 및 개념

AWS Organizations를 이해하는 데 필요한 용어와 핵심 개념을 알아봅니다. 이 단원에서는 조직의 각 구성 요소와 계정의 사용자가 수행 가능한 작업을 제어하는 새로운 레벨을 제공하기 위해 이러한 구성 요소가 함께 작동하는 방식에 대한 기본 사항을 설명합니다.

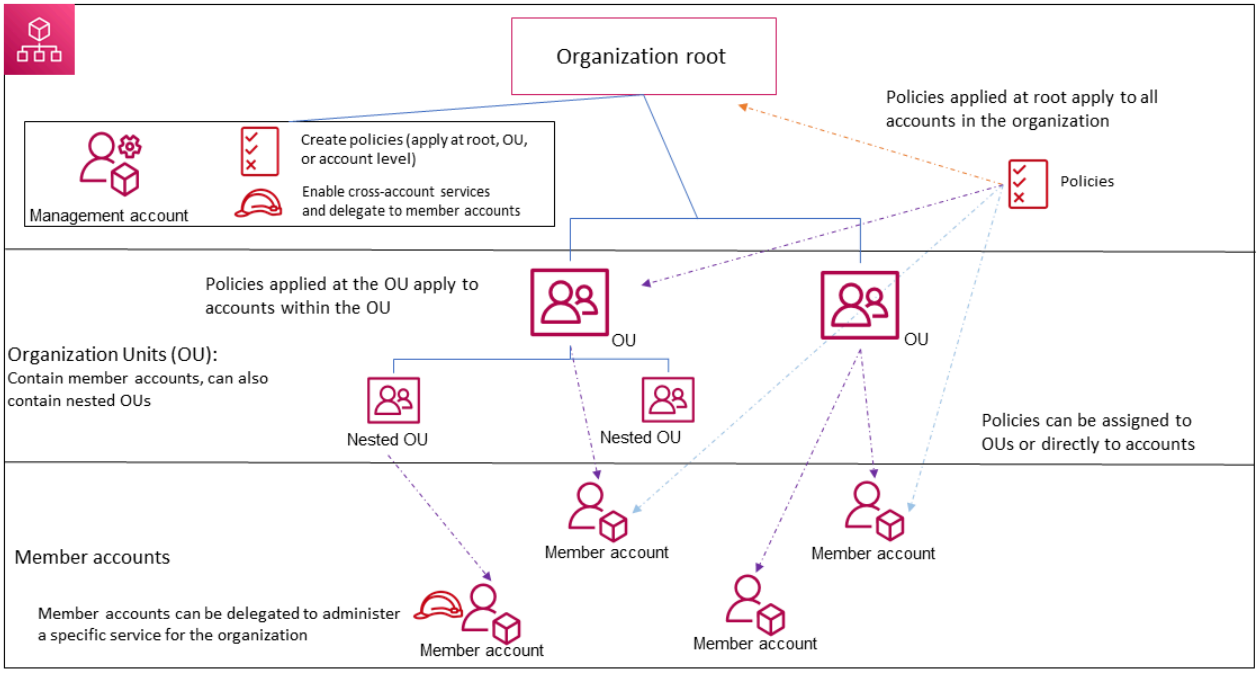
조직의 통합 결제

AWS Organizations에 대한 주요 기능 중 하나는 조직의 모든 계정에 대한 결제를 통합하는 기능입니다. 조직에서 결제를 처리하는 방법 및 여러 계정 간에 공유할 때 다양한 할인이 작동하는 방식에 대해 자세히 알아보세요. 해당 내용은 AWS Billing 사용 설명서에 있습니다.

AWS Organizations 용어 및 개념

AWS Organizations를 시작하는 데 도움이 되도록 이번 주제에서는 몇 가지 주요 개념을 설명합니다.

다음 도표는 루트에서 4가지 조직 단위(OU)로 구분되는 계정 5개로 구성된 기본 조직을 보여줍니다. 또 조직에는 일부 OU에 연결되거나 계정에 직접 적용되는 다양한 정책이 있습니다. 각 항목에 대한 설명은 이번 주제에 나오는 정의를 참조하세요.



조직

AWS 계정을 단일 단위로 관리할 수 있도록 통합하기 위해 생성하는 개체입니다. AWS Organizations 콘솔을 사용하여 조직 내 모든 계정을 중앙에서 확인하고 관리할 수 있습니다. 조직은 관리 계정 하나와 0개 이상의 멤버 계정을 갖습니다. 위에는 루트가, 아래에는 조직 단위가 있는 나무형 계층 구조로 계정을 조직할 수 있습니다. 각 계정은 루트에 바로 배치하거나, 계층 구조 내의 OU 중 하나에 배치할 수 있습니다. 조직은 사용자가 설정하는 기능 모음으로 결정되는 다양한 기능을 보유합니다.

루트

조직의 모든 계정에 대한 상위 컨테이너입니다. 정책을 루트에 적용하면, 해당 정책은 조직의 모든 조직 단위(OU)와 계정에 적용됩니다.

> **Note**
>
> 지금은 루트 하나만 있습니다. AWS Organizations는 사용자가 조직을 만들 때 이 루트를 자동으로 생성합니다.

조직 단위(OU)

루트에 있는 계정을 위한 컨테이너입니다. 또한 OU는 다른 OU를 포함할 수 있기 때문에 사용자는 위쪽에는 루트가, 아래쪽에는 OU 가지가, 맨 끝에는 나뭇잎에 해당하는 계정이 있는 거꾸로 된 나무 형태의 계층 구조를 만들 수 있습니다. 정책을 계층 구조 내의 노드 하나에 연결하면, 정책은 아래쪽으로 내려와 모든 가지(OU)와 잎(계정)에 영향을 줍니다. 각 OU는 상위 OU를 하나만 가질 수 있으며, 현재 각 계정은 한 OU의 멤버만 될 수 있습니다.

계정

Organizations의 계정은 AWS 리소스를 포함하는 표준 AWS 계정으로, 이러한 리소스에 액세스할 수 있는 자격 증명입니다.

> **Tip**
>
> AWS 계정은 사용자 계정과 동일한 계정이 아닙니다. AWS 사용자는 AWS Identity and Access Management(IAM)를 사용하여 생성하는 자격 증명으로서, 장기 자격 증명을 갖는 IAM 사용자 또는 단기 자격 증명을 갖는 IAM 역할의 형태를 취합니다. 하나의 AWS 계정은 많은 사용자와 역할을 포함할 수 있으며, 일반적으로 그러합니다.

조직에는 두 가지 유형의 계정이 있습니다. 하나는 관리 계정으로 지정된 단일 계정이며 다른 하나는 하나 이상의 멤버 계정입니다.

- 관리 계정은 조직을 만들 때 사용하는 계정입니다. 조직의 관리 계정에서 수행할 수 있는 사항은 다음과 같습니다.
  - 조직에서 계정 생성
  - 기존의 다른 계정을 조직에 초대
  - 조직에서 계정 제거
  - 위임된 관리자 계정 지정
  - 초대 관리
  - 조직 내 개체(루트, OU 또는 계정)에 정책 적용
  - 지원되는 AWS 서비스와의 통합을 지원하여 조직의 모든 계정에 서비스 기능 제공

  관리 계정은 지급인 계정을 담당하며 멤버 계정에서 발생한 모든 요금을 지불해야 합니다. 조직의 관리 계정은 변경할 수 없습니다.
- 멤버 계정은 조직의 나머지 모든 계정을 구성합니다. 하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다. 정책을 계정에 연결해 정책 제어를 해당 계정에만 적용할 수 있습니다.

> **Note**
>
> 일부 멤버 계정을 위임된 관리자 계정으로 지정할 수 있습니다. 아래에서 위임된 관리자를 참조하십시오.

위임된 관리자

Organizations 관리 계정과 그 사용자 및 역할은 해당 계정으로 수행해야 하는 작업에 대해서만 사용하는 것이 좋습니다. AWS 리소스를 조직의 다른 멤버 계정에 저장하고 관리 계정에는 저장하지 않는 것이 좋습니다. 이는 Organizations 서비스 제어 정책(SCP)과 같은 보안 기능이 관리 계정의 사용자나 역할을 제한하지 않기 때문입니다. 관리 계정에서 리소스를 분리하면 인보이스의 요금을 파악하는 데도 도움이 될 수 있습니다. 조직의 관리 계정에서 하나 이상의 멤버 계정을 위임된 관리자 계정으로 지정하면 이 권장 사항을 구현하는 데 도움이 됩니다. 위임된 관리자에는 다음 두 가지 유형이 있습니다.

- Organizations의 위임된 관리자: 이 계정에서는 조직 정책을 관리하고 조직 내 엔터티(루트, OU 또는 계정)에 정책을 연결할 수 있습니다. 관리 계정은 세분화된 수준에서 위임 권한을 제어할 수 있습니다. 자세한 정보는 에 대한 위임 관리자 AWS Organizations 섹션을 참조하세요.
- AWS 서비스의 위임된 관리자: 이 계정에서는 Organizations과 통합되는 AWS 서비스를 관리할 수 있습니다. 관리 계정은 필요에 따라 여러 멤버 계정을 여러 서비스에 위임된 관리자로 등록할 수 있습니다. 이러한 계정에는 특정 서비스에 대한 관리 권한과 함께 Organizations 읽기 전용 작업에 대한 권한이 있습니다. 자세한 정보는 Organizations과 연동되는 AWS 서비스의 위임된 관리자 섹션을 참조하세요.

초대

다른 계정에 조직 가입을 요청하는 과정입니다. 초대는 조직의 관리 계정에서만 발행할 수 있습니다. 초대는 계정 ID 또는 초대된 계정과 연결된 이메일 주소로 확장됩니다. 초대받은 계정이 초대를 수락하면, 해당 계정은 조직의 멤버 계정이 됩니다. 조직이 모든 멤버가 통합 결제 기능 지원에서 모든 기능 지원으로 전환하는 일을 승인해야 한다면, 현재 존재하는 모든 멤버 계정에 초대를 전송해야 합니다. 초대를 이용하려면 계정이 핸드셰이크를 교환해야 합니다. AWS Organizations 콘솔에서 작업할 때는 핸드셰이크가 표시되지 않을 수 있습니다. 그러나 AWS CLI 또는 AWS Organizations API를 사용하는 경우 핸드셰이크로 직접 작업해야 합니다.

핸드셰이크

두 당사자 간에 정보를 교환하는 다양한 단계로 구성된 과정입니다. AWS Organizations에서 이 핸드셰이크가 주로 사용되는 경우 중 하나는 초대를 위한 기본 작업을 구현할 때입니다. 핸드셰이크 메시지는 핸드셰이크 개시자와 받는 사람 간에 전달되고 응답됩니다. 메시지는 양 당사자가 현재

상태를 알 수 있도록 전달됩니다. 또한 핸드셰이크는 조직이 통합 결제 기능만 지원하는 데서 가 제공하는 모든 기능AWS Organizations을 지원하도록 변경할 때도 사용합니다. 일반적으로는 AWS Organizations API나 AWS CLI 같은 명령줄 도구를 사용할 때에만 핸드셰이크와 직접 상호 작용해야 합니다.

사용 가능한 기능 모음

- 모든 기능 – AWS Organizations가 사용할 수 있는 기본 기능 세트입니다. 통합 결제의 모든 기능과 조직 내 계정에 대한 더 많은 제어를 제공하는 고급 기능을 함께 제공합니다. 예를 들어 모든 기능을 활성화하면 조직의 관리 계정은 멤버 계정이 하는 일을 완전히 제어할 수 있습니다. 관리 계정은 SCP를 적용하여 계정의 사용자(루트 사용자 포함)와 역할이 액세스할 수 있는 서비스와 작업을 제한할 수 있습니다. 관리 계정은 멤버 계정이 조직에서 나가지 못하도록 할 수도 있습니다. 또한 지원되는 AWS 서비스와의 통합을 지원하여 이러한 서비스들이 조직의 모든 계정에 기능을 제공할 수 있도록 합니다.

  모든 기능을 활성화한 상태로 조직을 만들거나, 원래 통합 결제 기능만 제공하는 조직에서 모든 기능을 활성화할 수 있습니다. 모든 기능을 활성화하려면 초대받은 멤버 계정 모두가 관리 계정이 과정을 시작하면서 전송한 초대를 수락해 변경 사항을 승인해야 합니다.

- 통합 결제 – 이 기능 집합은 공유 결제 기능을 제공하지만 AWS Organizations의 추가적인 고급 기능을 포함하지는 않습니다. 예를 들어 조직에 통합할 다른 AWS 서비스를 모든 계정에서 작동하도록 하거나, 정책을 사용하여 다른 계정의 사용자 및 역할이 수행할 수 있는 작업을 제한할 수 없습니다. 고급 AWS Organizations 기능을 사용하려면 조직에서 모든 기능을 활성화해야 합니다.

서비스 제어 정책(SCP)

SCP의 영향을 받는 계정에서 사용자와 역할이 사용할 수 있는 서비스와 작업을 지정하는 정책입니다. SCP는 권한을 부여하지 않는다는 점을 제외하고 IAM 권한 정책과 비슷합니다. 대신, SCP는 조직, 조직 단위(OU) 또는 계정에 대한 최대 권한을 지정합니다. SCP를 조직 루트 또는 OU에 연결하면 SCP가 멤버 계정의 개체에 대한 권한을 제한합니다.

허용 목록 및 거부 목록 비교

허용 목록과 거부 목록은 SCP를 적용하여 계정에 사용 가능한 권한을 필터링할 수 있는 보완적인 전략입니다.

- 허용 목록 전략 – 허용되는 액세스를 명시적으로 지정합니다. 다른 모든 액세스는 묵시적으로 차단됩니다. 기본적으로 AWS Organizations는 `FullAWSAccess`라는 AWS 관리형 정책을 모든 루트, OU 및 계정에 연결합니다. 따라서 조직을 구축할 때 사용자가 원하기 전까지는 무엇도 차단

되지 않도록 합니다. 다시 말해서, 기본적으로 모든 권한이 허용됩니다. 권한을 제한할 준비가 끝났다면, `FullAWSAccess` 정책을 더욱 제한적이고 원하는 권한 모음만 허용하는 정책과 교체하면 됩니다. 이렇게 하면 영향받는 계정의 사용자와 역할은 IAM 정책이 모든 작업을 허용하더라도 지정된 수준의 액세스만 이용할 수 있습니다. 루트의 기본 정책을 교체하면, 조직의 모든 계정이 제한의 적용을 받게 됩니다. SCP는 권한을 부여하지 않으며 필터링만하기 때문에 계층 구조의 낮은 수준에 다시 권한을 추가할 수는 없습니다.

- 거부 목록 전략 – 허용되지 않는 액세스를 명시적으로 지정합니다. 다른 액세스는 모두 허용됩니다. 이 시나리오에서는 명시적으로 차단하지 않는 이상 모든 권한이 허용됩니다. 이는 AWS Organizations의 기본 동작입니다. 기본적으로 AWS Organizations는 `FullAWSAccess`라는 AWS 관리형 정책을 모든 루트, OU 및 계정에 연결합니다. 따라서 모든 계정은 AWS Organizations가 적용한 제한을 받지 않고 모든 서비스와 작업에 액세스할 수 있습니다. 위에서 설명한 허용 목록 기술과 달리, 거부 목록을 사용할 때는 "모두" 허용하는 기본 `FullAWSAccess` 정책을 그대로 둡니다. 그런 다음 원치 않는 서비스와 작업에 대한 액세스를 명시적으로 거부하는 추가 정책을 연결합니다. IAM 권한 정책과 마찬가지로, 서비스 작업의 명시적 거부는 해당 작업에 대한 모든 허용을 무시하게 됩니다.

인공 지능(AI) 서비스 옵트아웃 정책

조직의 모든 계정에서 AWS AI 서비스에 대한 옵트아웃 설정을 표준화하는 데 도움을 주는 정책 유형입니다. 특정 AWS AI 서비스는 Amazon AI 서비스 및 기술의 개발과 지속적인 개선을 위해 해당 서비스에서 처리한 고객 콘텐츠를 저장하고 사용할 수 있습니다. AWS 고객은 AI 서비스 옵트아웃 정책을 사용하여 서비스 개선을 위해 자신의 콘텐츠가 저장, 사용되지 않도록 옵트아웃할 수 있습니다.

백업 정책

조직의 모든 계정에서 리소스에 대한 백업 전략을 표준화하고 구현하는 데 도움을 주는 정책 유형입니다. 백업 정책에서 리소스에 대한 백업 계획을 구성하고 배포할 수 있습니다.

태그 정책

조직의 모든 계정에서 리소스 전반의 태그를 표준화하는 데 도움을 주는 정책 유형입니다. 태그 정책에서 특정 리소스에 대한 태그 지정 규칙을 지정할 수 있습니다.

AWS Organizations 자습서

이 단원의 자습서를 통해 AWS Organizations를 사용하여 작업을 수행하는 방법을 알아봅니다.

자습서: 조직 생성 및 구성

단계별 지침에 따라 설정하고 실행해 나만의 조직을 만들고, 첫 번째 멤버 계정을 초대하고, 사용자의 계정을 포함하는 OU 계층을 만들고, 일부 서비스 제어 정책(SCP)을 적용해보십시오.

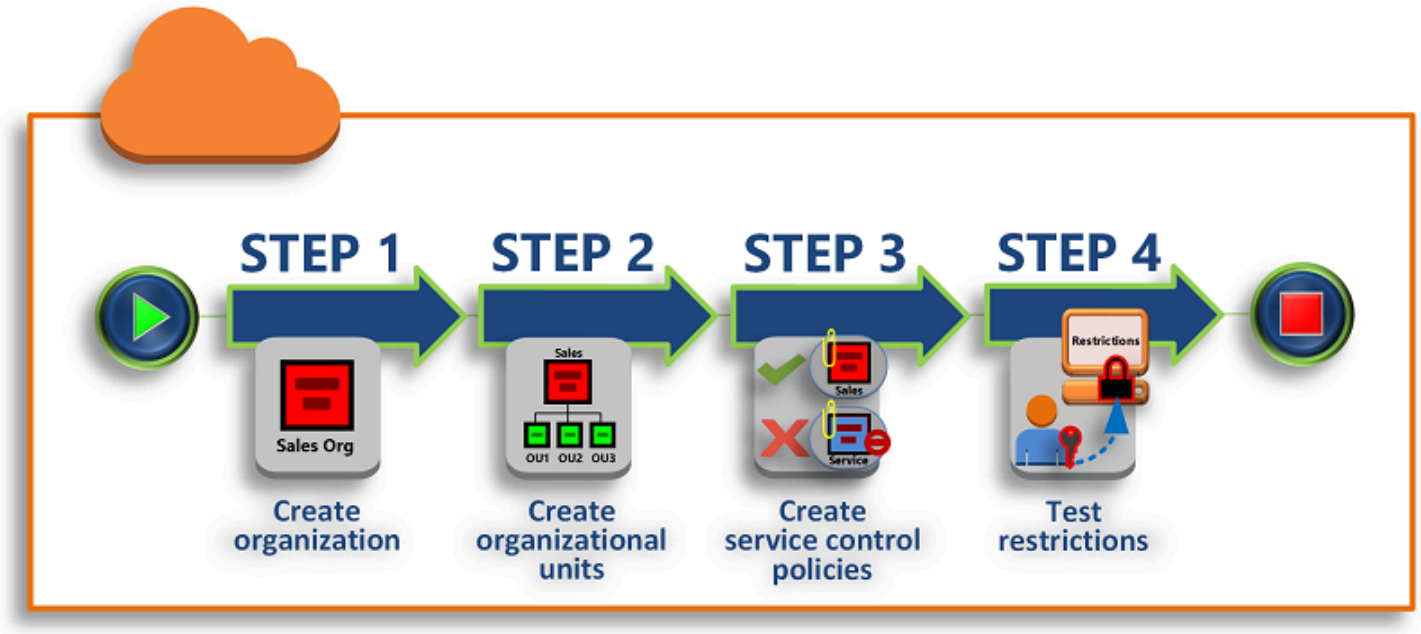
자습서: Amazon EventBridge를 사용하여 조직에 대한 중요 변경 사항 모니터링

지정한 작업이 조직에서 발생하면 이메일, SMS 문자 메시지 또는 로그 항목의 형식으로 경보를 트리거하도록 Amazon EventBridge를 구성하여 조직의 주요 변경 사항을 모니터링합니다. 예를 들어, 많은 조직에서 새 계정이 생성되는 경우, 계정이 조직에서 탈퇴하려고 하는 경우 등을 알고 싶어 합니다.

자습서: 조직 생성 및 구성

이 자습서에서는 AWS 멤버 계정 2개로 조직을 생성하고 구성합니다. 조직 내 멤버 계정 하나를 만들고, 다른 계정을 조직에 초대합니다. 그런 다음에는 허용 목록 기법을 사용하여 명시적으로 나열된 서비스와 작업만 계정 관리자가 위임할 수 있도록 지정합니다. 이를 통해 관리자는 AWS가 도입한 새로운 서비스를 승인한 후 회사 관계자가 사용하도록 허가할 수 있습니다. 따라서 AWS에서 새로운 서비스가 도입되는 경우 관리자가 적절한 정책의 허용 목록에 서비스를 추가할 때까지 해당 서비스는 금지된 상태로 유지됩니다. 또한 이 자습서는 거부 목록을 사용하여 멤버 계정에 있는 모든 사용자가 AWS CloudTrail이 생성하는 감사 로그에 대한 구성을 변경할 수 없도록 하는 방법도 보여줍니다.

다음 그림은 자습서의 기본 단계를 보여줍니다.



[1단계: 조직 만들기]

이 단계에서는 현재 AWS 계정을 관리 계정으로 사용하는 조직을 생성합니다. 또한 한 AWS 계정을 조직에 초대하고, 두 번째 계정을 멤버 계정으로 생성합니다.

[2단계: 조직 단위 만들기]

그런 다음에는 새로운 조직 내에 조직 단위(OU) 2개를 만들고 OU에 멤버 계정을 배치합니다.

[3단계: 서비스 제어 정책 생성]

[서비스 제어 정책(SCP)]을 사용하여 멤버 계정 사용자와 역할에 위임할 수 있는 작업을 제한할 수도 있습니다. 이 단계에서는 SCP 2개를 생성하고 조직의 OU에 연결해봅니다.

[4단계: 조직 정책 테스트]

각 테스트 계정에서 사용자로 로그인해 SCP가 해당 계정에 어떤 효과를 주는지 살펴보세요.

이 자습서에 있는 단계를 실행해도 AWS 청구서에 비용이 발생하지 않습니다. AWS Organizations는 무료 서비스입니다.

필요 조건

이 자습서는 여러분이 기존 AWS 계정 2개에 액세스할 수 있으며(3번째 계정은 자습서를 진행하면서 만들게 됩니다), 각 계정에 관리자로 로그인할 수 있다고 가정합니다.

이 자습서에서 계정은 다음과 같은 의미가 있습니다.

- 111111111111 - 조직을 만들 때 사용하는 계정입니다. 이 계정은 관리 계정이 됩니다. 이 계정의 소유자는 OrgAccount111@example.com이라는 이메일 주소를 가집니다.
- 222222222222 - 멤버 계정으로 조직에 초대한 계정입니다. 이 계정의 소유자는 member222@example.com이라는 이메일 주소를 가집니다.
- 333333333333 - 조직의 멤버로 생성한 계정입니다. 이 계정의 소유자는 member333@example.com이라는 이메일 주소를 가집니다.

위의 값을 테스트 계정과 관련된 값으로 대체하세요. 이 자습서에서는 되도록 프로덕션 계정은 사용하지 마세요.

1단계: 조직 만들기

이번 단계에서는 111111111111 계정에 관리자로 로그인해 해당 계정을 관리 계정으로 이용해 조직을 생성하고, 기존 계정 222222222222를 멤버 계정으로 조직에 초대합니다.

AWS Management Console

1. 111111111111 계정의 관리자로 AWS에 로그인한 후 AWS Organizations 콘솔을 엽니다.
2. 소개 페이지에서 조직 생성(Create organization)을 선택합니다.
3. 확인 대화 상자에서 조직 생성Create organization)을 선택합니다.

   > **Note**
   >
   > 기본적으로 조직은 모든 기능이 활성화된 상태로 생성됩니다. 통합 결제 기능만 활성화하여 조직을 생성할 수도 있습니다.

   AWS가 조직을 생성하고 AWS 계정 페이지를 표시합니다. 다른 페이지에 있는 경우 왼쪽의 탐색 창에서 AWS 계정을 선택합니다.

   AWS에서 이메일 주소를 확인한 적이 없는 계정을 사용하는 경우 확인 이메일이 관리 계정과 연결된 주소로 자동 전송됩니다. 확인 이메일을 받기까지 어느 정도 시간이 걸릴 수 있습니다.
4. 24시간 내에 이메일 주소를 확인하세요. 자세한 정보는 이메일 주소 확인 섹션을 참조하세요.

이제 여러분의 계정이 유일한 멤버 계정인 조직을 만들었습니다. 이것은 조직의 관리 계정입니다.

기존 계정을 조직에 가입하도록 초대

이제 조직을 확보했으니, 조직 내 계정 만들기를 시작할 수 있습니다. 이번 섹션의 단계에서는 기존 계정을 초대해 조직의 멤버가 되게 합니다.

AWS Management Console

기존 계정을 가입 초대하려면

1. AWS 계정 페이지로 이동하고 AWS 계정 추가(Add an AWS 계정)를 선택합니다.
2. AWS 계정 추가 페이지에서 기존 AWS 계정 초대를 선택합니다.
3. 초대할 AWS 계정 의 이메일 주소 또는 계정 ID(Email address or account ID of an AWS 계정 to invite) 상자에서, 초대할 계정 소유자의 이메일 주소(예: **member222@example.com**)를 입력합니다. 또는 AWS 계정 ID 번호를 알고 있다면 해당 번호를 대신 입력합니다.
4. 초대 이메일 메시지에 포함할 메시지(Message to include in the invitation email message) 상자에서, 원하는 텍스트를 입력합니다. 이 텍스트는 이메일에 포함되어 계정 소유자에게 전송됩니다.
5. 초대 보내기(Send invitation)를 선택합니다. AWS Organizations가 계정 소유자에게 초대를 전송합니다.

   > **Important**
   >
   > 메시지가 길 경우 오류 메시지를 펼칩니다. 조직에 대한 계정 한도를 초과했거나 조직이 아직 초기화되고 있기 때문에 계정을 추가할 수 없음을 나타내는 오류인 경우 조직을 생성한 후 한 시간 동안 기다렸다가 다시 시도합니다. 오류가 지속될 경우 AWS 지원에 문의하세요.

6. 자습서 목적 상 지금은 여러분 자신이 보낸 초대를 수락해야 합니다. 다음 중 하나를 수행하여 콘솔의 [Invitations] 페이지로 이동합니다.

   - 관리 계정에서 AWS가 전송한 이메일을 열고 해당 링크를 선택하여 초대를 수락합니다. 로그인 메시지가 나타나면, 초대받은 멤버 계정의 관리자로 로그인합니다.
   - AWS Organizations 콘솔을 열고 초대(Invitations) 페이지로 이동합니다.

7. AWS 계정 페이지에서 수락(Accept)과 확인(Confirm)을 차례로 선택합니다.

> **Tip**
>
> 초대 메시지의 수신이 지연될 수 있으며, 이 경우 초대를 수락하려면 기다려야 할 수 있습니다.

8. 멤버 계정에서 로그아웃한 다음 관리 계정 관리자로 다시 로그인합니다.

멤버 계정 생성

이번 단원의 단계에서는 자동으로 조직의 멤버가 되는 AWS 계정을 생성합니다. 자습서에서 이 계정을 333333333333이라고 하겠습니다.

AWS Management Console

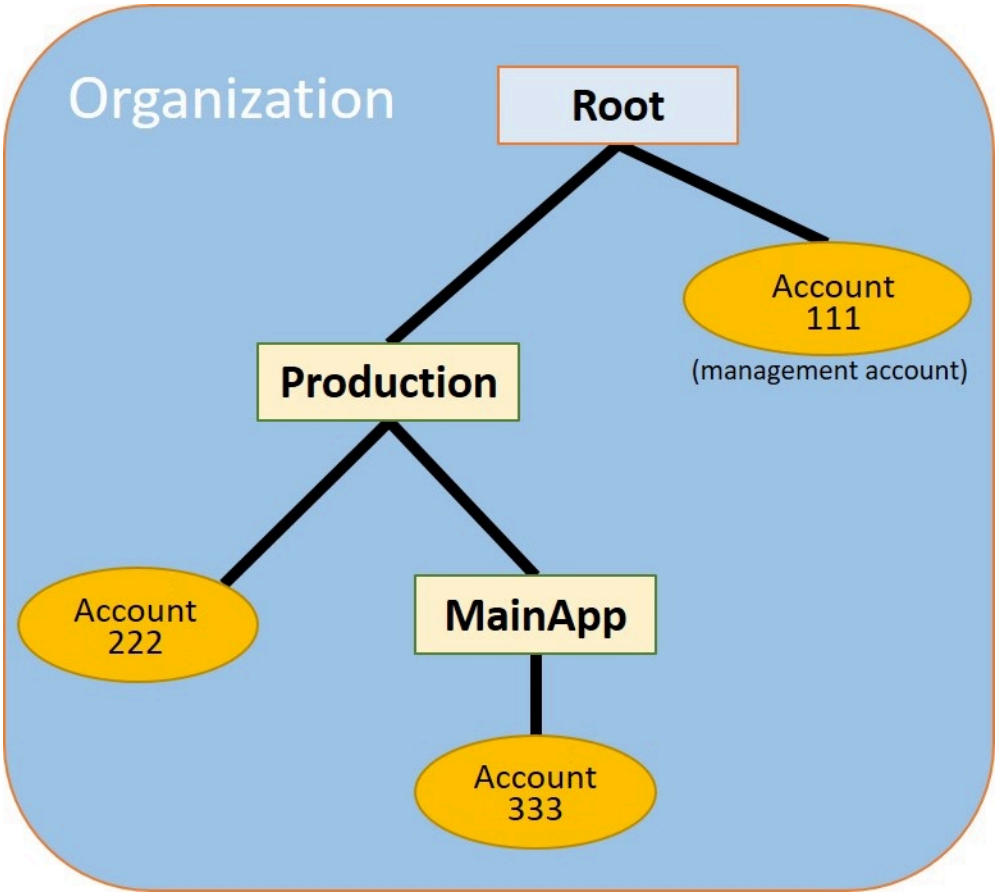
멤버 계정을 만들려면

1. AWS Organizations 콘솔의 AWS 계정 페이지에서 AWS 계정 추가(Add AWS 계정)를 선택합니다.
2. AWS 계정 추가(Add an AWS 계정) 페이지에서 AWS 계정 생성(Create an AWS 계정)을 선택합니다.
3. AWS 계정 이름에 계정 이름을 입력합니다(예: **`MainApp Account`**).
4. 계정 루트 사용자의 이메일 주소(Email address of the account's root user)에서, 계정을 대표하여 소식을 받을 사람의 이메일 주소를 입력합니다. 이 값은 하나만 존재해야 합니다. 두 계정이 같은 이메일 주소를 가지면 안 됩니다. 예를 들면 **`mainapp@example.com`** 등을 사용할 수 있습니다.
5. [IAM role name]을 공란으로 두어 기존 역할 이름인 `OrganizationAccountAccessRole`을 자동으로 사용하게 하거나, 이름을 직접 입력합니다. 이 역할은 사용자가 관리 계정의 IAM 사용자로 로그인하면 새로운 멤버 계정에 액세스할 수 있게 합니다. 본 자습서에서는 이 역할 이름을 공란으로 두어 AWS Organizations가 기본 이름으로 역할을 생성하도록 할 것입니다.
6. 생성(Create)AWS 계정을 선택합니다. AWS 계정 페이지에 새 계정이 표시되려면 페이지를 새로 고치고 잠시 기다려야 합니다.

> **Important**
>
> 조직에 대한 계정 한도를 초과했거나 조직이 아직 초기화되고 있기 때문에 계정을 추가할 수 없음을 나타내는 오류가 발생하면 조직을 생성한 후 한 시간 동안 기다렸다가 다시 시도하세요. 오류가 지속될 경우 AWS 지원에 문의하세요.

2단계: 조직 단위 만들기

이 섹션의 단계에서는 조직 단위(OU)를 만들고 조직 단위 내에 멤버 계정을 배치합니다. 작업이 완료되면 계층 구조가 다음 그림처럼 보일 것입니다. 관리 계정은 계속 루트에 남습니다. 멤버 계정 하나는 생산 OU로 이동하고 다른 멤버 계정은 생산 OU의 하위 OU인 MainApp OU로 이동합니다.



AWS Management Console

OU를 만들거나 채우려면

> **Note**
>
> 다음 단계에서는 객체 자체의 이름이나 객체 옆의 라디오 버튼을 선택할 수 있는 객체와 상호 작용합니다.
>
> - 객체 이름을 선택하면 객체 세부 정보를 표시하는 새 페이지가 열립니다.
> - 객체 옆에 있는 라디오 버튼을 선택하면 메뉴 옵션 선택 등의 다른 작업 시 해당 객체가 작업을 수행하게 됩니다.
>
> 다음 단계에서는 메뉴 선택 시 연결된 객체에 대해 작업을 수행할 수 있도록 라디오 버튼을 선택할 것입니다.

1. AWS Organizations 콘솔에서 AWS 계정 페이지로 이동합니다.
2. 루트(Root) 컨테이너 옆의 확인란 ☑ 을 선택합니다.
3. 하위 항목(Children) 탭에서 작업(Actions)을 선택한 다음 조직 단위(Organizational unit)에서 새로 만들기(Create new)를 선택합니다.
4. 루트에 조직 단위 생성(Create organizational unit in Root) 페이지에서 조직 단위 이름(Organizational unit name)에 **`Production`**을 입력한 다음 조직 단위 생성(Create organizational unit)을 선택합니다.
5. 새 Production OU 옆에 있는 확인란 ☑ 을 선택합니다.
6. 작업(Actions)을 선택한 다음 조직 단위(Organizational unit)에서 새로 만들기(Create new)를 선택합니다.
7. Production에 조직 단위 생성(Create organizational unit in Production) 페이지에서 두 번째 OU 이름에 **`MainApp`**을 입력한 다음 조직 단위 생성(Create organizational unit)을 선택합니다.

   이제 멤버 계정을 이상의 OU로 이동할 수 있습니다.

8. AWS 계정 페이지로 돌아가서 프로덕션 OU 옆에 있는 삼각형 ▶ 을 선택해 그 아래의 트리를 확장합니다. 이렇게 하면 Production의 하위 항목인 MainApp OU가 표시됩니다.
9. 333333333333 옆에 있는 확인란 ☑ (이름 아님)을(를) 선택하고 작업 선택 후 AWS 계정에서 이동을 선택합니다.
10. AWS 계정 '333333333333' 이동 페이지에서 프로덕션 옆에 있는 삼각형을 선택하여 확장합니다. MainApp 옆에 있는 라디오 버튼 ◉ (이름 아님)을(를) 선택한 다음 AWS 계정 이동을 선택합니다.
11. 222222222222 옆에 있는 확인란 ☑ (이름 아님)을(를) 선택하고 작업 선택 후 AWS 계정에서 이동을 선택합니다.
12. AWS 계정 '222222222222' 이동 페이지의 프로덕션 옆에 있는 라디오 버튼(이름이 아님)을 선택한 다음 AWS 계정 이동을 선택합니다.

3단계: 서비스 제어 정책 생성

이 섹션의 단계에서는 3가지 서비스 제어 정책(SCP)을 만들고 루트와 OU에 연결해 사용자가 조직 계정으로 할 수 있는 일을 제한합니다. 첫 번째 SCP는 모든 멤버 계정 사용자가 여러분이 구성한 어떤 AWS CloudTrail 로그도 생성하거나 수정하지 못하게 합니다. 관리 계정은 어떤 SCP의 영향도 받지 않으므로 CloudTrail SCP를 적용하고 나면 관리 계정에서 로그를 생성해야 합니다.

조직에 대해 서비스 제어 정책 유형 활성화

루트 내의 OU에 특정 유형의 정책을 연결하려면, 먼저 해당 조직에 정책 유형을 활성화해야 합니다. 정책 유형은 기본적으로 비활성화되어 있습니다. 이 섹션의 단계에서는 조직에 대해 서비스 제어 정책(SCP) 유형을 활성화하는 방법을 확인할 수 있습니다.

AWS Management Console

조직에 대해 SCP를 활성화하려면

1. 정책 페이지로 이동한 다음 서비스 제어 정책을 선택합니다.
2. 서비스 제어 정책 페이지에서 서비스 제어 정책 활성화(Enable service control policies)를 선택합니다.

이제 조직에서 SCP를 만들 수 있음을 알리는 녹색 배너가 나타납니다.

SCP 생성

이제 조직에서 서비스 제어 정책을 활성화했으므로 이 자습서에 필요한 세 가지 정책을 만들 수 있습니다.

AWS Management Console

CloudTrail 구성 작업을 차단하는 첫 번째 SCP를 만들려면

1. 정책 페이지로 이동한 다음 서비스 제어 정책을 선택합니다.
2. 서비스 제어 정책 페이지(Service control policies)에서 정책 생성(Create policy)을 선택합니다.
3. 정책 이름(Policy name)에 **Block CloudTrail Configuration Actions**을 입력합니다.
4. 정책 섹션의 오른쪽에 있는 서비스 목록에서 CloudTrail을 서비스로 선택합니다. 그런 다음 AddTags, CreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging 및 UpdateTrail 작업을 선택합니다.
5. 오른쪽 창에서 리소스 추가를 선택하고 CloudTrail 및 모든 리소스를 지정합니다. 그런 다음 리소스 추가를 선택합니다.

   왼쪽의 정책 문은 다음과 유사해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
```

```
            ]
        }
    ]
}
```

6. 정책 생성을 선택합니다.

두 번째 정책은 Production OU의 사용자와 역할에 대해 활성화하려는 서비스와 작업의 허용 목록을 정의합니다. 작업이 완료되면 Production OU의 사용자는 나열된 서비스 및 작업에만 액세스할 수 있습니다.

AWS Management Console

Production OU에 대해 승인된 서비스를 허용하는 두 번째 정책을 생성하려면

1. 서비스 제어 정책(Service control policies) 페이지에서 정책 생성(Create policy)을 선택합니다.
2. 정책 이름(Policy name)에 **`Allow List for All Approved Services`**을 입력합니다.
3. 커서를 정책 섹션의 오른쪽 창에 놓고 다음과 같은 정책을 붙여 넣습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. 정책 생성을 선택합니다.

최종 정책은 MainApp OU에서 사용이 차단된 서비스의 거부 목록을 제공합니다. 이 자습서의 경우 MainApp OU에 있는 계정의 Amazon DynamoDB에 대한 액세스를 차단합니다.

AWS Management Console

MainApp OU에서 사용할 수 없는 서비스에 대한 액세스를 거부하는 세 번째 정책을 생성하려면

1. 서비스 제어 정책(Service control policies) 페이지에서 정책 생성(Create policy)을 선택합니다.
2. 정책 이름(Policy name)에 **Deny List for MainApp Prohibited Services**을 입력합니다.
3. 정책(Policy) 섹션의 왼쪽에서 Amazon DynamoDB를 서비스로 선택합니다. 작업으로 모든 작업을 선택합니다.
4. 왼쪽 창에서 리소스 추가(Add resource)를 선택하고 DynamoDB 및 모든 리소스(All Resources)를 지정합니다. 그런 다음 리소스 추가를 선택합니다.

   오른쪽의 정책 문이 다음과 유사하게 업데이트됩니다.

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Deny",
         "Action": [ "dynamodb:*" ],
         "Resource": [ "*" ]
       }
     ]
   }
   ```

5. [Create policy]를 선택하여 SCP를 저장합니다.

OU에 SCP 연결

이제 SCP가 루트에서 활성화되었고, SCP를 루트와 OU에 연결할 수도 있습니다.

AWS Management Console

루트와 OU에 정책을 연결하려면

1. AWS 계정 페이지로 이동합니다.
2. AWS 계정 페이지에서 루트(Root)(라디오 버튼이 아닌 이름)를 선택하여 세부 정보 페이지로 이동합니다.

3. 루트 세부 정보 페이지에서 정책(Policies) 탭을 선택한 다음 서비스 제어 정책(Service Control Policies)에서 연결(Attach)을 선택합니다.
4. 서비스 제어 정책 연결(Attach a service control policy) 페이지에서 `Block CloudTrail Configuration Actions`라는 SCP 옆의 라디오 버튼을 선택한 다음 연결(Attach)을 선택합니다. 이 자습서에서는 모든 멤버 계정에 영향을 미치도록 루트에 연결하므로 다른 사람이 CloudTrail 구성을 변경하지 못합니다.

   루트(Root) 세부 정보 페이지의 정책(Policies) 탭에서 이제 2개의 SCP가 루트에 연결된 것이 보입니다. 방금 연결한 것과 기본 `FullAWSAccess` SCP입니다.
5. 다시 AWS 계정 페이지로 이동해 프로덕션(Production) OU(라디오 버튼이 아닌 이름)를 선택하여 세부 정보 페이지로 이동합니다.
6. Production OU의 세부 정보 페이지에서 정책(Policies) 탭을 선택합니다.
7. 서비스 제어 정책(Service Control Policies)에서 연결(Attach)을 선택합니다.
8. 서비스 제어 정책 연결(Attach a service control policy) 페이지에서 `Allow List for All Approved Services` 옆의 라디오 버튼을 선택한 다음 연결(Attach)을 선택합니다. 이렇게 하면 Production의 멤버 계정에 속한 사용자와 역할이 승인된 서비스에 액세스할 수 있습니다.
9. 정책(Policies) 탭을 다시 선택하면 2개의 SCP가 OU에 연결된 것이 보입니다. 방금 연결한 것과 기본 `FullAWSAccess` SCP입니다. 하지만 `FullAWSAccess` SCP는 모든 서비스와 작업을 허용하는 허용 목록이기 때문에, 승인된 서비스만 허용되도록 하려면 이제 이 SCP를 분리해야 합니다.
10. Production OU에서 기본 정책을 제거하려면 FullAWSAccess의 라디오 버튼을 선택하고, 분리(Detach)를 선택한 다음 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

    이 기본 정책을 제거하면, Production OU 아래에 있는 모든 멤버 계정은 이전 단계에서 연결한 허용 목록 SCP에 없는 모든 작업 및 서비스에 대한 액세스 권한을 즉시 잃어버리게 됩니다. 모든 승인된 서비스에 대한 허용 목록 SCP에 포함되지 않은 작업을 사용하기 위한 요청은 거부됩니다. 이러한 결과는 계정의 관리자가 멤버 계정 중 하나의 사용자에게 IAM 권한 정책을 연결하여 다른 서비스에 대한 액세스 권한을 부여하는 경우에도 마찬가지입니다.
11. 이제 `Deny List for MainApp Prohibited services`라는 SCP를 연결해 MainApp OU에 있는 계정 사용자 전원이 제한된 서비스를 이용하지 못하도록 할 수 있습니다.

    이렇게 하려면 AWS 계정 페이지로 이동하여 삼각형 아이콘을 선택하여 프로덕션(Production) OU의 분기를 확장한 다음 MainApp OU(라디오 버튼이 아닌 이름)를 선택해 해당 콘텐츠로 이동합니다.
12. MainApp 세부 정보 페이지에서 정책(Policies) 탭을 선택합니다.

13. 서비스 제어 정책(Service Control Policies)에서 연결(Attach)을 선택한 다음, 사용 가능한 정책 목록에서 MainApp 금지 서비스에 대한 거부 목록(Deny List for MainApp Prohibited Services) 옆에 있는 라디오 버튼을 선택한 다음 정책 연결(Attach policy)을 선택합니다.

4단계: 조직 정책 테스트

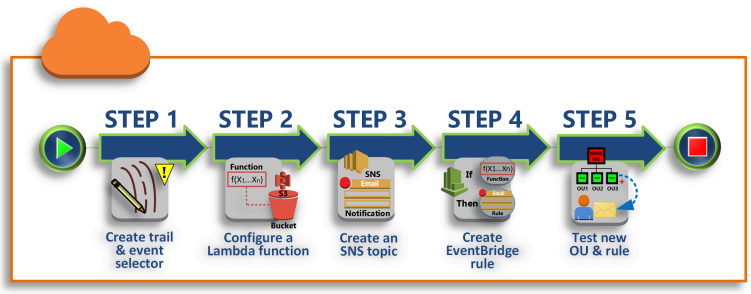
이제 멤버 계정의 사용자로 로그인해 다양한 AWS 작업을 수행해볼 수 있습니다.

- 관리 계정 사용자로 로그인하면, IAM 권한 정책이 허용하는 모든 작업을 수행할 수 있습니다. SCP는 관리 계정이 어떤 루트나 OU에 있더라도 계정의 사용자나 역할에는 영향을 주지 않습니다.
- 222222222222 계정의 사용자로 로그인하면, 허용 목록에서 허용되는 모든 작업을 수행할 수 있습니다. AWS Organizations는 허용 목록에 없는 서비스에서 작업을 수행하려는 시도를 거부합니다. 또한 AWS Organizations는 CloudTrail 구성 작업 수행도 거부합니다.
- 333333333333 계정의 사용자로 로그인하면, 허용 목록에서 허용되고 거부 목록에서 차단되지 않는 모든 작업을 수행할 수 있습니다. AWS Organizations는 허용 목록 정책에 없는 작업과 거부 목록 정책에 있는 작업을 수행하려는 시도를 거부합니다. 또한 AWS Organizations는 CloudTrail 구성 작업 수행도 거부합니다.

자습서: Amazon EventBridge를 사용하여 조직에 대한 중요 변경 사항 모니터링

이 자습서에서는 조직에 대한 변경 사항을 모니터링하도록 Amazon EventBridge(이전 Amazon CloudWatch Events)를 구성합니다. 먼저, 사용자가 특정 AWS Organizations 작업을 호출하면 트리거되는 규칙을 구성합니다. 그런 다음, 규칙이 트리거되면 AWS Lambda 함수를 실행하도록 Amazon EventBridge를 구성하고, 이벤트에 대한 세부 정보가 포함된 이메일을 전송하도록 Amazon SNS를 구성합니다.

다음 그림은 자습서의 기본 단계를 보여줍니다.



[1단계: 추적 및 이벤트 선택기 구성]

AWS CloudTrail에서 추적(trail)이라는 로그를 생성합니다. 모든 API 호출을 캡처하도록 이를 구성합니다.

[2단계: Lambda 함수 구성]

S3 버킷에 이벤트에 대한 세부 정보를 기록하는 AWS Lambda 함수를 생성합니다.

[3단계: 구독자에게 이메일을 전송하는 Amazon SNS 주제 생성]

이메일을 구독자에게 보내는 Amazon SNS 주제를 생성한 후, 주제를 직접 구독합니다.

[4단계: Amazon EventBridge 규칙 생성]

Amazon EventBridge가 지정된 API 호출 세부 사항을 Lambda 함수 및 SNS 주제 구독자에게 전달하도록 하는 규칙을 생성합니다.

[5단계: Amazon EventBridge 규칙 테스트]

모니터링되는 작업 중 하나를 실행하여 새 규칙을 테스트합니다. 이 자습서에서는 모니터링되는 작업이 조직 단위(OU)를 만드는 작업입니다. Lambda 함수가 생성하는 로그 항목을 확인하고, Amazon SNS가 구독자에게 보내는 이메일을 확인합니다.

> **도움말**
>
> 이 자습서를 비슷한 작업(계정 생성 완료 시 이메일 알림 전송 등)을 구성하기 위한 가이드로 사용할 수도 있습니다. 계정 생성은 비동기 작업이기 때문에 기본적으로 완료 시 알림이 발송되지 않습니다. AWS Organizations에서 AWS CloudTrail 및 Amazon EventBridge를 사용하는 방법에 대한 자세한 내용은 AWS Organizations의 로깅 및 모니터링 섹션을 참조하세요.

필요 조건

이 튜토리얼는 다음과 같이 가정합니다.

- 사용자는 조직의 관리 계정의 IAM 사용자로 AWS Management Console에 로그인할 수 있습니다. IAM 사용자에게는 CloudTrail에 로그를, Lambda에 함수를, Amazon SNS에 주제를, 그리고 Amazon EventBridge에 규칙을 생성하고 구성할 수 있는 권한이 있어야 합니다. 권한 부여에 대한 자세한 내용은 IAM 사용 설명서의 액세스 관리, 또는 액세스를 구성하려는 서비스의 설명서를 참조하세요.
- 1단계에서 구성한 CloudTrail 로그를 수신하려면 기존 Amazon Simple Storage Service(Amazon S3) 버킷에 대한 액세스 권한이 있거나 버킷을 생성할 수 있는 권한이 있어야 합니다.

> **Important**
>
> 현재 AWS Organizations는 전역적으로 사용할 수 있긴 하지만 미국 동부(버지니아 북부) 리전에서만 호스팅됩니다. 이 자습서의 단계를 수행하려면 해당 리전을 사용하여 AWS Management Console을 구성해야 합니다.

1단계: 추적 및 이벤트 선택기 구성

이 단계에서는 관리 계정에 로그인하고 AWS CloudTrail에 로그(추적이라고 함)를 구성합니다. 또한 모든 읽기/쓰기 API 호출을 캡처하여 Amazon EventBridge에서 트리거를 일으킬 호출이 발생되도록 추적에 이벤트 선택기도 구성합니다.

추적을 생성하려면

1. 조직의 관리 계정의 관리자로 AWS에 로그인한 다음, https://console.aws.amazon.com/cloudtrail/에서 CloudTrail 콘솔을 엽니다.
2. 콘솔의 오른쪽 상단에 있는 탐색 모음에서 미국 동부(버지니아 북부) 리전을 선택합니다. 다른 리전을 선택하는 경우 AWS Organizations가 Amazon EventBridge 구성 설정의 옵션으로 표시되지 않으며 CloudTrail이 AWS Organizations에 대한 정보를 캡처할 수 없습니다.
3. 탐색 창에서 [Trails]를 선택합니다.
4. 추적 생성을 선택합니다.
5. 추적 이름에 **`My-Test-Trail`**을 입력합니다.
6. 다음 옵션 중 하나를 수행하여 CloudTrail이 해당 로그를 제공하는 위치를 지정합니다.

   - 버킷을 생성해야 하는 경우 Create new S3 bucket(새 S3 버킷 생성)을 선택한 다음 Trail log bucket and folder(추적 로그 버킷 및 폴더)에 새 버킷의 이름을 입력합니다.

     > **Note**
     >
     > S3 버킷 이름은 전역적으로 고유해야 합니다.

   - 버킷이 이미 있는 경우 Use existing S3 bucket(기존 S3 버킷 사용)을 선택한 다음 S3 bucket(S3 버킷) 목록에서 버킷 이름을 선택합니다.
7. 다음을 선택합니다.
8. Choose log events(로그 이벤트 선택) 페이지의 Management events(관리 이벤트) 섹션에서 Read(읽기)와 Write(쓰기)를 선택합니다.

9. 다음을 선택합니다.
10. 선택 사항을 검토하고 Create trail(추적 생성)을 선택합니다.

Amazon EventBridge를 사용하면 경보 규칙이 들어오는 API 호출과 일치하는 경우 경보를 보내는 여러 가지 방법을 선택할 수 있습니다. 이 자습서에서는 API 호출을 기록할 수 있는 Lambda 함수를 호출하는 방법과, 주제의 구독자에게 이메일이나 문자 메시지를 보내는 Amazon SNS 주제에 정보를 전송하는 방법 등 두 가지 방법을 설명합니다. 다음 두 단계에서는 필요한 구성 요소인 Lambda 함수 및 Amazon SNS 주제를 생성합니다.

2단계: Lambda 함수 구성

이 단계에서는 사용자가 나중에 구성하는 Amazon EventBridge 규칙에 따라 이 함수에 전송되는 API 활동을 기록하는 Lambda 함수를 만듭니다.

Amazon EventBridge 이벤트를 기록하는 Lambda 함수를 만들려면

1. AWS Lambda에서 https://console.aws.amazon.com/lambda/ 콘솔을 엽니다.
2. Lambda를 처음 사용하는 경우 시작 페이지에서 Get Started Now(지금 시작)를 선택합니다. 처음 사용하는 경우가 아니라면 Create function(함수 만들기)을 선택합니다.
3. 함수 생성 페이지에서 Use a blueprint(블루프린트 사용)을 선택합니다.
4. 블루프린트 검색 상자에 필터로 **`hello`**를 입력하고 hello-world 블루프린트를 선택합니다.
5. 구성을 선택합니다.
6. 기본 정보 페이지에서 다음을 수행합니다.
   a. Lambda 함수 이름에서 이름(Name)에 **`LogOrganizationEvents`**를 입력합니다.
   b. 역할(Role)에서 기본 Lambda 권한을 가진 새 역할 생성(Create a new role with basic Lambda permissions)을 선택합니다. 이 역할은 필요한 데이터에 액세스할 수 있고 출력 로그를 쓸 수 있는 권한을 Lambda 함수에 부여합니다.
7. 다음 예와 같이 Lambda 함수 코드를 편집합니다.

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
```

```
};
```

이 샘플 코드는 **LogOrganizationEvents** 마커 문자열이 있는 이벤트를, 이벤트를 구성하는 JSON 문자열 앞에 기록합니다.

8. 함수 생성(Create function)을 선택합니다.

3단계: 구독자에게 이메일을 전송하는 Amazon SNS 주제 생성

이 단계에서는 정보를 구독자에게 이메일로 보내는 Amazon SNS 주제를 생성합니다. 이 주제를 나중에 만드는 Amazon EventBridge 규칙의 대상으로 지정합니다.

Amazon SNS 주제를 만들어 구독자에게 이메일을 전송하려면

1. https://console.aws.amazon.com/sns/v3/에서 Amazon SNS 콘솔을 엽니다.
2. 탐색 창에서 주제를 선택합니다.
3. [Create new topic]을 선택합니다.
   a. 주제 이름에 **OrganizationsCloudWatchTopic**을 입력합니다.
   b. 표시 이름에 **OrgsCWEvnt**를 입력합니다.
   c. 주제 생성을 선택합니다.
4. 이제 주제에 대한 구독을 생성할 수 있습니다. 방금 생성한 주제에 대한 ARN을 선택합니다.
5. 구독 생성을 선택합니다.
   a. [Create subscription] 페이지에서 [Protocol]에 대해 [Email]을 선택합니다.
   b. Endpoint(엔드포인트)에 이메일 주소를 입력합니다.
   c. 구독 생성을 선택합니다. AWS가 이전 단계에서 지정한 이메일 주소로 이메일을 보냅니다. 해당 이메일에 도착할 때까지 기다렸다가 이메일의 구독 확인 링크를 선택하여 이메일을 잘 수신했음을 확인합니다.
   d. 콘솔로 돌아가 페이지를 새로 고칩니다. [Pending confirmation] 메시지가 사라지고 대신 유효한 구독 ID가 표시됩니다.

4단계: Amazon EventBridge 규칙 생성

이제 필요한 Lambda 함수가 계정에 존재하므로 규칙의 기준이 충족되면 이 함수를 호출하는 Amazon EventBridge 규칙을 만듭니다.

EventBridge 규칙을 생성하려면

1. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
2. 콘솔을 미국 동부(버지니아 북부) 리전으로 설정해야 합니다. 그렇지 않으면 Organizations에 대한 정보를 사용할 수 없습니다. 콘솔의 오른쪽 상단에 있는 탐색 모음에서 미국 동부(버지니아 북부) 리전을 선택합니다.
3. 규칙을 만드는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서에서 Amazon EventBridge 시작하기를 참조하세요.

5단계: Amazon EventBridge 규칙 테스트

이 단계에서는 조직 단위(OU)를 생성한 다음 Amazon EventBridge 규칙을 살펴보고, 로그 항목을 생성하고, 이벤트에 대한 세부 정보가 들어 있는 이메일을 본인에게 전송합니다.

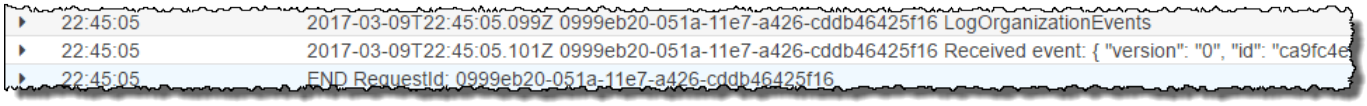
AWS Management Console

OU를 만들려면

1. AWS Organizations 콘솔의 AWS 계정 페이지를 엽니다.
2. Root OU 확인란 ☑ 을 선택하고, 작업(Actions)을 선택한 다음 조직 단위(Organizational unit)에서 새로 만들기(Create new)를 선택합니다.
3. OU의 이름에는 **`TestCWEOU`**을 입력한 후 조직 단위 생성을 선택합니다.

EventBridge 로그 항목을 보려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 페이지에서 로그를 선택합니다.
3. 로그 그룹(Log Groups) 아래에서 Lambda 함수 /aws/lambda/LogOrganizationEvents와 연결된 그룹을 선택합니다.
4. 각 그룹에는 하나 이상의 스트림이 있어야 하고, 현 시점에 그룹이 한 개 있어야 합니다. 이를 선택합니다.
5. 로그를 확인합니다. 다음과 같은 행이 표시될 것입니다.



6. 항목의 가운데 행을 선택하여 수신한 이벤트의 전체 JSON 텍스트를 확인합니다. 출력의 `requestParameters` 및 `responseElements` 섹션에서 API 요청의 세부 정보를 모두 볼 수 있습니다.

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
```

```
        "eventType": "AwsApiCall"
    }
}
```

7. 이메일 계정에서 OrgsCWEvnt(Amazon SNS 주제의 표시 이름)에서 보낸 메시지를 확인합니다. 이메일 본문에는 이전 단계에서 표시된 로그 항목과 동일한 JSON 텍스트 출력이 들어 있습니다.

정리: 더 이상 필요하지 않은 리소스 제거

요금이 부과되지 않게 하려면, 이 자습서 과정에서 생성했지만 유지하지 않으려는 AWS 리소스를 삭제해야 합니다.

AWS 환경을 정리하려면

1. CloudTrail 콘솔을 사용하여 1단계에서 생성한 **My-Test-Trail**이라는 추적을 삭제합니다.
2. 1단계에서 Amazon S3 버킷을 만는 경우 Amazon S3 콘솔을 사용하여 버킷을 삭제합니다.
3. Lambda 콘솔을 사용하여 2단계에서 생성한 **LogOrganizationEvents**라는 함수를 삭제합니다.
4. Amazon SNS 콘솔을 사용해 3단계에서 생성한 **OrganizationsCloudWatchTopic**이라는 Amazon SNS 주제를 삭제합니다.
5. CloudWatch 콘솔을 사용하여 4단계에서 생성한 **OrgsMonitorRule**이라는 EventBridge 규칙을 삭제합니다.
6. 마지막으로 Organizations 콘솔을 사용하여 5단계에서 생성한 **TestCWEOU**라는 OU를 삭제합니다.

그러면 다된 것입니다. 이 자습서에서는 조직에 대한 변경 사항을 모니터링하도록 EventBridge를 구성했습니다. 또한 사용자가 특정 AWS Organizations 작업을 호출하면 트리거되는 규칙을 구성했습니다. 이 규칙은 이벤트를 기록하고 해당 이벤트에 대한 세부 정보가 들어 있는 이메일을 전송하는 Lambda 함수를 실행했습니다.

다중 계정 관리의 모범 사례

다음 권장 사항은 AWS Organizations에서 다중 계정 환경을 설정하고 관리하는 방법을 알려 드립니다.

주제

단일 조직 내에서 계정 관리

단일 조직을 만들고 이 조직 내에서 모든 계정을 관리하는 것이 좋습니다. 조직은 사용자 환경 내 계정 간에 일관성을 유지할 수 있게 해주는 보안 경계입니다. 중앙에서 조직 내 계정 전체에 정책 또는 서비스 수준 구성을 적용할 수 있습니다. 다중 계정 환경 전반에서 일관된 정책, 중앙집중식 가시성, 프로그래밍적 제어를 구현하려면 단일 조직 내에서 이 작업을 수행하는 것이 가장 좋습니다.

루트 사용자에 대한 강력한 암호 사용

강력하고 고유한 암호를 사용하는 것이 좋습니다. 다수의 암호 관리자와 강력한 암호 생성 알고리즘 및 도구를 사용하면 이러한 목표를 달성하는 데 도움이 될 수 있습니다. 자세한 내용은 AWS 계정 루트 사용자의 암호 변경을 참조하십시오. 회사의 정보 보안 정책에 따라 루트 사용자의 암호에 대한 액세스

및 장기 저장을 관리합니다. 조직의 보안 요구 사항을 충족하는 암호 관리자 시스템 또는 이와 동등한 시스템에 암호를 저장하는 것이 좋습니다. 순환 종속성이 발생하지 않도록 하려면 보호된 계정으로 로그인하는 AWS 서비스를 사용하는 도구로 루트 사용자 암호를 저장하지 않아야 합니다. 어떤 방법을 선택하든 복원력에 우선 순위를 두는 것이 좋으며 보호 강화를 위해 여러 주체에게 이 저장소에 대한 액세스 권한을 부여하는 것을 고려할 것을 권장합니다. 암호 또는 암호 보관 위치에 대한 모든 액세스를 로그에 기록하고 모니터링해야 합니다. 추가 루트 사용자 암호 권장 사항은 AWS 계정의 루트 사용자 모범 사례를 참조하십시오.

루트 사용자 보안 인증 사용에 관한 프로세스의 문서화

각 단계에 관여한 개인에 대한 기록을 확보할 수 있도록 중요한 프로세스의 실행을 수행 시점에 문서화합니다. 암호를 관리하려면 암호화된 보안 암호 관리자를 사용하는 것이 좋습니다. 발생할 가능성이 있는 예외 상황 및 예기치 않은 이벤트에 대한 문서를 제공하는 것도 중요합니다. 자세한 내용은 로그인 사용 설명서의 AWS 로그인 사용자 설명서의 AWS Management Console 로그인 문제 해결 및 IAM 사용자 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

최소한 분기별로 루트 사용자에 대한 액세스 권한을 계속 보유하고 있는지, 연락처 번호가 유효한지 테스트하고 확인합니다. 이렇게 하면 프로세스가 작동하는지, 루트 사용자에 대한 액세스 권한을 유지 관리하고 있는지 확인하는 데 도움을 줍니다. 또한 루트 액세스를 담당하는 사람들이 프로세스가 성공하기 위해 수행해야 하는 단계를 이해하고 있음을 보여줍니다. 응답 시간과 성공률을 늘리려면 프로세스에 관련된 모든 담당자가 액세스가 필요할 경우 수행해야 하는 작업을 정확히 이해하도록 하는 것이 중요합니다.

루트 사용자 자격 증명에 MFA 사용

AWS 계정 루트 사용자 및 AWS 계정의 IAM 사용자에 대해 여러 다중 인증(MFA) 디바이스를 활성화하는 것이 좋습니다. 이를 통해 AWS 계정의 보안 기준을 높이고 AWS 계정 루트 사용자와 같이 권한이 높은 사용자에 대한 액세스 관리를 간소화할 수 있습니다. 다양한 고객 요구를 충족하기 위해 AWS은(는) FIDO 보안 키, 가상 인증자 애플리케이션, 시간 기반 일회용 암호(TOTP) 하드웨어 토큰 등 세 가지 유형의 IAM용 MFA 디바이스를 지원합니다.

각 유형의 인증자는 각기 다른 사용 사례에 적합하도록 물리적 및 보안 속성이 약간씩 다릅니다. FIDO2 보안 키는 최고 수준의 보안을 제공하며 피싱에 강합니다. 모든 형태의 MFA는 암호 전용 인증보다 더 강력한 보안 체계를 제공하므로 계정에 어떤 형태로든 MFA를 추가할 것을 강력하게 권장합니다. 보안 및 운영 요구 사항에 가장 적합한 디바이스 유형을 선택합니다.

TOTP 하드웨어 토큰과 같이 배터리 구동 장치를 기본 인증자로 선택하는 경우 배터리를 백업 메커니즘으로 사용하지 않는 인증자를 등록하는 것도 고려하십시오. 또한 디바이스의 기능을 정기적으로 점

검하고 만료일 전에 교체하는 것도 중단 없는 액세스를 유지하는 데 필수적입니다. 어떤 유형의 디바이스를 선택하든 디바이스 손실 또는 장애에 대한 복원력을 높이려면 최소 2개 이상의 디바이스(IAM은 사용자당 최대 8개의 MFA 디바이스 지원)를 등록하는 것이 좋습니다.

MFA 디바이스 스토리지에 대한 조직의 정보 보안 정책을 따르십시오. MFA 디바이스는 관련 암호와 분리하여 별도로 저장하는 것이 좋습니다. 이렇게 하면, 암호와 MFA 디바이스에 액세스하기 위해 다양한 리소스(사람, 데이터, 도구)가 있어야 합니다. 이렇게 분리함으로써 무단 액세스에 대한 별도의 보호 계층이 추가됩니다. 또한 MFA 디바이스 또는 해당 스토리지 위치에 대한 모든 액세스를 로그에 기록하고 모니터링하는 것이 좋습니다. 이렇게 하면 무단 액세스를 감지하고 이에 대응할 수 있습니다.

자세한 내용은 IAM 사용 설명서의 다중 인증(MFA)으로 루트 사용자 보안을 참조하십시오. MFA 활성화에 대한 설명은 AWS에서 다중 인증(MFA) 사용하기 및 AWS에서 사용자를 위한 MFA 디바이스 활성화를 참조하십시오.

루트 사용자 자격 증명에 대한 액세스를 모니터링하는 통제 수단 적용

루트 사용자 자격 증명에 액세스하는 일은 드물어야 합니다. Amazon EventBridge 와 같은 도구를 사용해 알림을 생성하여 관리 계정 루트 사용자 보안 인증의 로그인 및 사용을 알리도록 합니다. 이 알림에는 루트 사용자 자체에 사용되는 이메일 주소가 포함되나 이에 국한되지는 않습니다. 이 알림은 중요하며 놓치기 어렵도록 되어야 합니다. 예시는 AWS 계정 루트 사용자 활동의 모니터링 및 통지를 참조하세요. 이러한 알림을 받는 담당자는 루트 사용자 액세스가 정상적인지 확인하는 방법을 이해하고, 보안 인시던트가 진행 중이라고 판단되는 경우 에스컬레이션하는 방법을 이해해야 합니다. 자세한 내용은 의심스러운 이메일 보고 또는 취약성 보고를 참조하십시오. 또는 AWS에 문의하여 지원 및 추가 안내 요청을 받을 수도 있습니다.

연락 전화번호를 최신 상태로 유지하기

AWS 계정에 대한 액세스 권한을 복구하려면 문자 메시지 또는 전화를 받을 수 있는 유효하고 활성화된 연락 전화번호를 확보하는 것이 중요합니다. 계정 지원 및 복구 목적으로 AWS이(가) 연락할 수 있도록 전용 전화번호를 사용하는 것이 좋습니다. 계정 전화번호는 AWS Management Console 또는 계정 관리 API를 통해 쉽게 조회하고 관리할 수 있습니다.

AWS이(가) 사용자에게 연락할 수 있는 전용 전화번호를 가지는 방법에는 여러 가지가 있습니다. 전용 SIM 카드와 실제 휴대폰을 구입하는 것이 가장 좋습니다. 휴대폰과 SIM을 장기간 안전하게 보관하여 계정 복구 시 전화번호를 사용할 수 있도록 하세요. 또한 모바일 청구서를 담당하는 팀은 이 번호가 장기간 비활성 상태로 남아 있더라도 그 유지의 중요성을 이해해야 합니다. 보호를 강화하기 위해 조직 내에서 이 전화번호를 기밀로 유지해야 합니다.

AWS 연락처 정보 콘솔 페이지에 전화번호를 문서화하고 조직에서 해당 전화번호를 알아야 하는 특정 팀과 세부 정보를 공유하세요. 이러한 방식으로 전화번호를 다른 SIM으로 이전할 때 발생하는 위험을 최소화하는 데 도움이 됩니다. 기존 정보 보안 정책에 따라 전화를 보관합니다. 그러나 전화를 다른 관련 자격 증명 정보와 같은 위치에 저장하면 안 됩니다. 전화 또는 전화의 보관 위치에 대한 모든 액세스는 기록하고 모니터링해야 합니다. 계정과 연결된 전화번호가 변경될 경우 기존 문서에서 전화번호를 업데이트하는 프로세스를 구현합니다.

루트 계정에 그룹 이메일 주소 사용하기

회사에서 관리하는 이메일 주소를 사용합니다. 받은 메시지를 사용자 그룹에 직접 전달하는 이메일 주소를 사용합니다. 예를 들어 액세스 확인을 위해 AWS이(가) 계정 소유자에게 연락해야 하는 경우 이메일 메시지가 여러 당사자에게 배포됩니다. 이러한 방식은 개인이 휴가 중이거나 아프거나 회사를 떠난 경우에도 응답이 지연될 위험을 줄이는 데 도움이 됩니다.

보고 구조가 아닌 비즈니스 목적에 따라 워크로드 그룹화

프로덕션 워크로드 환경과 데이터를 최상위 워크로드 중심 OU에 분리하는 것이 좋습니다. OU는 회사의 보고 구조를 반영하기보다는 공통된 제어 집합을 기반으로 해야 합니다. 프로덕션 OU와는 별도로, 워크로드를 개발하고 테스트하는 데 사용되는 계정 및 워크로드 환경이 포함된 비-프로덕션 OU를 하나 이상 정의하는 것이 좋습니다. 추가적인 안내는 워크로드 지향 OU 구성을 참조하십시오.

여러 계정을 사용하여 워크로드 정리하기

AWS 계정은(는) AWS 리소스에 대한 자연 보안, 액세스, 청구 범위를 제공합니다. 여러 계정을 사용하면 계정 수준의 할당량과 API 요청 속도 한도를, 여기에 나열된 추가 혜택을 분산할 수 있어 이점이 있습니다. 보안, 로그, 인프라용 계정과 같은 전사적 차원의 기본 계정을 여러 개 사용하는 것이 좋습니다. 워크로드 계정의 경우 테스트/개발 워크로드에서 프로덕션 워크로드를 별도의 계정에 분리해야 합니다.

서비스 콘솔 또는 API/CLI 작업을 사용하여 조직 수준에서 AWS 서비스 활성화

한 가지 모범 사례로, 서비스 콘솔 또는 이에 상응하는 API 작업/CLI 명령어를 사용하여 AWS Organizations에서 통합하려는 모든 서비스를 활성화 또는 비활성화하는 것이 좋습니다. 이 방법을 사용하면 AWS 서비스가 조직에 필요한 모든 초기화 단계 (예: 필수 리소스 생성 및 서비스 비활성화 시 리소스 정리)를 수행할 수 있습니다. AWS Account Management은(는) AWS Organizations 콘솔 또는

API를 사용해야 활성화할 수 있는 유일한 서비스입니다. AWS Organizations와(과) 통합된 서비스 목록을 검토하려면 AWS 함께 사용할 수 있는 서비스 AWS Organizations을(를) 참조하십시오.

결제 도구를 사용하여 비용 추적 및 리소스 사용 최적화

조직을 관리하면 조직 내 계정에서 발생하는 모든 요금이 포함된 통합 청구서를 받게 됩니다. 비용 가시성에 대한 액세스가 필요한 비즈니스 사용자의 경우, 관리 계정의 역할에 결제 및 비용 도구를 검토할 수 있는 제한적 읽기 전용 권한을 부여할 수 있습니다. 예를 들어, 결제 보고서에 액세스할 수 있는 권한 집합을 만들거나 AWS Cost Explorer Service(시간 경과에 따른 비용 추세를 보는 도구) 및 Amazon S3 스토리지 렌즈 및 AWS Compute Optimizer와 같은 비용 효율성 서비스를 사용할 수 있습니다.

조직 리소스 전반의 태그 지정 전략 및 태그 적용 계획

계정과 워크로드가 확장되면 비용 추적, 액세스 제어 및 리소스 구성에 태그 기능이 유용할 수 있습니다. 태그 명명 전략에 대해서는 AWS 리소스 태깅의 지침을 따르세요. 리소스 외에도 조직 루트, 계정, OU, 정책의 태그를 만들 수 있습니다. 자세한 내용은 태깅 전략 구축을 참조하십시오.

관리 계정의 모범 사례

AWS Organizations의 관리 계정을 안전하게 보호하려면 다음 권장 사항을 따르는 것이 좋습니다. 이러한 권장 사항에서는 루트 사용자가 실제로 필요한 작업에만 루트 사용자를 사용하는 모범 사례 또한 준수한다고 가정합니다.

주제

- 관리 계정에 액세스할 수 있는 사용자 제한
- 액세스 권한이 있는 사람에 대한 검토 및 추적
- 관리 계정이 필요한 작업에 대해서만 관리 계정 사용
- 조직의 관리 계정에 워크로드를 배포하지 않기
- 탈중앙화를 위해 관리 계정 외부에 책임 위임하기

관리 계정에 액세스할 수 있는 사용자 제한

관리 계정은 계정 관리, 정책, 다른 AWS 서비스와의 통합, 통합 결제 등과 같이 언급된 모든 관리 작업의 핵심입니다. 따라서 조직을 변경할 권한이 필요한 관리자만 관리 계정에 액세스할 수 있도록 제한하십시오.

액세스 권한이 있는 사람에 대한 검토 및 추적

관리 계정에 대한 액세스 권한이 관리되고 있는지 확인하기 위해 해당 계정에 연결된 이메일 주소, 암호, MFA 및 전화번호에 액세스할 수 있는 회사 직원을 정기적으로 검토합니다. 기존의 회사 절차에 맞게 검토를 수행합니다. 적절한 사람만 액세스할 수 있도록 이 정보에 대한 월별 또는 분기별 검토를 추가합니다. 루트 사용자 자격 증명에 대한 액세스를 복구하거나 재설정하는 프로세스가 특정 개인에 의존하여 완료되지 않도록 합니다. 모든 프로세스는 당사자가 없을 가능성을 고려해야 합니다.

관리 계정이 필요한 작업에 대해서만 관리 계정 사용

관리 계정과 그 사용자 및 역할은 해당 계정으로 수행해야 하는 작업에 대해서만 사용하는 것이 좋습니다. 모든 AWS 리소스를 조직의 다른 AWS 계정에 저장하고 관리 계정이 접근하지 못하도록 합니다. 리소스를 다른 계정에 보관하는 것이 중요한 한 가지 이유는 Organizations 서비스 제어 정책(SCP)의 작동상 관리 계정의 사용자 또는 역할을 제한하지 않기 때문입니다. 관리 계정에서 리소스를 분리하면 인보이스의 요금을 파악하는 데도 도움이 됩니다.

조직의 관리 계정에 워크로드를 배포하지 않기

권한 있는 작업은 조직의 관리 계정 내에서 수행할 수 있으며 SCP는 관리 계정에는 적용되지 않습니다. 그러므로 관리 계정에 포함된 클라우드 리소스와 데이터는 관리 계정에서 관리해야 하는 항목으로만 제한해야 합니다.

탈중앙화를 위해 관리 계정 외부에 책임 위임하기

가능하면 관리 계정 외부에 책임과 서비스를 위임하는 것이 좋습니다. 관리 계정에 액세스하지 않고도 조직의 요구 사항을 관리할 수 있도록 팀에 자체 계정 권한을 부여합니다. 또한 조직 전체에 소프트웨어를 공유하는 AWS Service Catalog 또는 스택을 작성 및 배포하는 AWS CloudFormation StackSets와 같이 이 기능을 지원하는 서비스에 여러 명의 관리자를 등록할 수 있습니다.

자세한 내용을 확인하려면 보안 참조 아키텍처, 다중 계정을 사용한 AWS 환경 구성 및 AWS 함께 사용할 수 있는 서비스 AWS Organizations에서 다양한 AWS 서비스에 대해 멤버 계정을 위임 관리자로 등록하는 방법을 참조하십시오. 위임된 관리자 설정에 대한 자세한 내용은 AWS Account Management 에 대해 위임된 관리자 계정 활성화 및 에 대한 위임 관리자 AWS Organizations을(를) 참조하십시오.

멤버 계정의 모범 사례

조직의 멤버 계정 보안을 유지하려면 다음 권장 사항을 따르십시오. 이러한 권장 사항에서는 루트 사용자가 실제로 필요한 작업에만 루트 사용자를 사용하는 모범 사례 또한 준수한다고 가정합니다.

주제

계정 이름 및 속성 정의

멤버 계정의 경우 계정 용도를 반영하는 명명 구조와 이메일 주소를 사용하십시오. 예를 들어, `WorkloadsFooADev`에는 `Workloads+fooA+dev@domain.com`, `WorkloadsFooBDev`에는 `Workloads+fooB+dev@domain.com` 등입니다. 조직에 대해 정의된 사용자 지정 태그가 있는 경우, 해당 태그는 계정 사용량, 비용 센터, 환경 및 프로젝트를 반영하는 계정에 할당하는 것이 좋습니다. 이렇게 하면 계정을 쉽게 식별, 구성, 검색할 수 있습니다.

환경 및 계정 사용의 효율적 확장

규모를 확장할 때 새 계정을 만들기 전에 유사한 요구사항을 충족하는 계정이 이미 존재하지 않는지 확인하여 불필요한 중복을 피하세요. AWS 계정은(는) 공통 액세스 요구 사항을 기반으로 해야 합니다. 샌드박스 계정 등의 계정을 재사용하려는 경우 계정에서 불필요한 리소스나 워크로드를 정리하되 나중에 사용할 수 있도록 계정을 저장해 두는 것이 좋습니다.

계정을 해지하기 전에 해지 계정 할당량 한도가 적용된다는 점을 참고하세요. 자세한 내용은 에 대한 할당량 AWS Organizations 섹션을 참조하세요. 가능하면 계정을 해지하고 새 계정을 만드는 대신 계정을 재사용하는 정리 프로세스를 구현하는 것이 좋습니다. 이렇게 하면 리소스 실행으로 인한 비용 발생과 CloseAccount API 한도에 도달하는 것을 방지할 수 있습니다.

SCP를 사용하여 멤버 계정의 루트 사용자가 수행할 수 있는 작업을 제한합니다.

조직에서 서비스 제어 정책(SCP)을 만들고 조직의 루트에 연결하여 모든 멤버 계정에 적용하는 것이 좋습니다. 자세한 내용은 조직 계정 루트 사용자 보안 인증 보안을 참조하십시오.

멤버 계정에서 수행해야 하는 특정 루트 전용 작업을 제외한 모든 루트 작업을 거부할 수 있습니다. 다음 예제 SCP는 모든 멤버 계정의 루트 사용자가 AWS 서비스 API 호출을 하지 못하도록 합니다(단, “잘못 구성되어 모든 보안 주체에 대한 액세스를 거부하는 S3 버킷 정책 업데이트”(루트 보안 인증이 필요한 작업 중 하나)는 예외). 자세한 내용은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

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

    "Statement": [

        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
 "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }

        }

    ]
 }
```

대부분의 상황에서 모든 관리 작업은 관련 관리자 권한을 보유한 멤버 계정의 AWS Identity and Access Management(IAM) 역할로 수행할 수 있습니다. 이러한 역할에는 활동을 제한하고, 기록하고, 모니터링하는 적절한 제어 기능이 적용되어야 합니다.

조직 생성 및 관리

AWS Organizations 콘솔을 사용하거나 AWS Command Line Interface(AWS CLI) 명령 또는 그와 동등한 AWS SDK API 작업을 실행하여 다음의 작업을 수행할 수 있습니다.

- 조직 생성. 현재 계정을 관리 계정으로 이용하는 조직을 생성합니다. 조직 내 멤버 계정을 만들고, 다른 계정을 조직에 초대합니다.
- 조직 내에서 모든 기능을 활성화합니다. AWS Organizations를 사용하려면 모든 기능을 활성화하는 것이 좋습니다. 조직을 생성할 때 통합 결제를 위해 모든 기능 또는 기능 하위 집합을 활성화하는 옵션이 있습니다. 모든 기능 활성화가 기본값이고 통합 결제 기능이 포함됩니다.

  모든 기능이 활성화되어 있으면 AWS Organizations의 서비스 제어 정책(SCP)과 같은 고급 계정 관리 기능을 사용할 수 있습니다. SCP는 조직 내 모든 계정에 허용되는 최대 권한에 대한 중앙 집중식 관리를 제공합니다. 이는 계정이 조직의 액세스 제어 지침을 준수하는 데 도움을 줍니다.
- 조직에 대한 세부 정보를 확인합니다. 조직과 조직의 루트, 조직 단위(OU) 및 계정에 대한 세부 정보를 확인합니다.
- 조직을 삭제합니다. 필요 없는 조직을 삭제합니다.

> **Note**
>
> 이번 섹션에 나오는 절차는 작업 수행에 필요한 최소 권한을 지정합니다. 일반적으로 API에 적용 또는 명령줄 도구에 액세스 등이 있습니다.
> 콘솔에서 작업을 수행하려면 추가 권한이 필요할 때도 있습니다. 예를 들어 조직 내 모든 사용자에게 읽기 전용 권한을 부여한 후 선택한 사용자가 특정 작업을 수행하게 하는 다른 권한을 부여할 수 있습니다.

조직 생성

AWS 계정을 관리 계정으로 시작하는 조직을 생성할 수 있습니다. 조직을 생성할 때 조직이 통합 결제 기능만 지원할지, 아니면 모든 기능을 지원할지(권장)를 선택할 수 있습니다.

조직을 만든 후 관리 계정에서 다음과 같은 방법으로 조직에 계정을 추가할 수 있습니다.

- 조직에 멤버 계정으로 자동 추가되는 다른 AWS 계정을 만듭니다.
- 이메일 주소를 확인한 후 기존 AWS 계정을 초대하여 조직에 멤버 계정으로 가입시킬 수 있습니다.

조직 생성

AWS Management Console을 사용하거나 AWS CLI 또는 임의의 SDK API에서 명령을 사용하여 조직을 생성할 수 있습니다.

> **최소 권한**
>
> 현재 AWS 계정으로 조직을 생성하려면 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:CreateOrganization`
> - `iam:CreateServiceLinkedRole`
>
> 이 권한은 서비스 보안 주체 `organizations.amazonaws.com`에 대해서만 제한할 수 있습니다.

AWS Management Console

조직을 생성하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 기본적으로 조직은 모든 기능이 활성화된 상태로 생성됩니다. 그러나 다음 단계 중 하나를 선택할 수 있습니다.

   - 모든 기능을 활성화한 상태로 조직을 생성하려면 소개 페이지에서 조직 생성(Create an organization)을 선택합니다.
   - 통합 결제 기능만 있는 조직을 생성하려면 소개 페이지의 조직 생성(Create an organization)에서 통합 결제 기능(consolidated billing features)을 선택하고 확인 대화 상자에서 조직 생성(Create an organization)을 선택합니다.

   실수로 잘못된 옵션을 선택했다면 즉시 설정(Settings) 페이지로 이동한 다음 조직 삭제(Delete organization)를 선택하여 다시 시작할 수 있습니다.
3. 조직이 생성되고 AWS 계정 페이지가 표시됩니다. 표시되는 유일한 계정은 관리 계정입니다. 이 계정은 현재 루트 조직 단위(OU)에 저장되어 있습니다.

   필요한 경우 Organizations가 관리 계정과 연결된 주소로 확인 이메일을 자동으로 전송합니다. 확인 이메일을 받기까지 어느 정도 시간이 걸릴 수 있습니다. 24시간 내에 이메일 주소를 확인

하세요. 자세한 정보는 이메일 주소 확인 섹션을 참조하세요. 관리 계정의 이메일 주소를 확인하지 않고 새 계정을 만들어 조직에 추가할 수 있습니다. 그러나 기존 계정을 초대하는 경우 먼저 이메일 확인을 완료해야 합니다.

> **Note**
>
> 해당 계정에서 이전에 이메일 주소를 확인한 경우 계정을 사용하여 조직을 만들 때 다시 요청되지 않습니다.

AWS CLI & AWS SDKs

조직을 생성하려면

다음 명령 중 하나를 사용하여 조직을 생성할 수 있습니다.

- AWS CLI: create-organization

  다음 예제에서는 조직을 생성하고 현재 로그인된 AWS 계정을 조직의 관리 계정으로 만듭니다.

```
$ aws organizations create-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [  ...DEPRECATED - DO NOT USE ... ]
    }
}
```

> **Important**
>
> `AvailablePolicyTypes` 필드는 더 이상 사용되지 않으며 조직에서 활성화된 정책에 대한 정확한 정보를 담고 있지 않습니다. 조직에 대해 실제로 활성화된 정책 유형의 정확하고 완전한 목록을 보려면 다음 섹션의 AWS CLI 부분에 설명된 대로 `ListRoots` 명령을 사용합니다.

- AWS SDK: CreateOrganization

이제 다음과 같이 계정을 조직에 추가할 수 있습니다.

- 자동으로 AWS 조직에 속하는 AWS 계정을 만들려면 조직 내 멤버 계정 생성 단원을 참조하세요.
- 조직에 기존 계정을 초대하려면 조직에 AWS 계정 가입하도록 초대하기 단원을 참조하세요.

이메일 주소 확인

조직을 생성한 후 조직에 가입하도록 계정을 초대하려면 조직의 관리 계정에 대해 제공한 이메일 주소의 소유자임을 입증해야 합니다.

조직을 생성할 때 이전에 관리 계정이 확인되지 않은 경우 AWS는 지정된 이메일 주소로 확인 이메일을 자동으로 보냅니다. 확인 이메일을 받기까지 어느 정도 시간이 걸릴 수 있습니다.

24시간 내에 이메일의 지침을 따라 이메일 주소를 확인합니다.

24시간 내에 이메일 주소를 확인하지 않을 경우, 확인 요청을 다시 보내서 다른 AWS 계정을 조직에 초대할 수 있습니다. 확인 이메일을 받지 못한 경우 이메일 주소가 올바른지 확인하고, 필요한 경우 수정하세요.

- 관리 계정과 연결된 이메일 주소를 확인하려면 관리 계정에서 조직 세부 정보 보기 단원을 참조하세요.
- 관리 계정과 연결된 이메일 주소를 변경하려면 AWS Billing 사용 설명서의 AWS 계정 관리를 참조하세요.

AWS Management Console

확인 요청을 재전송하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 설정(Settings) 페이지로 이동한 다음 확인 요청 보내기(Send verification request)를 선택합니다. 이 옵션은 관리 계정이 확인되지 않은 경우에만 표시됩니다.
3. 24시간 내에 이메일 주소를 확인하세요.

   이메일 주소를 확인한 후 다른 AWS 계정을 초대하여 조직에 가입시킬 수 있습니다. 자세한 정보는 조직에 AWS 계정 가입하도록 초대하기 섹션을 참조하세요.

관리 계정의 이메일 주소를 변경할 경우 계정의 상태가 "확인되지 않은 이메일"로 돌아가고 새로운 이메일 주소에 대해 확인 프로세스를 완료해야 합니다.

> **Note**
>
> 관리 계정의 이메일 주소를 변경하기 전에 조직에 가입하도록 계정을 초대했는데 초대가 아직 수락되지 않은 경우 관리 계정의 새 이메일 주소를 확인할 때까지 초대를 수락할 수 없습니다. 이전 절차에 따라 확인 요청을 재전송합니다. 이메일에 응답하여 프로세스를 완료하면 초대된 계정에서 초대를 수락할 수 있습니다.

조직 내 모든 기능 활성화

AWS Organizations에는 두 가지 기능 집합이 있습니다.

- 모든 기능 – 이 기능 집합은 AWS Organizations에서 작업하기 위한 기본 방식이며 통합 결제 기능을 포함하고 있습니다. 조직을 생성할 때 모든 기능 활성화가 기본값입니다. 모든 기능을 활성화하면 지원되는 AWS 서비스 및 조직 관리 정책과의 통합과 같이 AWS Organizations에서 제공하는 고급 계정 관리 기능을 사용할 수 있습니다.
- 통합 결제 기능 – 모든 조직은 조직 내 계정을 중앙에서 관리하는 기본 관리 도구를 제공하는 이 기능 하위 집합을 지원합니다.

조직을 생성할 때 통합 결제 기능만 활성화하더라도 나중에 모든 기능을 활성화할 수 있습니다. 이 페이지에서는 모든 기능 활성화 절차를 설명합니다.

모든 기능을 활성화하기 전에

통합 결제 기능만 지원하는 조직에서 모든 기능을 지원하는 조직으로 전환하기 전에 다음 사항에 유의해야 합니다.

- 모든 기능을 활성화하는 과정을 시작하면, AWS Organizations는 사용자가 조직에 초대한 모든 멤버 계정에 요청을 전송합니다. 초대받은 모든 계정은 요청을 수락해 모든 기능 활성화를 승인해야 합니다. 승인을 받아야 조직 내 모든 기능을 활성화하는 과정을 완료할 수 있습니다. 계정이 요청을 거부하는 경우 조직에서 계정을 제거하거나 요청을 다시 보내야 합니다. 모든 기능을 활성화하는 프로세스를 완료하려면 먼저 요청을 수락해야 합니다. 으로 생성한AWS Organizations 계정은 추가 제어 승인이 필요 없기 때문에 요청을 받지 않습니다.

- 모든 기능을 활성화하는 동안 계속해서 조직에 계정을 초대할 수 있습니다. 초대된 계정의 소유자는 초대를 통해 통합 결제만 있는 조직에 가입하는지, 아니면 모든 기능이 활성화된 조직에 가입하는지를 알 수 있습니다.
  - 모든 기능을 활성화하는 프로세스 중에 계정을 초대하는 경우 가입하려는 조직에 모든 기능이 활성화되어 있다는 내용이 초대에 표시됩니다. 해당 계정이 초대를 수락하기 전에 모든 기능을 활성화하는 프로세스를 취소하면 해당 초대가 취소됩니다. 통합 결제 기능만 있는 조직의 멤버가 되게 하려면 계정을 다시 초대해야 합니다.
  - 계정을 초대했는데 모든 기능을 활성화하기 위한 프로세스를 시작하기 전에 초대가 아직 수락되지 않은 경우 초대가 취소됩니다. 조직에 통합 결제 기능만 있다고 초대에 명시되어 있기 때문입니다. 모든 기능을 활성화한 조직의 멤버가 되게 하려면 계정을 다시 초대해야 합니다.
- 조직에 계정을 계속 만들 수도 있습니다. 이 프로세스는 해당 변경의 영향을 받지 않습니다.
- AWS Organizations는 또한 모든 멤버 계정에 서비스 연결 역할(`AWSServiceRoleForOrganizations`)이 있는지 확인합니다. 이 역할은 모든 계정에서 모든 기능을 활성화하는 데 필수적입니다. 초대된 계정의 역할을 삭제했다면 모든 기능을 활성화하는 초대를 수락하여 역할을 다시 생성합니다. AWS Organizations를 사용하여 생성된 계정을 삭제하면 계정은 특별히 그 역할을 다시 생성하라는 초대를 수신합니다. 조직이 모든 기능을 활성화하는 절차를 완료하려면 이러한 모든 초대가 수락되어야 합니다.
- 모든 기능을 활성화하면 SCP를 사용할 수 있게 되므로, 계정 관리자가 조직, 조직 단위 또는 계정에 SCP를 연결하는 효과를 이해해야 합니다. SCP는 영향받는 계정에서 사용자와 심지어는 관리자가 할 수 있는 일을 제한할 수 있습니다. 예를 들어 관리 계정은 멤버 계정이 조직에서 나가지 못하게 하는 SCP를 적용할 수 있습니다.
- 관리 계정은 어떤 SCP의 영향도 받지 않습니다. 관리 계정의 사용자와 역할이 SCP를 적용해 할 수 있는 일은 제한할 수 없습니다. SCP는 멤버 계정에만 영향을 줍니다.
- 통합 결제 기능에서 모든 기능으로 마이그레이션하는 것은 단방향 작업입니다. 조직을 모든 기능 활성화에서 통합 결제 기능 전용으로 다시 바꿀 수는 없습니다.
- (권장하지 않음) 조직에서 통합 결제 기능만 활성화된 경우 멤버 계정 관리자는 서비스 연결 역할(`AWSServiceRoleForOrganizations`)을 삭제하도록 선택할 수 있습니다. 나중에 조직 내에서 모든 기능을 활성화도록 선택하면 이 역할은 필수이며, 모든 계정 내에서 모든 기능을 활성화하는 초대를 수락하는 과정의 일부로 다시 생성됩니다. AWS Organizations가 이 역할을 사용하는 방법에 대한 자세한 내용은 AWS Organizations 및 서비스 연결 역할을 참조하세요.

모든 기능 활성화 과정 시작

조직의 관리 계정에 로그인하면, 모든 기능을 활성화하는 프로세스를 시작할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

> **최소 권한**
>
> 조직 내 모든 기능을 활성화하려면 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

초대한 멤버 계정에 조직 내 모든 기능 활성화에 동의하도록 요청

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 설정 탭에서 모든 기능을 활성화하는 프로세스 시작을 선택합니다.
3. 모든 기능 활성화 페이지에서 모든 기능을 활성화하는 프로세스 시작을 선택하여 전환한 후에는 통합 결제 기능만으로는 돌아갈 수 없다는 점을 양해해 주시기 바랍니다.

   AWS Organizations는 조직 내 (생성된 계정이 아닌) 초대받은 모든 계정에 조직 내 모든 기능 활성화에 동의해 줄 것을 요청합니다. AWS Organizations를 사용하여 생성된 계정이 있고, 멤버 계정 관리자가 서비스 연결 역할(`AWSServiceRoleForOrganizations`)을 삭제한 경우 AWS Organizations는 계정에 이 역할을 다시 생성하라는 요청을 전송합니다.

   콘솔에 초대된 계정의 요청 승인 상태(Request approval status) 목록이 표시됩니다.

   > **Tip**
   >
   > 나중에 이 페이지로 돌아가려면 설정(Settings) 페이지를 열고 요청 전송 날짜(Request sent date) 섹션에서 상태 보기(View status)를 선택합니다.

4. 모든 기능 활성화(Enable all features) 페이지에 조직의 각 계정에 대한 현재 요청 상태가 표시됩니다. 요청에 동의한 계정에는 수락함(ACCEPTED) 상태가 표시됩니다. 아직 동의하지 않은 계정에는 미결(OPEN) 상태가 표시됩니다.

AWS CLI & AWS SDKs

초대한 멤버 계정에 조직 내 모든 기능 활성화에 동의하도록 요청

다음 명령 중 하나를 사용하여 조직의 모든 기능을 활성화할 수 있습니다.

- AWS CLI: enable-all-features

  다음 명령은 조직의 모든 기능을 활성화하는 프로세스를 시작합니다.

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

  출력 결과에는 초대된 멤버 계정이 동의해야 하는 핸드셰이크의 세부 정보가 나타납니다.

- AWS SDK: EnableAllFeatures

> **주의**
>
> - 요청이 멤버 계정에 전송되면 90일 카운트다운이 시작됩니다. 모든 계정은 해당 기간 내에 요청을 승인해야 하며, 승인하지 않으면 요청은 만료됩니다. 요청이 만료되면 요청 시도와 관련된 모든 요청은 취소되며, 2단계부터 다시 시작해야 합니다.
> - 모든 기능을 활성화하도록 요청하면 기존의 수락되지 않은 계정 초대는 모두 취소됩니다.

- 모든 기능 마이그레이션 프로세스 중에도 새 계정 초대를 시작하고 새 계정을 생성할 수 있습니다.

조직의 초대된 모든 계정이 요청을 승인하면, 프로세스를 완료하고 모든 기능을 활성화할 수 있습니다. 또한 조직에 초대 받은 멤버 계정이 없다면 과정을 즉시 완료할 수 있습니다. 프로세스를 완료하려면 모든 기능 활성화 과정 완료 단원으로 진행합니다.

모든 기능을 활성화하거나 서비스 연결 역할을 다시 생성하는 요청 승인

조직의 초대 받은 멤버 계정 중 하나에 로그인하면, 관리 계정이 보낸 요청을 승인할 수 있습니다. 계정이 조직에 가입하도록 원래 초대된 경우 해당 초대는 모든 기능을 활성화하는 것이고, 필요한 경우 `AWSServiceRoleForOrganizations` 역할의 재생성 승인을 묵시적으로 포함합니다. 대신 AWS Organizations를 사용하여 계정이 생성되고 `AWSServiceRoleForOrganizations` 서비스 연결 역할을 삭제한 경우 역할을 다시 생성하라는 초대만 수신합니다. 이렇게 하려면 다음 단계를 완료하세요.

Important

모든 기능을 활성화하면 조직의 관리 계정은 멤버 계정에 정책 기반 제어를 적용할 수 있습니다. 이러한 제어를 통해 사용자와 관리자가 계정에서 수행할 수 있는 작업을 제한할 수 있습니다. 이러한 제한은 계정을 조직에서 나가지 못하게 할 수 있습니다.

최소 권한

멤버 계정에 대한 모든 기능 활성화 요청을 승인하려면, 다음과 같은 권한이 있어야 합니다.

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListHandshakesForAccount` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `iam:CreateServiceLinkedRole` - 멤버 계정에 `AWSServiceRoleForOrganizations` 역할을 다시 생성해야 하는 경우에만 필요합니다.

AWS Management Console

조직 내 모든 기능 활성화 요청을 수락하는 방법

1. AWS Organizations 콘솔에서 AWS Organizations 콘솔에 로그인합니다. 멤버 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 수임하거나, 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 조직 내 모든 기능 활성화에 대한 동의가 계정에 어떤 의미가 있는지 읽은 다음 [Accept]를 선택합니다. 조직 내 모든 계정이 요청을 수락하고 관리 계정 관리자가 과정을 완료하기 전까지는 페이지에 진행 과정이 미완수로 표시됩니다.

AWS CLI & AWS SDKs

조직 내 모든 기능 활성화 요청을 수락하는 방법

요청을 수락하려면 `"Action": "APPROVE_ALL_FEATURES"`로 핸드셰이크를 수락해야 합니다.

- AWS CLI:
  - accept-handshake
  - list-handshakes-for-account

  다음 예제에서는 계정에 사용할 수 있는 핸드셰이크를 표시하는 방법을 보여 줍니다. 출력의 네 번째 줄에 있는 `"Id"` 값은 다음 명령을 위해 필요한 값입니다.

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
                }
            ],
```

```
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
}
```

다음 예제에서는 이전 명령의 핸드셰이크 ID를 사용하여 해당 핸드셰이크를 수락합니다.

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
```

```
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
}
```

- AWS SDK:
  - list-handshakes-for-account
  - AcceptHandshake

모든 기능 활성화 과정 완료

모든 초대받은 멤버 계정이 모든 기능을 활성화하는 요청을 승인해야 합니다. 조직에 초대받은 멤버 계정이 존재하지 않는 경우, [Enable all features progress] 페이지에 프로세스를 완료할 수 있음을 알리는 녹색 배너가 표시됩니다.

> **최소 권한**
>
> 조직에 모든 기능을 활성화하는 과정을 완료하려면 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:AcceptHandshake`
> - `organizations:ListHandshakesForOrganization`
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

모든 기능 활성화 과정 완료

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 설정(Settings) 페이지에서, 초대된 모든 계정이 모든 기능을 활성화하는 요청을 수락한 경우 페이지 상단에 녹색 상자가 나타나 이를 알려줍니다. 녹색 상자에서 계속해서 완료(Go to finalize)를 선택합니다.
3. 모든 기능 활성화(Enable all features) 페이지에서 완료(Finalize)를 선택한 다음 완료(Finalize)를 다시 선택합니다.
4. 이제 조직에 모든 기능이 활성화되었습니다.

AWS CLI & AWS SDKs

모든 기능 활성화 과정 완료

과정을 완료하려면 `"Action": "ENABLE_ALL_FEATURES"`로 핸드셰이크를 수락해야 합니다.

- AWS CLI:
  - list-handshakes-for-organization
  - accept-handshake

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
```

```
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

다음 예제에서는 조직에 사용할 수 있는 핸드셰이크를 표시하는 방법을 보여 줍니다. 출력의 네 번째 줄에 있는 "Id" 값은 다음 명령을 위해 필요한 값입니다.

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- AWS SDK:
  - AcceptHandshake
  - AcceptHandshake

다음 단계:

- 사용하려는 정책 유형을 활성화합니다. 이제 조직의 계정을 관리하는 정책을 연결할 수 있습니다. 자세한 정보는 에서 정책 관리 AWS Organizations 섹션을 참조하세요.
- 지원되는 서비스와의 통합을 활성화합니다. 자세한 정보는 다른 AWS 서비스와 함께 AWS Organizations 사용 섹션을 참조하세요.

조직 세부 정보 보기

다음 작업을 수행하여 조직의 요소에 대한 세부 정보를 조회할 수 있습니다.

주제

- 관리 계정에서 조직 세부 정보 보기
- 루트 컨테이너 세부 정보 보기
- OU 세부 정보 보기
- 계정 세부 정보 보기
- 정책 세부 정보 보기

관리 계정에서 조직 세부 정보 보기

AWS Organizations 콘솔에서 조직의 관리 계정에 로그인하면 조직의 세부 정보를 확인할 수 있습니다.

> 최소 권한
>
> 조직에 대한 세부 정보를 보려면 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:DescribeOrganization`

AWS Management Console

조직에 대한 세부 정보를 보려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. 설정(Settings) 페이지로 이동합니다. 이 페이지에는 조직 ID, 조직의 관리 계정에 할당된 계정 이름 및 이메일 주소를 비롯해 조직에 대한 세부 정보가 표시됩니다.

AWS CLI & AWS SDKs

조직에 대한 세부 정보를 보려면

다음 명령 중 하나를 사용하여 조직의 세부 정보를 볼 수 있습니다.

- AWS CLI: describe-organization

  다음 예제에서는 이 명령의 출력에 포함되는 정보를 보여줍니다.

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

  > **Important**
  >
  > `AvailablePolicyTypes` 필드는 더 이상 사용되지 않으며 조직에서 활성화된 정책에 대한 정확한 정보를 담고 있지 않습니다. 조직에 대해 실제로 활성화된 정책 유형의 정확하고 완전한 목록을 보려면 다음 섹션의 AWS CLI 부분에 설명된 대로 `ListRoots` 명령을 사용합니다.

- AWS SDK: DescribeOrganization

루트 컨테이너 세부 정보 보기

AWS Organizations 콘솔에서 조직의 관리 계정에 로그인하면 루트 컨테이너의 세부 정보를 확인할 수 있습니다.

최소 권한

루트 세부 정보를 보려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization`(콘솔 전용)
- `organizations:ListRoots`

루트는 OU(조직 단위) 계층 구조에서 최상위 컨테이너이며 일반적으로 OU로서 동작합니다. 그러나 계층 구조의 최상위에 있는 컨테이너이기 때문에 루트를 변경하면 조직의 다른 모든 OU와 모든 AWS 계정에 영향을 미칩니다.

AWS Management Console

루트 세부 정보를 보려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지로 이동해 루트 OU(라디오 버튼이 아닌 이름)를 선택합니다.
3. 루트(Root) 세부 정보 페이지가 나타나고 루트의 세부 정보가 표시됩니다.

AWS CLI & AWS SDKs

루트 세부 정보를 보려면

다음 명령 중 하나를 사용하여 루트의 세부 정보를 볼 수 있습니다.

- AWS CLI: list-roots

다음 예제에서는 조직에서 현재 활성화된 정책 유형을 비롯해 루트의 세부 정보를 검색하는 방법을 보여줍니다.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
```

```
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- AWS SDK: ListRoots

OU 세부 정보 보기

AWS Organizations 콘솔에서 조직의 관리 계정에 로그인하면 조직의 OU 세부 정보를 확인할 수 있습니다.

> 최소 권한
>
> 조직 단위(OU)에 대한 세부 정보를 보려면 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:DescribeOrganizationalUnit`
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
> - `organizations:ListOrganizationsUnitsForParent` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
> - `organizations:ListRoots` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

OU 세부 정보를 보려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 검토하려는 OU의 이름(라디오 버튼 아님)을 선택합니다. 원하는 OU가 다른 OU의 하위 항목이라면 상위 OU 옆에 있는 삼각형 아이콘을 선택해 확장한 후 계층 구조의 다음 레벨에 있는 OU를 확인합니다. 원하는 OU를 찾을 때까지 반복합니다.

   조직 단위 세부 정보(Organizational unit details) 상자에 OU에 대한 정보가 나타납니다.

AWS CLI & AWS SDKs

OU 세부 정보를 보려면

다음 명령을 사용하여 OU의 세부 정보를 볼 수 있습니다.

- AWS CLI, AWS SDK:
  - list-roots
  - list-children
  - describe-organizational-unit

다음 예제에서는 AWS CLI를 사용해 OU에서 ID를 찾는 방법을 보여줍니다. 먼저 `list-roots` 명령으로 계층 구조를 트래버스한 다음 루트에서 `list-children`을 수행하고 원하는 대상을 찾을 때까지 각 하위 항목에 대해 반복적으로 수행하여 OU ID를 찾습니다.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

OU의 ID를 찾았다면, 다음 예제에서 OU에 대한 세부 정보를 검색하는 방법을 보여 줍니다.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
```

```
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- AWS SDK:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

계정 세부 정보 보기

AWS Organizations 콘솔에서 조직의 관리 계정에 로그인하면 계정의 세부 정보를 확인할 수 있습니다.

> 최소 권한
>
> AWS 계정에 대한 세부 정보를 보려면 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
> - `organizations:ListAccounts` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

AWS 계정 세부 정보를 보려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지로 이동해 검토하려는 계정의 이름(라디오 버튼 아님)을 선택합니다. 원하는 계정이 OU의 하위 계정인 경우 하위 계정을 확인하기 위해 OU


옆에 있는 삼각형 아이콘을 선택해 확장해야 할 수 있습니다. 계정을 찾을 때까지 반복합니다.

계정 세부 정보(Account details) 상자에 계정에 대한 정보가 표시됩니다.

AWS CLI & AWS SDKs

AWS 계정의 세부 정보를 보려면

다음 명령을 사용하여 계정의 세부 정보를 볼 수 있습니다.

- AWS CLI:
  - list-accounts – 조직 내 모든 계정의 세부 정보를 나열합니다.
  - describe-account – 지정한 계정의 세부 정보만 나열합니다.

  두 명령 모두 각 계정에 대해 동일한 세부 정보를 응답에 포함하여 반환합니다.

  다음 예제에서는 지정한 계정의 세부 정보를 검색하는 방법을 보여줍니다.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
}
```

- AWS SDK:
  - ListAccounts
  - DescribeAccount

정책 세부 정보 보기

AWS Organizations 콘솔에서 조직의 관리 계정에 로그인하면 정책의 세부 정보를 확인할 수 있습니다.

최소 권한

정책 세부 정보를 보려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribePolicy`
- `organizations:ListPolicies`

AWS Management Console

정책의 세부 정보를 보려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 다음 중 하나를 수행합니다.
   - 정책(Policies) 페이지로 이동한 다음 검토하려는 정책의 정책 유형을 선택합니다.
   - AWS 계정 페이지로 이동한 다음 정책이 연결된 OU 또는 계정으로 이동합니다. 마지막으로 정책(Policies) 탭을 선택하면 연결된 정책 목록이 표시됩니다.
3. 정책의 이름(라디오 버튼 아님)을 선택합니다.

   정책의 세부 정보 페이지에서는 JSON 정책 텍스트, 정책이 연결된 OU 및 계정 목록을 비롯하여 정책에 대한 모든 정보를 볼 수 있습니다.

AWS CLI & AWS SDKs

정책의 세부 정보를 보려면

다음 명령 중 하나를 사용하여 정책의 세부 정보를 볼 수 있습니다.

- AWS CLI:
  - list-policies
  - describe-policy – 지정한 정책의 세부 정보만 나열합니다.

다음 예제에서는 검토할 정책의 정책 ID를 찾는 방법을 보여줍니다. 명령을 통해 지정한 유형의 모든 정책만을 반환하려면 정책 유형을 지정해야 합니다.

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

응답에는 JSON 정책 문서를 제외한 모든 세부 정보가 포함됩니다.

다음 예제에서는 JSON 정책 문서를 포함하여 지정한 정책의 세부 정보만 검색하는 방법을 보여줍니다.

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":
[\"us-west-2\"]},\"rules\":{\"My-Backup-Rule\"
                    :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-
Backup-Vault\"}}},\"selections\":{\"tags\":{
                    \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
```

```
                    My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\"]}}}}}}"
    ]
}
```

- AWS SDK:
  - ListPolicies
  - DescribePolicy

조직 삭제

조직이 더 이상 필요 없다면, 삭제할 수 있습니다. 조직을 삭제해도 관리 계정이 해지되는 것은 아니며 조직에서 관리 계정이 제거되고 조직 자체가 삭제됩니다. 이전 관리 계정은 더 이상 AWS Organizations에서 관리하지 않는 독립형 AWS 계정 계정이 됩니다. 그런 다음 이 계정을 독립형 계정으로 계속 사용하거나, 다른 조직을 생성하는 데 사용하거나, 다른 조직의 초대를 수락하여 해당 조직에 이 계정을 멤버 계정으로 추가할 수 있습니다.

> **Important**
>
> - 삭제한 조직은 복구할 수 없습니다. 조직 내에 어떤 정책을 생성했든 간에 모든 계정이 삭제되며 복구할 수 없습니다.
> - 조직의 모든 멤버 계정을 제거한 후에만 조직을 삭제할 수 있습니다. AWS Organizations를 사용하여 만든 일부 계정은 제거하지 못할 수 있습니다. 독립형 AWS 계정으로 작동하는 데 필요한 모든 정보가 있는 경우에만 멤버 계정을 제거할 수 있습니다. 이러한 필수 정보를 제공한 후 계정을 삭제하는 자세한 방법은 멤버 계정에서 조직 탈퇴 단원을 참조하세요.
> - 조직에서 제거하기 전에 멤버 계정을 해지한 경우 일정 기간 동안 '일시 중지' 상태가 되며 최종적으로 해지될 때까지 조직에서 계정을 제거할 수 없습니다. 이 과정에는 최대 90일이 소요될 수 있으며 모든 멤버 계정이 완전히 해지될 때까지 조직을 삭제하지 못할 수 있습니다.

조직을 삭제하여 조직에서 관리 계정을 제거하면 해당 계정에 다음과 같은 방식으로 영향을 미칠 수 있습니다.

- 계정은 자체 요금만 지불할 책임이 있으며 더 이상 다른 계정에서 발생하는 요금에 대해서는 책임이 없습니다.

- 다른 서비스와의 통합이 비활성화될 수 있습니다. 예를 들어 AWS IAM Identity Center이 작동하려면 조직이 필요하기 때문에 IAM Identity Center를 지원하는 조직에서 계정을 제거할 경우 해당 계정의 사용자는 더 이상 해당 서비스를 이용할 수 없습니다.

조직의 관리 계정은 서비스 제어 정책(SCP)의 영향을 받지 않으므로, SCP를 더 이상 사용할 수 없게 되더라도 권한 변경은 없습니다.

주제

조직 삭제

조직을 삭제하여 이전 관리 계정을 더 이상 AWS Organizations에서 관리하지 않는 독립형 AWS 계정(으)로 되돌리려면 다음 절차를 따르십시오.

> 최소 권한
>
> 조직을 삭제하려면 관리 계정의 사용자 또는 역할로 로그인하고 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

조직 삭제

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 조직을 삭제하기 전에 먼저 조직의 모든 계정을 제거해야 합니다. 자세한 정보는 조직에서 멤버 계정 제거 섹션을 참조하세요.
3. 설정(Settings) 페이지로 이동한 다음 조직 삭제(Delete organization)를 선택합니다.
4. 조직 삭제(Delete organization) 확인 대화 상자에서 텍스트 상자 윗줄에 표시된 조직 ID를 입력합니다. 그런 다음 조직 삭제(Delete organization)를 선택합니다.

> **Important**
>
> 이 작업을 수행하여도 관리 계정이 해지되지는 않으며 대신 독립형 AWS 계정(으)로 돌아갑니다. 계정을 해지하려면 조직 내 멤버 계정 해지의 단계를 따르십시오.

AWS CLI & AWS SDKs

조직 삭제

다음 명령 중 하나를 사용하여 조직을 삭제합니다.

- AWS CLI: delete-organization

  다음 예제에서는 자격 증명이 사용된 AWS 계정이 관리 계정인 조직을 삭제합니다.

  ```
  $ aws organizations delete-organization
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS SDKs: DeleteOrganization

조직 내 AWS 계정 관리

조직이란 함께 관리할 수 있는 AWS 계정 모음입니다. 다음 작업을 실행하면 조직의 일부의 계정을 관리할 수 있습니다.

- 조직 내 계정의 세부 정보를 확인합니다. 계정의 고유 ID 번호, Amazon 리소스 이름(ARN) 및 관련 정책을 확인할 수 있습니다.
- 조직에서 모든 AWS 계정 목록을 내보냅니다. 조직 내 모든 계정에 대한 계정 세부 정보가 포함된 .csv 파일을 다운로드할 수 있습니다.
- 기존 AWS 계정을 조직에 초대합니다. 초대를 생성하고, 생성한 초대를 관리하고, 초대를 수락 또는 거부합니다.
- 조직의 일부로 AWS 계정을 생성합니다. 자동으로 조직의 일부가 되는 AWS 계정을 생성하고 액세스합니다.
- 조직의 대체 연락처를 업데이트합니다. 조직의 AWS 계정에 대한 대체 연락처를 업데이트합니다.
- 조직에서 AWS 계정을 제거합니다. 관리 계정의 관리자로서 조직에서 더 이상 관리할 필요가 없는 멤버 계정을 제거합니다. 멤버 계정의 관리자로서 조직에서 계정을 제거합니다. 관리 계정이 멤버 계정에 정책을 연결했다면, 계정 제거를 차단당할 수 있습니다.
- AWS 계정을 삭제(또는 해지)합니다. AWS 계정이 더 이상 필요 없는 경우 해당 계정을 해지하여 사용을 차단하거나 요금이 발생하지 않도록 할 수 있습니다.

조직에 속하는 데 따른 영향

- 조직에 합류하는 AWS 계정에 미치는 영향은 무엇입니까?
- 조직에서 생성하는 AWS 계정에 미치는 영향은 무엇입니까?

조직에 가입한 AWS 계정에 미치는 영향은?

AWS 계정에 조직 가입 초대를 하고 계정 소유자가 이 초대를 수락하면 AWS Organizations는 자동적으로 새 멤버 계정을 다음과 같이 변경합니다.

- AWS Organizations는 `AWSServiceRoleForOrganizations`라는 서비스 연결 역할을 생성합니다. 조직이 모든 기능을 지원하려면 계정에 이 역할이 있어야 합니다. 조직이 통합 결제 기능만 지원하는 경우에는 역할을 삭제할 수 있습니다. 해당 역할을 삭제하고 이후 조직의 모든 기능을 활성화한 경우 AWS Organizations에서 계정에 대한 역할을 다시 생성합니다.

- 조직 루트, 또는 계정이 속하는 OU에 연결된 다양한 정책이 있을 수 있습니다. 이 경우 이러한 정책은 초대된 계정의 모든 사용자 및 역할에 즉시 적용됩니다.
- 조직에 대해 다른 AWS 서비스에 대한 서비스 신뢰를 활성화할 수 있습니다. 이렇게 하면 신뢰할 수 있는 해당 서비스는 초대된 계정이 포함된 조직의 멤버 계정에서 서비스 연결 역할을 생성하거나 작업을 수행할 수 있습니다.

> **Note**
>
> 초대된 멤버 계정의 경우 IAM 역할을 OrganizationAccountAccessRole자동으로 생성하지 AWS Organizations 않습니다. 이 역할은 관리 계정의 사용자에게 멤버 계정에 대한 관리 액세스 권한을 부여합니다. 초대된 계정에 대해 관리 제어 수준을 활성화하려면 직접 역할을 추가할 수 있습니다. 자세한 정보는 초대된 멤버 OrganizationAccountAccessRole 계정에서 생성 섹션을 참조하세요.

통합 결제 기능만 활성화된 조직에 가입하도록 계정을 초대할 수 있습니다. 나중에 조직의 모든 기능을 활성화하려면 초대된 계정이 변경 사항을 승인해야 합니다.

조직에서 생성한 AWS 계정에 미치는 영향은?

조직에서 AWS 계정을 생성할 때 AWS Organizations는 자동적으로 새 멤버 계정을 다음과 같이 변경합니다.

- AWS Organizations는 `AWSServiceRoleForOrganizations`라는 서비스 연결 역할을 생성합니다. 조직이 모든 기능을 지원하려면 계정에 이 역할이 있어야 합니다. 조직이 통합 결제 기능만 지원하는 경우에는 역할을 삭제할 수 있습니다. 해당 역할을 삭제하고 이후 조직의 모든 기능을 활성화한 경우 AWS Organizations에서 계정에 대한 역할을 다시 생성합니다.
- AWS OrganizationsIAM 역할을 생성합니다. OrganizationAccountAccessRole 이 역할은 관리 계정에게 새 멤버 계정에 대한 액세스 권한을 부여합니다. 이 역할은 삭제할 수 있지만 복구 옵션으로 사용할 수 있도록 삭제하지 않는 것이 좋습니다.
- OU 트리의 루트에 연결된 정책이 있는 경우에는 생성된 계정의 모든 사용자 및 역할에 이러한 정책이 즉시 적용됩니다. 기본적으로 새 계정은 루트 OU에 추가됩니다.
- 조직의 또 다른 AWS 서비스를 위한 서비스 신뢰 관계를 활성화한 경우에는 신뢰 관계가 생성된 서비스가 서비스 연결 역할을 생성하거나 생성된 계정을 포함하여 조직의 어떤 멤버 계정으로든 작업을 수행할 수 있습니다.

조직에 AWS 계정 가입하도록 초대하기

조직을 만들고 관리 계정과 연결된 이메일 주소를 소유하고 있는지 확인한 후 기존 AWS 계정 조직을 조직에 초대할 수 있습니다.

계정을 초대하면 계정 소유자에게 초대를 AWS Organizations 보내면 계정 소유자가 초대를 수락할지 거절할지 결정합니다. AWS Organizations 콘솔을 사용하여 다른 계정에 보내는 초대를 시작하고 관리할 수 있습니다. 다른 계정에 초대를 보내는 일은 조직의 관리 계정에서만 할 수 있습니다.

> **Note**
>
> 모든 계정에 대한 청구 내역 및 보고서는 조직의 지급인 계정에 유지됩니다. 계정을 새 조직으로 이동하기 전에 유지하려는 멤버 계정에 대한 청구 및 보고서 내역을 다운로드하십시오. 여기에는 비용 및 사용 보고서, 세부 결제 보고서 또는 Cost Explorer 서비스에서 생성된 보고서가 포함될 수 있습니다.

관리자인 경우 조직의 초대를 수락하거나 거절할 수도 있습니다. AWS 계정수락한 경우 사용자의 계정은 조직의 멤버가 됩니다. 사용자의 계정은 조직에 가입할 수 있습니다. 따라서 여러 개의 가입 초대를 수신한 경우 하나만 수락할 수 있습니다.

계정이 조직 가입 초대를 수락하는 순간 조직의 관리 계정은 새 멤버 계정에서 발생한 모든 요금을 부담하게 됩니다. 멤버 계정에 연결된 결제 방법이 더 이상 사용되지 않습니다. 대신 조직의 관리 계정에 연결된 결제 방법이 멤버 계정에서 발생한 모든 요금을 지불합니다.

초대된 계정이 조직에 가입하고 조직이 모든 기능 모드에 있는 경우 관리 계정은 초대된 구성원 계정에 대한 전체 관리 액세스 권한 및 제어 권한을 가집니다. 하지만 생성된 계정과 달리 `OrganizationAccountAccessRole` IAM 역할은 관리 계정이 수임할 권한이 있는 구성원 계정에 자동으로 생성되지 않습니다. 초대된 계정이 구성원이 된 후에 계정을 생성하고 구성하려면 다음 단계를 초대된 멤버 OrganizationAccountAccessRole 계정에서 생성 따르세요.

> **Note**
>
> 기존 계정을 가입하도록 초대하는 대신 조직에 계정을 생성하면 관리 계정 관리자의 사용자에게 `OrganizationAccountAccessRole` 생성된 계정에 대한 액세스 권한을 부여하는 데 사용할 수 있는 IAM 역할 (기본 이름) 이 AWS Organizations 자동으로 생성됩니다.

AWS Organizations 초대된 구성원 계정에 서비스 연결 역할을 자동으로 생성하여 다른 서비스 간의 AWS Organizations 통합을 지원합니다. AWS 자세한 정보는 AWS Organizations 및 서비스 연결 역할을 참조하세요.

하루에 보낼 수 있는 초대장 수는 최대 및 최소 값 단원을 참조하세요. 수락된 초대는 이 할당량에 포함되지 않습니다. 하나의 초대가 수락되는 즉시 다른 초대를 같은 날에 전송할 수 있습니다. 각 초대는 15일 이내에 응답받아야 하며 응답이 없으면 만료됩니다.

계정으로 전송된 초대는 조직의 계정 할당량을 기준으로 계산됩니다. 초대된 계정에서 초대를 거부하면 해당 카운트가 복원되고 관리 계정이 초대를 취소하거나 초대가 만료됩니다.

자동으로 조직의 일부가 되는 계정을 생성하는 방법은 조직 내 멤버 계정 생성을(를) 참조하세요.

Important

청구상의 제약으로 인해 동일한 AWS 판매자 (AWS 인도의 경우) AWS 계정 에게만 초대하고 관리 계정으로 AWS 분할할 수 있습니다.

- Amazon Web Services India Private Limited (이하 “AWS India”) (이전 명칭: Amazon Internet Services Private Limited) 에서 조직의 관리 계정을 생성한 경우, 조직의 모든 계정은 관리 계정과 동일한 레코드 셀러 계정이어야 합니다. 예를 들어 인도의 AWS 판매자는 다른 AWS 인도 계정만 조직에 초대할 수 있습니다. AWS 인도 계정이나 다른 AWS 셀러의 계정은 통합할 수 없습니다.
- 조직의 모든 계정은 관리 계정과 동일한 AWS 파티션에 속해야 합니다. 상업용 AWS 리전 파티션의 계정은 중국 지역 파티션의 계정이나 지역 파티션의 계정을 보유한 조직에 속할 수 없습니다. AWS GovCloud (US)

AWS 계정에 초대 보내기

계정을 조직에 초대하려면 먼저 관리 계정과 연결된 이메일 주소의 소유자임을 입증해야 합니다. 자세한 정보는 이메일 주소 확인 섹션을 참조하세요. 이메일 주소를 확인한 후 다음 단계에 따라 계정을 조직에 초대합니다.

최소 권한

조직에 AWS 계정 가입하도록 초대하려면 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization`(콘솔 전용)

- `organizations:InviteAccountToOrganization`

AWS Management Console

다른 계정을 조직에 초대하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 로 AWS이미 이메일 주소를 확인했다면 이 단계를 건너뛰세요.

   이메일 주소를 아직 확인하지 않은 경우 조직 생성 후 24시간 내에 확인 이메일의 지침을 따릅니다. 확인 이메일 메시지를 받기까지 어느 정도 시간이 걸릴 수 있습니다. 이메일 주소를 확인할 때까지 다른 계정을 초대하여 조직에 가입시킬 수 없습니다.
3. AWS 계정 페이지로 이동하고 AWS 계정 추가를 선택합니다.
4. AWS 계정계정 추가 페이지에서 기존 AWS 계정 초대를 선택합니다.
5. 기존 초대 AWS페이지에서 초대할 이메일 주소 또는 계정 AWS 계정 ID에 초대할 계정과 연결된 이메일 주소 또는 계정 ID 번호를 입력합니다.
6. (선택 사항) 초대 이메일 메시지에 포함할 메시지(Message to include in the invitation email message)에서, 초대된 계정 소유자에게 보내는 이메일 초대장에 넣을 텍스트를 입력합니다.
7. (선택 사항) 태그 추가(Add tags) 섹션에서, 관리자가 초대를 수락한 후 계정에 자동으로 적용되는 태그를 하나 이상 지정합니다. 이렇게 하려면 태그 추가(Add tag)를 선택한 다음 키 및 값(선택 사항)을 입력합니다. 값을 공백으로 남겨두면 `null`이 아닌 빈 문자열로 설정됩니다. AWS 계정에는 최대 50개의 태그를 연결할 수 있습니다.
8. [Send invitation]을 선택합니다.

   > **Important**
   >
   > 조직의 계정 할당량을 초과했거나 조직이 초기화 중이므로 계정을 추가할 수 없다는 메시지를 받은 경우 AWS Support에 문의하세요.

9. 초대(Invitations) 페이지로 리디렉션되면, 이 페이지에서 미결 및 수락 상태의 모든 초대를 확인할 수 있습니다. 방금 생성한 초대가 목록 상단에 표시되며 상태는 OPEN으로 설정됩니다.

   AWS Organizations 조직에 초대한 계정 소유자의 이메일 주소로 초대장을 보냅니다. 이 이메일 메시지에는 계정 소유자가 세부 정보를 보고 초대를 수락할지 거절할지 선택할 수 있는

AWS Organizations 콘솔 링크가 포함되어 있습니다. 또는 초대된 계정의 소유자가 이메일 메시지를 건너뛰고 AWS Organizations 콘솔로 직접 이동하여 초대를 확인하고 초대를 수락하거나 거절할 수도 있습니다.

이 계정에 대한 초대는 조직에 있을 수 있는 최대 계정 수를 기준으로 즉시 계산됩니다. AWS Organizations 에서는 계정이 초대를 수락할 때까지 기다리지 않습니다. 초대된 계정이 거부한 경우 관리 계정은 초대를 취소합니다. 초대된 계정이 지정된 시간 내에 응답하지 않은 경우 초대는 만료됩니다. 어느 경우든 초대는 더 이상 할당량에 포함되지 않습니다.

AWS CLI & AWS SDKs

다른 계정을 조직에 초대하려면

다음 명령 중 하나를 사용하여 다른 계정이 조직에 가입하도록 초대할 수 있습니다.

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
```

```
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```

- AWS SDK: InviteAccountToOrganization

조직에 대해 보류 중인 초대 관리

관리 계정에 로그인하면 조직의 연결된 AWS 계정 을 모두 확인하고 보류 중인(미결) 초대를 취소할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

최소 권한

조직에 대해 보류 중인 초대를 관리하려면, 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListHandshakesForOrganization`
- `organizations:CancelHandshake`

AWS Management Console

조직이 다른 계정에 보낸 초대를 확인하거나 취소하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 초대(Invitations) 페이지로 이동합니다.

   이 페이지에 조직이 전송한 모든 초대와 초대의 현재 상태가 표시됩니다.

   > **Note**
   >
   > 수락, 취소 및 거부된 초대는 30일 동안 계속해서 목록에 나타납니다. 그 후에는 삭제되어 목록에 더 이상 표시되지 않습니다.

3. 취소하려는 초대 옆에 있는 라디오 버튼  을 선택한 다음 초대 취소(Cancel invitation)를 선택합니다. 라디오 버튼이 회색으로 표시되어 있으면 초대를 취소할 수 없습니다.

   초대 상태가 미결(OPEN)에서 취소됨(CANCELED)으로 변경됩니다.

   AWS 초대를 취소했음을 알리는 이메일 메시지를 계정 소유자에게 보냅니다. 새 초대를 보내지 않는 한 해당 계정은 조직에 가입할 수 없게 됩니다.

AWS CLI & AWS SDKs

조직이 다른 계정에 보낸 초대를 확인하거나 취소하려면

다음 명령을 사용하여 초대를 보거나 취소할 수 있습니다.

- AWS CLI: list-handshakes-for-organization, 취소-핸드셰이크
- 다음 예는 해당 조직이 다른 계정으로 보낸 초대를 보여 줍니다.

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
```

```
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
```

```
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
```

```
            ]
        }
    ]
}
```

다음 예는 계정에 대한 초대를 취소하는 방법을 보여 줍니다.

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
```

```
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS SDK:, ListHandshakesForOrganizationCancelHandshake

조직에서 보낸 초대 수락 또는 거부

조직에 가입하라는 초대를 받을 AWS 계정 수 있습니다. 여러분은 초대를 수락하거나 거부할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

> **Note**
>
> 조직을 포함한 계정의 상태는 어떤 비용 및 사용량 데이터가 표시되는지에 영향을 줍니다.
>
> - 멤버 계정이 조직을 탈퇴하여 독립형 계정이 되는 경우 해당 계정은 조직의 멤버였을 때의 시간 범위로부터 비용 및 사용량 데이터에 대한 액세스를 할 수 없습니다. 해당 계정은 독립형 계정으로 생성된 데이터에만 액세스할 수 있습니다.
> - 멤버 계정이 조직 A를 탈퇴하여 조직 B에 가입하는 경우 계정은 조직 A의 계정이었을 때의 시간 범위로부터 비용 및 사용량에 대한 데이터에 액세스할 수 없습니다. 해당 계정은 조직 B의 멤버로 생성된 데이터에만 액세스할 수 있습니다.
> - 계정이 이전에 속했던 조직에 다시 가입하는 경우 계정은 과거 비용 및 사용량 데이터에 대한 액세스를 다시 얻습니다.

> **Note**
>
> 멤버 계정과 독립형 계정에서만 조직 가입 초대를 수락하거나 거절할 수 있습니다. 초대가 구성원 계정으로 전송된 경우 초대를 수락하기 전에 해당 계정이 현재 조직에서 탈퇴해야 합니다. 이미 AWS 조직에 속한 관리 계정으로 초대를 받은 경우 조직에서 모든 멤버 계정을 제거하고 조직을 삭제하기 전까지는 해당 계정에서 초대를 수락할 수 없습니다.

> **최소 권한**
>
> AWS 조직 가입 초대를 수락하거나 거부하려면 다음 권한이 있어야 합니다.
>
> - `organizations:ListHandshakesForAccount`— 콘솔에서 초대 목록을 보는 데 필요합니다. AWS Organizations
> - `organizations:AcceptHandshake`.
> - `organizations:DeclineHandshake`.
> - `iam:CreateServiceLinkedRole`— 초대를 수락하려면 다른 서비스와의 통합을 지원하기 위해 구성원 계정에 서비스 연결 역할을 생성해야 하는 경우에만 필요합니다. AWS 자세한 정보는 AWS Organizations 및 서비스 연결 역할을 참조하세요.

AWS Management Console

초대를 수락하거나 거부하려면

1. 조직 가입 초대는 계정 소유자의 이메일 주소로 전송됩니다. 초대 이메일 메시지를 받은 계정 소유자는 이메일 초대장의 지침을 따르거나, 브라우저에서 AWS Organizations 콘솔로 이동한 후 초대(Invitations)를 선택하거나, 멤버 계정의 초대(member account's Invitation)로 곧바로 이동할 수 있습니다.
2. 메시지가 표시되면 초대된 계정에 IAM 사용자로 로그인하거나, IAM 역할을 맡거나, 계정의 루트 사용자로 로그인(권장되지 않음)합니다.
3. 멤버 계정의 초대(member account's Invitation) 페이지에 계정의 미결 조직 가입 초대가 표시됩니다.

   초대 수락(Accept invitation) 또는 초대 거부(Decline invitation)를 적절히 선택합니다.

- 앞선 단계에서 초대 수락(Accept invitation)을 선택한 경우 내 계정이 멤버가 된 조직의 세부 정보를 보여주는 조직 보기(Organization overview) 페이지가 콘솔에 나타납니다. 조직의 ID와 소유자의 이메일 주소를 확인할 수 있습니다.

  > **Note**
  >
  > 수락된 초대는 30일 동안 계속해서 목록에 나타납니다. 그 후에는 삭제되어 목록에 더 이상 표시되지 않습니다.

  AWS Organizations 새 구성원 계정에 서비스 연결 역할을 자동으로 생성하여 다른 서비스 간의 AWS Organizations 통합을 지원합니다. AWS 자세한 정보는 AWS Organizations 및 서비스 연결 역할을 참조하세요.

  AWS 초대를 수락했다는 내용의 이메일 메시지를 조직의 관리 계정 소유자에게 보냅니다. 또한 멤버 계정 소유자에게는 계정이 조직의 멤버가 되었음을 알리는 이메일 메시지가 전송됩니다.
- 이전 단계에서 거부(Decline)를 선택했다면, 계정은 다른 보류 중인 초대를 표시하는 멤버 계정의 초대 페이지에 계속 표시됩니다.

  AWS 초대를 거부했음을 알리는 이메일 메시지를 조직의 관리 계정 소유자에게 보냅니다.

  > **Note**
  >
  > 거부된 초대는 30일 동안 목록에 계속 나타납니다. 그 후에는 삭제되어 목록에 더 이상 표시되지 않습니다.

AWS CLI & AWS SDKs

초대를 수락하거나 거부하려면

다음 명령을 사용하여 초대를 수락하거나 거부할 수 있습니다.

- AWS CLI: accept-handshake, decline-handshake

  다음 예는 조직 가입 초대를 수락하는 방법을 보여 줍니다.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
```

```
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
```

```
}
```

다음 예는 조직 가입 초대를 거부하는 방법을 보여 줍니다.

- AWS SDK:, AcceptHandshakeDeclineHandshake

조직 내 멤버 계정 생성

이 페이지에서는 AWS Organizations에서 조직 내 AWS 계정을 생성하는 방법을 설명합니다. AWS를 시작하고 단일 AWS 계정을 생성하는 방법에 대해 자세히 알아보려면 리소스 센터 시작하기를 참조하세요.

조직이란 중앙에서 관리하는 AWS 계정 모음입니다. 다음 절차를 실행하면 조직의 일부의 계정을 관리할 수 있습니다.

- 조직의 일부인 AWS 계정 생성
- 관리 계정 액세스 역할이 있는 멤버 계정 액세스

Important

- 조직 내 멤버 계정을 생성할 때 AWS Organizations는 멤버 계정 내에 AWS Identity and Access Management(IAM) 역할 `OrganizationAccountAccessRole`을 자동적으로 생성하여 관리 계정 내 사용자 및 역할이 멤버 계정에 대한 전체 관리 제어를 사용할 수 있도록 합니다. 이 역할에는 멤버 계정에 적용되는 모든 서비스 제어 정책(SCP)이 적용됩니다.

  AWS Organizations는 또한 `OrganizationAccountAccessRole` 역할을 포함한 관리형 정책을 멤버 계정에 추가합니다. 이를 통해 중앙 집중식 제어가 가능하므로 정책이 업데이트될 때마다 동일한 관리형 정책에 연결된 추가 계정이 자동으로 업데이트됩니다. 이전에는 조직 내에서 생성된 새 계정에 해당 단일 계정에만 적용되는 인라인 정책이 추가되었습니다. 인라인 및 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서에서 관리형 정책과 인라인 정책을 참조하세요.

  AWS Organizations는 또한 일부 AWS 서비스와의 통합을 활성화하는 `AWSServiceRoleForOrganizations`라는 서비스 연결 역할을 자동적으로 생성합니다. 다른 서비스가 통합을 허용하도록 구성해야 합니다. 자세한 정보는 AWS Organizations 및 서비스 연결 역할 섹션을 참조하세요.

- 이 조직이 AWS Control Tower로 관리되는 경우 AWS Control Tower 콘솔 또는 API에서 AWS Control Tower Account Factory를 사용하여 계정을 만듭니다. Organizations에서 계정을 만들 경우 해당 계정이 AWS Control Tower에 등록되지 않습니다. 자세한 내용은 AWS Control Tower 사용 설명서의 AWS Control Tower 외부 리소스 참조를 참조하세요.

> **Note**
>
> 조직의 일부로 생성한 AWS 계정은 AWS 마케팅 이메일을 자동으로 구독하지 않습니다. 마케팅 이메일을 수신하도록 계정을 옵트인하려면 https://pages.awscloud.com/communication-preferences을(를) 참조하세요.

조직의 일부인 AWS 계정 생성

조직의 관리 계정에 로그인하면 자동으로 조직의 일부가 되는 멤버 계정을 생성할 수 있습니다. 다음 절차를 사용하여 계정을 생성하면 AWS Organizations은(는) 다음 기본 연락처 정보를 관리 계정에서 새 멤버 계정으로 자동으로 복사합니다.

- 전화번호
- 회사 이름
- 웹사이트 URL
- Address

또한 관리 계정의 커뮤니케이션 언어 및 Marketplace 정보(일부 AWS 리전의 계정 공급업체)를 복사합니다.

> **Note**
>
> AWS은(는) 멤버 계정이 독립 실행형 계정으로 운영되는 데 필요한 모든 정보를 자동으로 수집하지 않습니다. 조직에서 멤버 계정을 제거해 해당 계정을 독립형 계정으로 만들어야 하는 경우 제거하기 전에 먼저 계정에 대해 필요한 정보를 제공해야 합니다. 자세한 내용은 멤버 계정에서 조직 탈퇴 섹션을 참조하세요.

최소 권한

조직의 멤버 계정을 만들려면 다음과 같은 권한이 있어야 합니다.

- `organizations:CreateAccount`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `iam:CreateServiceLinkedRole`(멤버 계정에서 필수 서비스 연결 역할을 생성할 수 있도록 보안 주체 `organizations.amazonaws.com`에 부여)

AWS Management Console

자동으로 조직의 일부가 되는 AWS 계정을 생성하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 AWS 계정 추가를 선택합니다.
3. AWS 계정 추가 페이지에서 AWS 계정 생성을 선택합니다(기본으로 선택되어 있음).
4. AWS 계정 생성 페이지의 AWS 계정 이름에서 계정에 할당할 이름을 입력합니다. 이 이름은 계정을 조직 내 다른 모든 계정과 구분하는 데 도움이 되며, 소유자의 IAM 별칭이나 이메일 이름과는 다릅니다.
5. 계정 소유자의 이메일 주소(Email address of the account's owner)에 계정 소유자의 이메일 주소를 입력합니다. 이 이메일 주소는 계정의 루트 사용자에 대한 사용자 이름 자격 증명이 되기 때문에 다른 AWS 계정과 이미 연결되어 있으면 안 됩니다.
6. (선택 사항) 새 계정에서 자동으로 생성되는 IAM 역할에 할당할 이름을 지정합니다. 이 역할은 새로 만든 멤버 계정에 액세스할 수 있는 권한을 조직의 관리 계정에 부여합니다. 이름을 지정하지 않으면 AWS Organizations가 기본 이름 `OrganizationAccountAccessRole`을 적용합니다. 일관성을 위해 모든 계정에 기본 이름을 사용하는 것이 좋습니다.

Important

이 역할 이름을 기억해 두세요. 나중에 관리 계정을 이용하는 사용자 및 역할에게 새 계정에 대한 액세스 권한을 부여할 때 필요합니다.

7. (선택 사항) 태그 섹션에서 태그 추가를 선택하고 키 및 값(선택 사항)을 입력하여 새 계정에 하나 이상의 태그를 추가합니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 계정에는 최대 50개의 태그를 연결할 수 있습니다.
8. AWS 계정 생성(Create)을 선택합니다.

   - 조직의 계정 할당량을 초과했음을 나타내는 오류가 발생하면 조직에 계정을 추가하려고 하면 "할당량 초과" 메시지가 표시됩니다. 단원을 참조하세요.
   - 조직이 아직 초기화되고 있기 때문에 계정을 추가할 수 없음을 나타내는 오류가 발생하면 한 시간 동안 기다렸다가 다시 시도하세요.
   - AWS CloudTrail 로그에서 계정 생성이 성공했는지 여부에 대한 정보를 확인할 수도 있습니다. 자세한 정보는 AWS Organizations의 로깅 및 모니터링 섹션을 참조하세요.
   - 오류가 지속될 경우 AWS Support에 문의하세요.

   AWS 계정 페이지가 나타나고 새 계정이 목록에 추가됩니다.
9. 이제 계정이 존재하고 관리 계정에서 사용자에게 관리자 액세스 권한을 부여하는 IAM 역할을 갖게 되었으므로 조직 내 멤버 계정에 액세스의 단계에 따라 계정에 액세스할 수 있습니다.

> **Note**
>
> 사용자가 계정을 생성하면 AWS Organizations는 처음에 임의로 생성된 길고(64자) 복잡한 암호를 루트 사용자에게 할당합니다. 이 초기 암호는 검색할 수 없습니다. 루트 사용자로 계정에 최초 액세스할 때는 암호 복구 작업을 거쳐야 합니다. 자세한 정보는 루트 사용자로 멤버 계정에 액세스 섹션을 참조하세요.

AWS CLI & AWS SDKs

자동으로 조직의 일부가 되는 AWS 계정을 생성하려면

다음 명령 중 하나를 사용하여 계정을 생성할 수 있습니다.

- AWS CLI: create-account

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
```

```
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

그리고 다음 명령을 사용하여 계정 생성 상태를 확인할 수 있습니다.

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- AWS SDK: CreateAccount

조직 내 멤버 계정에 액세스

조직에서 계정을 생성하면 AWS Organizations에서는 루트 사용자 외에 기본적으로 `OrganizationAccountAccessRole`이라는 IAM 역할을 자동으로 생성합니다. 계정을 생성할 때 다른 이름을 지정할 수 있지만 모든 계정에서 일관되게 이름을 지정하는 것이 좋습니다. 이 설명서에서는 기본 이름으로 역할을 참조합니다. AWS Organizations는 다른 사용자나 역할을 생성하지 않습니다. 조직 내 계정에 액세스하려면 다음 방법 중 하나를 사용해야 합니다.

- AWS 계정을 생성할 때는 해당 계정의 모든 AWS 서비스및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 ID로 시작합니다. 이 자격 증명은 AWS 계정루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에는 루트 사용자를 가급적 사용하지 않는 것이 좋습니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오. 추가 루트 사용자 보안 권장 사항은 AWS 계정의 루트 사용자 모범 사례를 참조하십시오.

- AWS Organizations의 일부로 제공되는 도구를 사용하여 계정을 만드는 경우 이 방식으로 생성한 모든 신규 계정에 존재하는 `OrganizationAccountAccessRole`이라는 사전 구성된 역할을 사용하여 계정에 액세스할 수 있습니다. 자세한 설명은 관리 계정 액세스 역할이 있는 멤버 계정 액세스 섹션을 참조하세요.
- 기존 계정을 조직에 가입하도록 초대하고 해당 계정에서 초대를 수락한 경우, 초대받은 멤버 계정에 관리 계정이 액세스할 수 있게 허용하는 IAM 역할을 생성할 수 있습니다. 이 역할은 AWS Organizations를 사용하여 만든 계정에 자동으로 추가된 역할과 동일합니다. 이 역할을 생성하려면 초대된 멤버 OrganizationAccountAccessRole 계정에서 생성 단원을 참조하세요. 역할을 생성한 후에는 관리 계정 액세스 역할이 있는 멤버 계정 액세스에 있는 단계를 이용해 역할에 액세스할 수 있습니다.
- AWS IAM Identity Center을 사용하여 AWS Organizations에서 IAM Identity Center에 대한 신뢰할 수 있는 액세스를 활성화합니다. 이렇게 하면 사용자가 회사 자격 증명으로 AWS 액세스 포털에 로그인한 후, 자신에게 할당된 관리 계정 또는 멤버 계정에 있는 리소스에 액세스할 수 있습니다.

  자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 계정 권한을 참조하세요. IAM Identity Center의 신뢰할 수 있는 액세스 설정에 대한 자세한 내용은 AWS IAM Identity Center 및 AWS Organizations 단원을 참조하세요.

> **최소 권한**
>
> 조직 내 다른 계정에서 AWS 계정에 액세스하려면 다음과 같은 권한이 있어야 합니다.
>
> - `sts:AssumeRole` – `Resource` 요소는 별표(*), 또는 새로운 멤버 계정에 액세스해야 하는 사용자의 계정 ID 번호로 설정해야 합니다.

루트 사용자로 멤버 계정에 액세스

새 계정을 만들 때 처음에 AWS Organizations에서 루트 사용자에게 최소 64자 길이의 암호를 할당합니다. 모든 문자는 무작위로 생성되고 특정 문자 세트가 표시된다는 보장은 없습니다. 이 초기 암호는 검색할 수 없습니다. 루트 사용자로 계정에 최초 액세스할 때는 암호 복구 작업을 거쳐야 합니다. 자세한 내용은 AWS로그인 사용 설명서의 루트 사용자 암호를 잊어버렸습니다를 참조하십시오. AWS 계정

참고

- 가장 좋은 방법은 더 제한적인 권한을 가진 다른 사용자나 역할을 생성하기를 제외하고는 사용자 계정에 액세스하기 위해 루트 사용자를 사용하지 마세요. 그런 다음 해당 사용자나 역할로 로그인하세요.
- 루트 사용자에 대해 멀티 팩터 인증(MFA)를 설정하는 것도 좋습니다. 암호를 재설정한 후 루트 사용자에게 MFA 디바이스를 할당합니다.
- 정확하지 않은 이메일 주소로 조직의 멤버 계정을 생성한 경우 루트 사용자로 계정에 로그인할 수 없습니다. AWS 결제 및 지원에 문의하여 지원을 받으세요.

초대된 멤버 OrganizationAccountAccessRole 계정에서 생성

조직의 일부인 멤버 계정을 생성했다면 AWS는 기본적으로 역할을 맡을 수 있는 관리 계정의 IAM 사용자에게 관리자 권한을 부여하는 계정에 역할을 자동으로 생성합니다. 기본적으로 역할 이름은 `OrganizationAccountAccessRole`입니다. 자세한 정보는 관리 계정 액세스 역할이 있는 멤버 계정 액세스을 참조하세요.

그러나 조직에 초대한 멤버 계정은 생성한 관리자 역할을 자동으로 받지 않습니다. 다음 절차에 따라 직접 획득해야 합니다. 이 작업은 생성된 계정을 위해 자동으로 설정된 역할을 복제합니다. 일관성을 유지하고 기억하기 쉽도록 되도록 직접 만든 역할과 같은 이름인 `OrganizationAccountAccessRole`을 사용하세요.

AWS Management Console

멤버 계정에서 AWS Organizations 관리자 역할을 생성하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔에 로그인합니다. 멤버 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 수임하거나, 루트 사용자로 로그인(권장되지 않음)해야 합니다. 사용자 또는 역할에게 IAM 역할 및 정책을 생성할 권한이 있어야 합니다.
2. IAM 콘솔에서 역할로 이동한 다음 역할 생성을 선택합니다.
3. 선택한 AWS 계정다음 기타를 선택합니다. AWS 계정
4. 관리자에게 액세스 권한을 부여하려는 관리 계정의 12자리 계정 ID 번호를 입력합니다. 옵션에서 다음 사항을 참고하십시오.

- 계정은 회사 내부의 계정이기 때문에 이 역할에 대해 외부 ID 필요(Require external ID)를 선택해서는 안 됩니다. 외부 ID 옵션에 대한 자세한 내용은 외부 ID는 언제 사용해야 하나요? 를 참조하십시오. IAM 사용 설명서에서
- MFA를 활성화하고 구성했다면 멀티 팩터 인증 장치를 이용한 인증을 요구하게 할 수도 있습니다. MFA에 대한 자세한 내용은 IAM 사용 설명서의 멀티 팩터 인증 (MFA) 사용을 참조하십시오. AWS

5. 다음을 선택합니다.
6. 권한 추가 페이지에서 이름이 지정된 AWS **AdministratorAccess** 관리형 정책을 선택한 후 다음을 선택합니다.
7. 이름, 검토 및 생성 페이지에서 역할 이름과 선택적 설명을 지정합니다. 되도록 새 계정의 역할에 할당된 기본 이름과 동일한 `OrganizationAccountAccessRole`을 사용하세요. [Create role]을 선택하여 변경 사항을 커밋합니다.
8. 새로운 역할이 이용 가능한 역할 목록에 표시됩니다. 새 역할의 이름을 선택하여 세부 정보를 봅니다. 제공된 링크 URL에 특히 유의해야 합니다. 이 URL을 역할에 액세스해야 하는 멤버 계정 사용자에게 제공합니다. 또한 15단계에서 필요하므로 역할 ARN을 기록해 두세요.
9. https://console.aws.amazon.com/iam/에서 IAM 콘솔에 로그인합니다. 이번에는 정책을 만들어서 사용자나 그룹에 할당할 권한이 있는 관리 계정의 사용자로 로그인합니다.
10. 정책으로 이동한 다음 정책 생성을 선택합니다.
11. [Service]에서 [STS]를 선택합니다.
12. 작업(Actions)에서 필터 상자에 **AssumeRole**을 입력하기 시작하고 해당 항목이 나타나면 그 옆에 있는 확인란을 선택합니다.
13. 리소스에서 특정 항목이 선택되어 있는지 확인한 다음 ARN 추가를 선택합니다.
14. AWS 멤버 계정 ID 번호를 입력하고 이전에 1~8단계에서 생성한 역할의 이름을 입력합니다. ARN 추가를 선택합니다.
15. 여러 멤버 계정의 역할을 맡는 권한을 부여하는 경우 각 계정에 대해 14단계 및 15단계를 반복합니다.
16. 다음을 선택합니다.
17. 검토 및 생성 페이지에서 새 정책의 이름을 입력한 다음 Create policy (정책 생성) 를 선택하여 변경 사항을 저장합니다.
18. 탐색 창에서 사용자 그룹을 선택한 다음 구성원 계정 관리를 위임하는 데 사용할 그룹 이름 (확인란이 아님) 을 선택합니다.
19. 권한 탭을 선택합니다.

20. [권한 추가] 를 선택하고 [정책 연결] 을 선택한 다음 11-18단계에서 만든 정책을 선택합니다.

선택한 그룹의 멤버인 사용자는 이제 9단계에서 캡처한 URL을 이용해 멤버 계정의 역할에 액세스할 수 있습니다. 이들은 조직에서 사용자가 생성한 계정에 액세스할 때와 같은 방식으로 멤버 계정에 액세스할 수 있습니다. 역할을 이용해 멤버 계정을 관리하는 방법에 대한 자세한 내용은 관리 계정 액세스 역할이 있는 멤버 계정 액세스을(를) 참조하세요.

관리 계정 액세스 역할이 있는 멤버 계정 액세스

AWS Organizations 콘솔을 사용하여 멤버 계정을 생성하면 AWS Organizations가 자동으로 계정에 `OrganizationAccountAccessRole`이라는 IAM 역할을 생성합니다. 이 역할은 멤버 계정에 대한 완전한 관리 권한을 갖습니다. 이 역할에 대한 액세스 범위에는 관리 계정의 모든 보안 주체가 포함되며, 조직의 관리 계정에 해당 액세스 권한을 부여하도록 역할이 구성됩니다. 초대된 멤버 OrganizationAccountAccessRole 계정에서 생성에 있는 단계를 이용하면 초대한 멤버 계정과 같은 역할을 만들 수 있습니다. 이 역할을 이용해 멤버 계정에 액세스하려면, 역할을 맡을 수 있는 권한이 있는 관리 계정에서 사용자로 로그인해야 합니다. 이러한 권한을 구성하려면 다음 절차를 수행해야 합니다. 관리 용이성을 위해 되도록 사용자 대신 그룹에 권한을 부여하세요.

AWS Management Console

역할 액세스를 위해 관리 계정에 있는 IAM 그룹의 멤버에게 권한을 부여하려면

1. 관리 계정에서 관리자 권한이 있는 사용자로 https://console.aws.amazon.com/iam/의 IAM 콘솔에 로그인합니다. 해당 사용자가 멤버 계정의 역할에 액세스하도록 IAM 그룹에 권한을 위임하기 위해 필요한 작업입니다.
2. ???에서 나중에 필요한 관리형 정책 생성부터 시작합니다.

   탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.
3. Visual 편집기 탭에서 서비스 선택을 선택하고 검색 상자에 **STS**를 입력하여 목록을 필터링한 다음 STS 옵션을 선택합니다.
4. 작업 섹션에서 검색 상자에 입력하여 목록을 필터링한 다음 AssumeRole옵션을 선택합니다. **`assume`**
5. 리소스 섹션에서 [특정] 을 선택하고 [ARN 추가] 를 선택한 다음 멤버 계정 번호와 이전 섹션에서 만든 역할 이름을 입력합니다 (이름을 지정하는 것이 `OrganizationAccountAccessRole` 좋습니다).
6. 대화 상자에 올바른 ARN이 표시되면 [ARN 추가] 를 선택합니다.

7. (선택 사항) 멀티 팩터 인증(MFA)을 요구하거나 지정된 IP 주소 범위에서 역할에 대한 액세스를 제한하려면 요청 조건 섹션을 확장하고 적용할 옵션을 선택합니다.
8. 다음을 선택합니다.
9. 검토 및 생성 페이지에서 새 정책의 이름을 입력합니다. 예: **`GrantAccessToOrganizationAccountAccessRole`**. 또한 설명(선택 사항)을 추가할 수도 있습니다.
10. 정책 생성을 선택하여 새로운 관리형 정책을 저장합니다.
11. 정책을 사용할 수 있으므로 그룹에 연결할 수 있습니다.

    탐색 창에서 사용자 그룹을 선택한 다음 구성원 계정에서 역할을 수임할 구성원이 속한 그룹의 이름 (확인란이 아님) 을 선택합니다. 필요한 경우 그룹을 새로 만들어도 됩니다.
12. 권한 탭을 선택하고 권한 추가, 정책 연결을 차례로 선택합니다.
13. (선택 사항) 검색 상자에 Step 2에서 Step 10까지 방금 생성한 정책의 이름이 표시될 때까지 정책 이름을 입력하여 목록을 필터링할 수 있습니다. 모든 유형을 선택한 다음 고객 관리를 선택하여 AWS 관리형 정책을 모두 필터링할 수도 있습니다.
14. 정책 옆의 체크박스를 선택한 다음 정책 연결을 선택합니다.

다음 절차에 따라 그룹 멤버인 IAM 사용자는 이제 AWS Organizations 콘솔에 있는 새 역할로 전환할 수 있는 권한을 얻게 됩니다.

AWS Management Console

멤버 계정의 역할로 전환하려면

역할을 이용할 때, 사용자는 새 멤버 계정의 관리자 권한을 얻습니다. 새 역할로의 전환을 위해 그룹 멤버인 IAM 사용자에게 다음을 수행하도록 지시합니다.

1. AWS Organizations 콘솔의 오른쪽 상단에서 현재 로그인 이름이 있는 링크를 선택한 후 역할 전환(Switch Role)을 선택합니다.
2. 관리자가 제공한 계정 ID 번호와 역할 이름을 입력합니다.
3. 표시 이름에 역할을 사용하는 동안 탐색 모음 오른쪽 위에 사용자 이름 대신 표시할 텍스트를 입력합니다. 색상을 선택할 수도 있습니다.
4. 역할 전환을 선택합니다. 이제 수행하는 모든 작업은 전환한 역할에 부여된 권한으로 수행하게 됩니다. 다시 전환할 때까지는 원래 IAM 사용자와 관련된 권한을 더 이상 이용할 수 없습니다.

5. 역할의 권한이 필요한 작업을 수행 완료했으면, 다시 일반 IAM 사용자로 전환해도 됩니다. 오른쪽 상단에서 역할 이름 (표시 이름으로 지정한 이름) 을 선택한 다음 [Back to] 를 선택합니다. *UserName*

추가 리소스

- 역할 전환 권한 부여에 대한 자세한 내용은 IAM User Guide의 역할 전환 권한 부여를 참조하십시오.
- 위임 권한이 부여된 역할을 사용하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 전환 (콘솔) 을 참조하십시오.
- 교차 계정 액세스를 위한 역할 사용에 대한 자습서는 IAM 사용 설명서의 자습서: IAM 역할 AWS 계정 사용에 대한 액세스 위임을 참조하십시오.
- AWS 계정 해지에 대한 자세한 내용은 조직 내 멤버 계정 해지 단원을 참조하세요.

조직에 대한 AWS 계정 세부 정보 내보내기

AWS Organizations를 사용하면 조직의 관리 계정 사용자 및 위임된 관리자가 조직 내의 모든 계정 세부 정보가 포함된 .csv 파일을 내보낼 수 있습니다. 따라서 조직 관리자는 계정을 쉽게 보고 상태별로 (`ACTIVE`, `SUSPENDED` 또는 `PENDING`) 필터링할 수 있습니다. 조직에 많은 계정이 있는 경우.csv 파일 다운로드 옵션을 사용하면 스프레드시트에서 계정 세부 정보를 쉽게 보고 정렬할 수 있습니다.

이전에는 계정을 볼 수 있는 유일한 방법은 AWS Organizations 콘솔에서 계정 계층 또는 목록 표시를 보는 것이었습니다.

> **Note**
>
> 관리 계정의 보안 주체만 계정 목록을 다운로드할 수 있습니다.

조직에서 모든 AWS 계정 목록 내보내기

조직의 관리 계정에 로그인하면 조직에 속한 모든 계정 목록을 .csv 파일로 가져올 수 있습니다. 목록에는 개별 계정 세부 정보가 포함되어 있지만 계정이 속한 조직 단위(OU)는 지정하지 않습니다.

.csv 파일에는 각 계정에 대한 다음 정보가 포함되어 있습니다.

- 계정 ID - 숫자 계정 식별자입니다. 예: 123456789012

- ARN - 계정에 Amazon 리소스 이름입니다. 예: `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`.
- 이메일 - 계정과 연결된 이메일 주소입니다. 예: marymajor@example.com
- 이름 - 계정 생성자가 제공한 계정 이름입니다. 예: 단계 테스트 계정
- 상태 - 조직 내 계정 상태입니다. 값은 `PENDING`, `ACTIVE` 또는 `SUSPENDED`일 수 있습니다.
- 가입 방법 - 계정 생성 방법을 지정합니다. 값은 `INVITED` 또는 `CREATED`일 수 있습니다.
- 가입 타임스탬프 - 계정이 조직에 가입한 날짜 및 시간입니다.

> 최소 권한
>
> 조직의 모든 멤버 계정으로 .csv 파일을 내보내려면 다음 권한이 있어야 합니다.
>
> - `organizations:DescribeOrganization`
> - `organizations:ListAccounts`

AWS Management Console

조직의 모든 AWS 계정에 대해 .csv 파일을 내보내려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 작업(Actions)을 선택한 다음 AWS 계정에서 계정 목록 내보내기(Export account list)를 선택합니다. 페이지 상단의 파란색 배너는 “내보내기가 진행 중입니다!”를 나타냅니다.
3. 파일이 준비되면 배너가 녹색으로 바뀌고 “다운로드가 준비되었습니다!”를 나타냅니다. Download CSV를 선택합니다. 파일 `Organization_accounts_information.csv`가 디바이스에 다운로드됩니다.

AWS CLI & AWS SDKs

계정 세부 정보가 포함된 .csv 파일을 내보내는 유일한 방법은 AWS Management Console을 사용하는 것입니다. AWS CLI를 사용하여 계정 목록 .csv 파일을 내보낼 수 없습니다.

조직에서 멤버 계정 제거

조직 내 계정 관리의 일환으로 더 이상 필요하지 않은 멤버 계정을 제거하세요. 구성원 계정을 제거하면 해당 계정이 해지되는 것이 아니라 조직에서 해당 구성원 계정이 제거됩니다. 이전 멤버 계정은 더 이상 AWS Organizations에서 관리하지 않는 독립형 AWS 계정 계정이 됩니다. 이후, 해당 계정에는 더 이상 정책이 적용되지 않으며 자체 청구서 결제에 대한 책임이 있습니다. 계정이 조직에서 제거된 후, 조직의 관리 계정은 해당 계정에서 발생한 비용에 대해 더 이상 청구되지 않습니다.

관리 계정을 제거하는 방법은 조직 삭제 단원을 참조하세요

주제

조직에서 계정을 제거하기 전 고려할 사항

계정을 제거하기 전에 다음 사항을 고려해야 합니다.

- 계정에 독립형 계정으로 작동하는 데 필요한 정보가 있는 경우에만 조직에서 계정을 제거할 수 있습니다. AWS Organizations 콘솔, API 또는 AWS CLI 명령을 사용하여 조직에 계정을 생성하는 경우 독립형 계정의 모든 필수 정보가 자동으로 수집되지 않습니다. 독립형으로 만들려는 각 계정마다 지원 계획을 선택하고, 필요한 계약 정보를 제공 및 확인하고, 현행 결제 방법을 제공해야 합니다. AWS에서는 이 결제 수단을 사용해 해당 계정이 조직에 연결되어 있지 않을 때 발생하는 모든 청구 가능한 AWS 활동(AWS 프리 티어 이외)에 대해 비용을 청구합니다. 아직 이 정보가 없는 계정을 제거하려면 멤버 계정에서 조직 탈퇴의 단계를 따르세요.
- 조직에서 생성된 계정을 제거하려면 계정을 만든 후 7일 이상 기다려야 합니다. 초대된 계정에는 이 대기 기간이 적용되지 않습니다.
- 계정이 성공적으로 조직을 떠나는 순간 AWS 계정의 소유자는 발생한 모든 신규 AWS 비용을 책임지게 되며, 해당 계정의 결제 방법이 사용됩니다. 조직의 관리 계정은 더 이상 책임이 없습니다.
- 제거하려는 계정은 조직에 대해 활성화된 어떠한 AWS 서비스에서도 위임된 관리자 계정이 아니어야 합니다. 계정이 위임된 관리자인 경우 먼저 위임된 관리자 계정을 조직에 남아 있는 다른 계정으로 변경해야 합니다. AWS 서비스에 대한 위임된 관리자 계정을 비활성화하거나 변경하는 방법에 관한 자세한 내용은 해당 서비스에 대한 설명서를 참조하세요.
- 조직에 생성된 계정(AWS Organizations 콘솔 또는 `CreateAccount` API를 사용하여 생성된 계정)을 제거한 후에도 (i) 생성된 계정에는 관리 계정의 계약 조항이 적용되며 (ii) 생성하는 관리 계정은

생성된 계정이 수행하는 모든 작업에 대해 여전히 공동으로 그리고 각기 책임이 있습니다. 고객의 계약, 그리고 계약 하에 있는 권리 및 의무는 사전 동의 없이 할당 또는 전송될 수 없습니다. 당사의 동의를 얻으려면, AWS에 문의하십시오.

- 멤버 계정이 조직을 탈퇴할 때 해당 계정은 조직의 멤버였을 때의 시간 범위로부터 비용 및 사용량 데이터에 대한 액세스를 할 수 없습니다. 하지만 조직의 관리 계정은 여전히 데이터에 액세스할 수 있습니다. 멤버 계정이 조직에 다시 가입하면 계정은 다시 데이터에 액세스할 수 있습니다.
- 멤버 계정이 조직을 나가면 계정에 연결된 모든 태그가 삭제됩니다.
- 조직에서 멤버 계정을 제거해도 조직의 관리 계정으로 액세스할 수 있도록 생성된 IAM 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 역할 또는 인스턴스 프로필 삭제를 참조하세요.

조직에서 계정 제거의 영향

조직에서 계정을 제거할 경우 계정이 직접 변경되지는 않습니다. 그러나 다음과 같은 간접적인 영향이 발생합니다.

- 계정은 이제 자체 요금을 지불할 책임이 있으며 계정에 유효한 결제 방법이 연결되어 있어야 합니다.
- 계정의 보안 주체는 더 이상 조직에 적용된 정책의 영향을 받지 않습니다. 즉, SCP에 의해 가해지는 제한이 사라지므로 해당 계정의 사용자와 역할은 이전보다 더 많은 권한을 갖게 될 수 있습니다. 다른 조직 정책 유형은 더 이상 적용하거나 처리할 수 없습니다.
- 어떤 정책에서 `aws:PrincipalOrgID` 조건 키를 사용하여 조직 내 AWS 계정의 사용자 및 역할만 액세스하도록 제한한 경우 멤버 계정을 제거하기 전에 이러한 정책을 검토하고 가능하면 업데이트해야 합니다. 정책을 업데이트하지 않으면 계정이 조직을 나갈 때 계정의 사용자와 역할이 리소스에 대한 액세스 권한을 잃을 수 있습니다.
- 다른 서비스와의 통합이 비활성화될 수 있습니다. AWS 서비스와의 통합이 활성화된 조직에서 계정을 제거하면 해당 계정의 사용자는 더 이상 해당 서비스를 사용할 수 없습니다.

조직에서 멤버 계정 제거

조직의 관리 계정에 로그인하면 조직에서 더 이상 필요 없는 멤버 계정을 제거할 수 있습니다. 이렇게 하려면 다음 절차를 완료하세요. 이 절차는 멤버 계정에만 적용됩니다. 관리 계정을 제거하려면 조직을 삭제해야 합니다.

Note

조직에서 삭제된 멤버 계정에는 해당 조직 계약이 더 이상 적용되지 않습니다. 필요한 경우 멤버 계정이 새 계약을 체결할 수 있도록 관리 계정 관리자는 조직에서 멤버 계정을 삭제하기 전에 이 사실을 해당 멤버 계정에게 알려줘야 합니다. 현재 유효한 조직 계약의 목록은 AWS Artifact 콘솔의 AWS Artifact 조직 계약 페이지에서 볼 수 있습니다.

최소 권한

조직에서 하나 이상의 멤버 계정을 제거하려면 다음 권한이 있는 관리 계정의 사용자 또는 역할로 로그인해야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:RemoveAccountFromOrganization`

5단계에서 멤버 계정의 사용자 또는 역할로 로그인하도록 선택할 경우 해당 사용자 또는 역할은 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:LeaveOrganization` – 조직 관리자는 이 권한을 제거한 계정에 정책을 적용하여 조직에서 계정을 제거하지 못하도록 할 수 있습니다.
- IAM 사용자로 로그인했는데 계정에 결제 정보가 없는 경우 사용자에게 `aws-portal:ModifyBilling` 및 `aws-portal:ModifyPaymentMethods` 권한(계정이 아직 세분화된 권한으로 마이그레이션되지 않은 경우) 또는 `payments:CreatePaymentInstrument` 및 `payments:UpdatePaymentPreferences` 권한(계정이 세분화된 권한으로 마이그레이션된 경우)이 있어야 합니다. 또한 멤버 계정에는 결제에 대한 IAM 사용자 액세스가 활성화되어야 합니다. 아직 활성화되지 않은 경우 AWS Billing 사용 설명서의 Billing and Cost Management 콘솔에 대한 액세스 활성화를 참조하세요.

AWS Management Console

조직에서 멤버 계정을 제거하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서, 조직에서 제거할 각 멤버 계정을 찾아서 그 옆에 있는 확인란☑을 선택합니다. OU 계층 구조를 탐색하거나, AWS 계정만 보기(View AWS 계정 only)를 활성화하여 OU 구조 없이 단순 계정 목록을 표시할 수 있습니다. 계정이 많은 경우 이동할 모든 항목을 찾기 위해 목록 하단에 있는 'ou-name'에서 추가 계정 로드(Load more accounts in 'ou-name')를 선택해야 할 수도 있습니다.

   AWS 계정 페이지에서, 조직에서 제거할 멤버 계정의 이름을 찾아서 선택합니다. 원하는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다(▶ 선택).
3. 작업(Actions)을 선택한 다음 AWS 계정에서 조직에서 제거(Remove from organization)를 선택합니다.
4. 'account-name'(#account-id-num) 계정을 조직에서 제거하시겠습니까?라는 대화 상자에서 계정 제거(Remove account)를 선택합니다.
5. AWS Organizations가 하나 이상의 계정 제거에 실패한 경우 일반적으로 계정이 독립형 계정으로 작동하는 데 필요한 모든 정보가 제공되지 않았기 때문입니다. 다음 단계를 수행합니다.

   a. 실패한 계정에 로그인합니다. [Copy link]를 선택하고 이를 새로운 익명 브라우저 창의 주소 표시줄에 붙여넣음으로써 로그인하는 것이 좋습니다. 익명 창을 사용하지 않는 경우, 관리 계정에서 로그아웃되고 이 대화 상자로 다시 돌아갈 수 없습니다.

   b. 브라우저에서 이 계정에서 누락된 모든 단계를 완료할 로그인 절차로 직접 이동합니다. 제시되는 모든 단계를 수행합니다. 이러한 단계에는 다음 작업이 포함되어 있을 수 있습니다.

      - 연락처 정보 제공
      - 올바른 결제 방법 제공
      - 전화 번호 확인
      - 지원 플랜 옵션 선택

c. 마지막 로그인 단계를 완료한 후 AWS는 자동적으로 멤버 계정의 AWS Organizations 콘솔로 브라우저를 리디렉션합니다. [Leave organization]을 선택한 다음 확인 대화 상자에서 확인을 선택합니다. 다른 조직에 대해 보류 중인 계정 가입 초대를 확인할 수 있는 AWS Organizations 콘솔의 시작하기 페이지로 이동했습니다.

d. 계정에 대한 액세스 권한을 부여하는 IAM 역할을 조직에서 제거합니다.

> **Important**
>
> 조직에서 계정이 생성된 경우 Organizations는 조직의 관리 계정에 의한 액세스를 활성화한 IAM 역할을 계정에 자동으로 생성했습니다. 계정이 가입하도록 초대된 경우 Organizations에서 해당 역할을 자동으로 생성하지는 않았지만 사용자 또는 다른 관리자가 동일한 혜택을 받기 위해 계정을 생성했을 수 있습니다. 두 경우 모두 조직에서 계정을 제거할 때 이러한 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 이 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 역할 또는 인스턴스 프로필 삭제를 참조하세요.

AWS CLI & AWS SDKs

조직에서 멤버 계정을 제거하려면

다음 명령 중 하나를 사용하여 멤버 계정을 삭제할 수 있습니다.

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: RemoveAccountFromOrganization

조직에서 멤버 계정이 제거된 후에는 조직에서 계정에 대한 액세스 권한을 부여하는 IAM 역할을 제거해야 합니다.

> **Important**
>
> 조직에서 계정이 생성된 경우 Organizations는 조직의 관리 계정에 의한 액세스를 활성화한 IAM 역할을 계정에 자동으로 생성했습니다. 계정이 가입하도록 초대된 경우 Organizations에서 해당 역할을 자동으로 생성하지는 않았지만 사용자 또는 다른 관리자가 동일한 혜택을 받기 위해 계정을 생성했을 수 있습니다. 두 경우 모두 조직에서 계정을 제거할 때 이러한 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 이 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 역할 또는 인스턴스 프로필 삭제를 참조하세요.

멤버 계정은 대신 조직 탈퇴를 통해 스스로 제거할 수 있습니다. 자세한 내용은 멤버 계정에서 조직 탈퇴 섹션을 참조하세요.

멤버 계정에서 조직 탈퇴

멤버 계정에 로그인하면 조직에서 해당 계정만 제거할 수 있습니다. 이렇게 하려면 다음 절차를 완료하세요. 이 절차는 멤버 계정에만 적용됩니다. 관리 계정은 이 방법을 사용하여 조직에서 나갈 수 없습니다. 관리 계정을 제거하려면 조직을 삭제해야 합니다.

> **Note**
>
> 조직을 포함한 계정의 상태는 어떤 비용 및 사용량 데이터가 표시되는지에 영향을 줍니다.
>
> - 멤버 계정이 조직을 탈퇴하여 독립형 계정이 되는 경우 해당 계정은 조직의 멤버였을 때의 시간 범위로부터 비용 및 사용량 데이터에 대한 액세스를 할 수 없습니다. 해당 계정은 독립형 계정으로 생성된 데이터에만 액세스할 수 있습니다.
> - 멤버 계정이 조직 A를 탈퇴하여 조직 B에 가입하는 경우 계정은 조직 A의 계정이었을 때의 시간 범위로부터 비용 및 사용량에 대한 데이터에 액세스할 수 없습니다. 해당 계정은 조직 B의 멤버로 생성된 데이터에만 액세스할 수 있습니다.
> - 계정이 이전에 속했던 조직에 다시 가입하는 경우 계정은 과거 비용 및 사용량 데이터에 대한 액세스를 다시 얻습니다.

Important

조직에서 나가면 조직의 관리 계정에서 사용자를 대신하여 수락한 조직 계약이 더 이상 적용되지 않습니다. 해당 조직 계약의 목록은 AWS Artifact 콘솔의 AWS Artifact 조직 계약 페이지에서 볼 수 있습니다. 조직을 떠나기 전에 해당되는 경우 법무, 개인정보 보호 또는 규정 준수 팀의 도움을 받아 새 계약이 필요한지에 대한 여부를 결정해야 합니다.

최소 권한

AWS 조직에서 나가려면 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:LeaveOrganization` – 조직 관리자는 이 권한을 제거한 계정에 정책을 적용하여 조직에서 계정을 제거하지 못하도록 할 수 있습니다.
- IAM 사용자로 로그인했는데 계정에 결제 정보가 없는 경우 사용자에게 `aws-portal:ModifyBilling` 및 `aws-portal:ModifyPaymentMethods` 권한(계정이 아직 세분화된 권한으로 마이그레이션되지 않은 경우) 또는 `payments:CreatePaymentInstrument` 및 `payments:UpdatePaymentPreferences` 권한(계정이 세분화된 권한으로 마이그레이션된 경우)이 있어야 합니다. 또한 멤버 계정에는 결제에 대한 IAM 사용자 액세스가 활성화되어야 합니다. 아직 활성화되지 않은 경우 AWS Billing 사용 설명서의 Billing and Cost Management 콘솔에 대한 액세스 활성화를 참조하세요.

AWS Management Console

멤버 계정에서 조직을 탈퇴하려면

1. AWS Organizations 콘솔에서 AWS Organizations 콘솔에 로그인합니다. 멤버 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 수임하거나, 루트 사용자로 로그인(권장되지 않음)해야 합니다.

   기본적으로 AWS Organizations를 사용하여 생성한 멤버 계정에는 루트 사용자 암호에 대한 액세스 권한이 없습니다. 필요한 경우 루트 사용자로 멤버 계정에 액세스의 절차를 수행하여 루트 사용자 암호를 복구하세요.

2. 조직 대시보드 페이지에서 이 조직 탈퇴를 선택합니다.
3. 조직 탈퇴 확인 대화 상자에서 조직 탈퇴를 선택합니다. 확인 메시지가 나타나면 계정 제거 선택을 확인합니다. 확인되면 다른 조직에 대해 보류 중인 계정 가입 초대를 확인할 수 있는 AWS Organizations 콘솔의 시작하기 페이지로 리디렉션됩니다.

   아직 조직을 탈퇴할 수 없음이라는 메시지가 나타나면 해당 계정에 독립 실행형 계정으로 작동하는 데 필요한 정보 중 일부가 없는 것입니다. 이 경우, 다음 단계로 가십시오.
4. 조직 탈퇴 확인 대화 상자에 아직 조직을 탈퇴할 수 없음이 표시되면 계정 가입 단계 완료 링크를 선택합니다.
5. AWS에 가입 페이지에서 이 계정이 독립 실행형 계정이 되는 데 필요한 모든 필수 정보를 입력합니다. 여기에는 다음과 같은 유형의 정보가 포함됩니다.

   - 담당자 이름 및 주소
   - 올바른 결제 방법
   - 전화번호 확인
   - Support 플랜 옵션
6. 로그인 절차가 완료되었다는 대화 상자가 표시되면 [Leave organization]을 선택합니다.

   확인 대화 상자가 표시됩니다. 계정 제거 선택을 확인합니다. 다른 조직에 대해 보류 중인 계정 가입 초대를 확인할 수 있는 AWS Organizations 콘솔의 시작하기 페이지로 이동했습니다.
7. 계정에 대한 액세스 권한을 부여하는 IAM 역할을 조직에서 제거합니다.

> **Important**
>
> 조직에서 계정이 생성된 경우 Organizations는 조직의 관리 계정에 의한 액세스를 활성화한 IAM 역할을 계정에 자동으로 생성했습니다. 계정이 가입하도록 초대된 경우 Organizations에서 해당 역할을 자동으로 생성하지는 않았지만 사용자 또는 다른 관리자가 동일한 혜택을 받기 위해 계정을 생성했을 수 있습니다. 두 경우 모두 조직에서 계정을 제거할 때 이러한 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 이 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 역할 또는 인스턴스 프로필 삭제를 참조하세요.

AWS CLI & AWS SDKs

멤버 계정으로 조직에서 나가려면

다음 명령 중 하나를 사용하여 조직을 나갈 수 있습니다.

- AWS CLI: leave-organization

  다음 예제는 명령 실행에 사용되는 자격 증명을 가진 계정이 조직을 나가도록 합니다.

  ```
  $ aws organizations leave-organization
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS SDK: LeaveOrganization

멤버 계정이 조직을 떠난 후에는 조직에서 계정에 대한 액세스 권한을 부여하는 IAM 역할을 제거해야 합니다.

> **Important**
>
> 조직에서 계정이 생성된 경우 Organizations는 조직의 관리 계정에 의한 액세스를 활성화한 IAM 역할을 계정에 자동으로 생성했습니다. 계정이 가입하도록 초대된 경우 Organizations에서 해당 역할을 자동으로 생성하지는 않았지만 사용자 또는 다른 관리자가 동일한 혜택을 받기 위해 계정을 생성했을 수 있습니다. 두 경우 모두 조직에서 계정을 제거할 때 이러한 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 이 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 역할 또는 인스턴스 프로필 삭제를 참조하세요.

관리 계정의 사용자가 대신 조직에서 계정 제거를 사용하여 멤버 계정을 제거할 수도 있습니다. 자세한 내용은 조직에서 멤버 계정 제거 섹션을 참조하세요.

조직 내 멤버 계정 해지

조직에 더 이상 구성원 계정이 필요하지 않은 경우 이 섹션의 지침에 따라 AWS Organizations 콘솔에서 계정을 폐쇄할 수 있습니다. 조직이 모든 기능 모드인 경우에만 AWS Organizations 콘솔을 사용하여 구성원 계정을 폐쇄할 수 있습니다.

루트 사용자로 로그인한 AWS Management Console 후 의 계정 페이지에서 AWS 계정 직접 계정을 닫을 수도 있습니다. 자세한 step-by-step 지침은 AWS 계정 관리 가이드의 닫기를 AWS 계정 참조하십시오.

관리 계정을 폐쇄하려면 을 참조하십시오조직의 관리 계정 폐쇄하기.

회원 계정 해지 방법

조직의 관리 계정에 로그인하면 조직에 속한 멤버 계정을 해지할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

> **Important**
>
> 회원 계정을 폐쇄하기 전에 고려 사항을 검토하고 계정 폐쇄에 미치는 영향을 이해하는 것이 좋습니다. 자세한 내용은 계정 관리 가이드의 계정을 폐쇄하기 전에 알아야 할 사항 및 계정을 폐쇄한 후 예상되는AWS 사항을 참조하십시오.

AWS Management Console

AWS Organizations 콘솔에서 멤버 계정을 폐쇄하려면

1. AWS Organizations 콘솔에 로그인합니다.
2. AWS 계정 페이지에서 해지하려는 멤버 계정의 이름을 찾아서 선택합니다. OU 계층 구조를 탐색하거나, OU 구조 없이 단순 계정 목록만 볼 수 있습니다.
3. 페이지 상단에 계정 이름 옆에 있는 해지(Close)를 선택합니다. 통합 결제 모드의 조직은 콘솔에서 닫기 버튼을 볼 수 없습니다. 통합 결제 모드에서 계정을 폐쇄하려면 계정 관리 가이드의 계정을 폐쇄하는 방법에서 독립형 계정 탭에 있는 단계를 따르세요.AWS
4. 모든 필수 계정 해지 문을 승인하려면 각 확인란을 선택합니다.
5. 멤버 계정 ID를 입력한 다음 계정 폐쇄를 선택합니다.

> **Note**
>
> 해지하는 모든 구성원 계정은 AWS Organizations 콘솔에서 해당 계정 이름 옆에 SUSPENDED 레이블이 표시됩니다.

계정 페이지에서 멤버 계정을 폐쇄하려면

필요에 따라 의 계정 페이지에서 AWS 멤버 계정을 직접 폐쇄할 수 AWS Management Console있습니다. step-by-step지침을 보려면 AWS 계정 관리 가이드의 AWS 계정 닫기에 있는 지침을 따르십시오.

AWS CLI & AWS SDKs

폐쇄하려면 AWS 계정

다음 명령 중 하나를 사용하여 AWS 계정을 해지할 수 있습니다.

- AWS CLI: close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: CloseAccount

해지하지 않도록 멤버 계정 보호

멤버 계정이 우발적으로 해지되지 않도록 보호하고 싶다면 IAM 정책을 생성하여 해지가 면제되는 계정을 지정할 수 있습니다. 이러한 정책으로 보호된 멤버 계정은 해지할 수 없습니다. SCP에서는 관리 계정의 보안 주체에 영향을 주지 않으므로 이 작업을 수행할 수 없습니다.

두 가지 방법 중 하나로 계정 해지를 거부하는 IAM 정책을 생성할 수 있습니다.

- `Resource` 요소에 보호하려는 각 계정의 `arn`을 포함하여 정책에 명시적으로 나열합니다. 예제는 이 정책에 나열된 멤버 계정이 해지되지 않도록 방지 섹션을 참조하세요.
- 개별 계정에 태그를 지정하여 계정이 해지되지 않도록 방지합니다. 정책에 `aws:ResourceTag` 태그 전역 조건 키를 사용하여 태그가 있는 계정이 해지되지 않도록 방지합니다. 계정에 태그를 지정하는 방법은 Organizations 리소스 태그 지정을 참조하세요. 예제는 태그가 있는 멤버 계정이 해지되지 않도록 방지 섹션을 참조하세요.

멤버 계정 해지를 방지하는 IAM 정책 예제

다음 코드 예시는 회원 계정의 계정 폐쇄를 제한하는 데 사용할 수 있는 두 가지 방법을 보여줍니다.

태그가 있는 멤버 계정이 해지되지 않도록 방지

관리 계정의 자격 증명에 다음 정책을 연결할 수 있습니다. 이 정책은 `aws:ResourceTag` 태그 전역 조건`AccountType` 키, `Critical` 태그 값을 포함하여 태그 지정된 모든 멤버가 관리 계정의 보안 주체에 의해 해지되지 않도록 방지합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

이 정책에 나열된 멤버 계정이 해지되지 않도록 방지

관리 계정의 자격 증명에 다음 정책을 연결할 수 있습니다. 이 정책은 관리 계정의 보안 주체가 Resource 요소에 명시적으로 지정된 멤버 계정을 해지하지 않도록 방지합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

조직의 관리 계정 폐쇄하기

조직의 관리 계정을 폐쇄하려면 먼저 조직의 모든 구성원 계정을 닫거나 제거해야 합니다. 관리 계정을 폐쇄하면 폐쇄 후 기간이 만료된 후 해당 조직 내에서 생성한 인스턴스와 정책도 삭제됩니다. AWS Organizations

관리 계정을 폐쇄하는 방법

다음 절차를 사용하여 관리 계정을 폐쇄하십시오.

> **Important**
>
> 관리 계정을 폐쇄하기 전에 고려 사항을 검토하고 계정 폐쇄에 미치는 영향을 이해하는 것이 좋습니다. 자세한 내용은 계정 관리 가이드의 계정을 폐쇄하기 전에 알아야 할 사항 및 계정을 폐쇄한 후 예상되는AWS 사항을 참조하십시오.

AWS Management Console

계정 페이지에서 관리 계정을 폐쇄하려면

> **Note**
>
> AWS Organizations 콘솔에서 직접 관리 계정을 폐쇄할 수는 없습니다.

1. 폐쇄하려는 관리 계정의 루트 AWS Management Console 사용자로 에 로그인합니다. IAM 사용자 또는 역할로 로그인한 상태에서는 계정을 폐쇄할 수 없습니다.
2. 조직에 활성 회원 계정이 남아 있지 않은지 확인하세요. 이 작업을 수행하려면 AWS Organizations 콘솔로 이동하여 모든 구성원 계정이 계정 이름 Suspended 옆에 표시되는지 확인합니다. 아직 활성 상태인 회원 계정이 있는 경우 다음 단계로 조직 내 멤버 계정 해지 넘어가기 전에 에 제공된 지침을 따라야 합니다.
3. 오른쪽 상단의 탐색 표시줄에서 계정 이름 또는 번호를 선택한 다음 계정을 선택합니다.
4. 계정 페이지에서 페이지 하단으로 스크롤하여 계정 닫기 섹션으로 이동합니다. 계정 폐쇄 절차를 읽고 이해했는지 확인하세요.
5. 계정 해지 버튼을 선택하여 계정 폐쇄 프로세스를 시작합니다.
6. 몇 분 내에 계정이 폐쇄되었다는 확인 이메일을 받게 됩니다.

AWS CLI & AWS SDKs

이 작업은 AWS SDK 중 하나의 API 작업에서 AWS CLI 또는 지원되지 않습니다. 이 작업은 를 사용해야만 수행할 수 있습니다. AWS Management Console

조직의 대체 연락처 업데이트

AWS Organizations 콘솔을 사용하거나 AWS CLI 또는 AWS SDK를 사용하여 프로그래밍 방식으로 조직 내 계정의 대체 연락처를 업데이트할 수 있습니다. 대체 연락처를 업데이트하는 방법을 알아보려면 AWS Account Management Reference에서 Accessing or updating the alternate contacts를 참조하세요.

조직의 기본 연락처 정보 업데이트

AWS Organizations 콘솔을 사용하거나 AWS CLI 또는 AWS SDK를 사용하여 프로그래밍 방식으로 조직 내 계정의 기본 연락처 정보를 업데이트할 수 있습니다. 기본 연락처 정보를 업데이트하는 방법을 알아보려면 AWS 계정 관리 참조의 기본 계정 연락처 액세스 또는 업데이트를 참조하세요.

조직의 활성화된 AWS 리전 업데이트

AWS Organizations 콘솔을 사용하여 조직 내의 계정에 대해 활성화된 AWS 리전을 업데이트할 수 있습니다. 활성화된 AWS 리전을 업데이트하는 방법은 AWS 계정 관리 참조의 계정에서 사용 가능한 AWS 리전 지정을 참조하세요.

에서 정책 관리 AWS Organizations

의 정책을 AWS Organizations 사용하면 조직의 에 추가 관리 유형을 적용할 수 있습니다. AWS 계정 조직에서 모든 기능이 활성화되어 있을 때 정책을 사용할 수 있습니다.

AWS Organizations 콘솔에는 각 정책 유형의 활성화 또는 비활성화 상태가 표시됩니다. Organize accounts(계정 구성) 탭의 왼쪽 탐색 창에서 Root를 선택합니다. 화면 오른쪽의 세부 정보 창에는 사용 가능한 모든 정책 유형이 표시됩니다. 목록에는 해당 조직 루트에서 활성화된 항목과 비활성화된 항목이 표시됩니다. 활성화 옵션이 있으면 해당 유형이 현재 비활성화된 상태입니다. 비활성화 옵션이 있으면 해당 유형이 현재 활성화된 상태입니다.

정책 유형

Organizations는 다음과 같은 두 가지 범주의 정책 유형을 제공합니다.

권한 부여 정책

권한 부여 정책은 조직의 AWS 계정 보안을 중앙에서 관리하는 데 도움이 됩니다.

- SCP(서비스 제어 정책)는 조직의 모든 계정에 사용 가능한 최대 권한을 중앙에서 제어합니다.

관리 정책

관리 정책을 사용하면 AWS 서비스와 해당 기능을 중앙에서 구성하고 관리할 수 있습니다.

- 인공 지능(AI) 서비스 옵트아웃 정책을 사용하면 조직의 모든 계정에 대한 AWS AI 서비스의 데이터 수집을 제어할 수 있습니다.
- 백업 정책을 사용하면 중앙 집중식으로 관리하고 조직 계정 전체의 AWS 리소스에 백업 계획을 적용할 수 있습니다.
- 태그 정책은 조직 계정의 AWS 리소스에 첨부된 태그를 표준화하는 데 도움이 됩니다.

다음 표에는 각 정책 유형의 특성 중 일부가 요약되어 있습니다. 이러한 정책 유형에 대한 추가 특성은 에 대한 할당량 AWS Organizations 섹션을 참조하세요.

정책 유형	관리 계정 영향	루트, OU 또는 계정에 연결할 수 있는 최대 수	최대 크기	OU 또는 계정에 대한 효과적인 정책 보기 지원
SCP	 아니요	5	5,120자	 아니요
AI 서비스 옵트아웃 정책	 예	5	2,500자	 예
백업 정책	 예	10	10,000자	 예
태그 정책	 예	10	10,000자	 예

조직에서 정책 사용

- 정책 유형 활성화 및 비활성화
- 조직의 정책에 대한 정보 가져오기
- 에 대한 위임 관리자 AWS Organizations
- 관리 정책
- 서비스 제어 정책(SCP)

정책 유형 활성화 및 비활성화

정책 유형 활성화

정책을 생성하여 조직에 연결하려면 먼저 해당 정책 유형을 사용하도록 활성화해야 합니다. 정책 유형을 활성화하는 것은 조직 루트의 일회성 작업입니다. 조직의 관리 계정에서만 정책 유형을 활성화할 수 있습니다.

> 최소 권한
>
> 정책 유형을 활성화하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.
>
> - `organizations:EnablePolicyType`
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
> - `organizations:ListRoots` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

정책 유형을 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 정책(Policies) 페이지에서 활성화할 정책 유형의 이름을 선택합니다.
3. 정책 유형 페이지에서 정책 유형 활성화(Enable ***policy type***)를 선택합니다.

   지정된 유형의 사용 가능한 정책 목록으로 페이지가 바뀝니다.

AWS CLI & AWS SDKs

정책 유형을 활성화하려면

다음 명령 중 하나를 사용하여 정책 유형을 활성화할 수 있습니다.

- AWS CLI: enable-policy-type

  다음 예제에서는 조직에 백업 정책을 활성화하는 방법을 보여 줍니다. 조직의 루트 ID를 지정해야 합니다.

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

이제 지정한 정책 유형과 함께 ENABLED의 Status가 출력의 PolicyTypes 목록에 포함됩니다.

- AWS SDK: EnablePolicyType

정책 유형 비활성화

조직에서 특정 정책 유형을 더 이상 사용하지 않으려면 해당 유형을 실수로 사용하지 않도록 비활성화할 수 있습니다. 조직의 관리 계정에서만 정책 유형을 비활성화할 수 있습니다.

Important

- 정책 유형을 비활성화하면 지정된 유형의 모든 정책이 조직 루트의 모든 엔터티에서 자동으로 분리됩니다. 정책은 삭제되지 않습니다.
- (서비스 제어 정책 유형만 해당) 나중에 SCP 정책 유형을 다시 활성화하면 조직 루트의 모든 엔터티는 처음에 기본 FullAWSAccess SCP에만 연결됩니다. 조직에서 SCP가 비활성화되면 엔터티에 대한 SCP의 연결이 손실됩니다. 나중에 SCP를 다시 활성화하려면 해당 SCP를 조직의 루트, OU, 계정에 적절히 다시 연결해야 합니다.

최소 권한

SCP를 비활성화하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListRoots` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

정책 유형을 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 정책(Policies)페이지에서 비활성화하려는 정책 유형의 이름을 선택하세요.
3. 정책 유형 페이지에서 정책 유형 비활성화(Disable ***policy type***)를 선택합니다.
4. 확인 대화 상자에서 **disable**이라는 단어를 입력한 다음 비활성화(Disable)를 선택합니다.

   지정된 유형의 사용 가능한 정책 목록이 사라집니다.

AWS CLI & AWS SDKs

정책 유형을 비활성화하려면

다음 명령 중 하나를 사용하여 정책 유형을 비활성화할 수 있습니다.

- AWS CLI: disable-policy-type

  다음 예제에서는 조직에 대해 백업 정책을 비활성화하는 방법을 보여 줍니다. 조직의 루트 ID를 지정해야 합니다.

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
```

```
}
```

지정한 정책 유형이 더 이상 출력의 `PolicyTypes` 목록에 포함되지 않습니다.

- AWS SDK: DisablePolicyType

조직의 정책에 대한 정보 가져오기

이 섹션은 조직 내 정책에 대한 세부 정보를 확인하는 다양한 방법을 설명합니다. 이러한 절차는 모든 정책 유형에 적용됩니다. 해당 유형의 정책을 해당 조직 루트의 모든 엔터티에 연결하려면 먼저 조직 루트에서 정책 유형을 활성화해야 합니다.

모든 정책 나열

> 최소 권한
>
> 조직 내 정책을 나열하려면 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:ListPolicies`

AWS Management Console에서, 또는 AWS Command Line Interface(AWS CLI) 명령이나 AWS SDK 작업을 사용해 조직의 정책을 볼 수 있습니다.

AWS Management Console

조직의 모든 정책을 나열하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 정책(Policies) 페이지에서 나열할 정책을 선택합니다.

   지정된 정책 유형이 활성화되어 있으면 조직에서 현재 사용 가능한 해당 유형의 모든 정책 목록이 콘솔에 표시됩니다.
3. 정책(Policies) 페이지로 돌아가서 각 정책 유형에 대해 위의 과정을 반복합니다.

AWS CLI & AWS SDKs

조직의 모든 정책을 나열하려면

다음 명령 중 하나를 사용하여 조직의 모든 정책을 나열할 수 있습니다.

- AWS CLI: list-policies

  다음 예시에서는 조직의 모든 서비스 제어 정책의 목록을 가져오는 방법을 보여줍니다. 표시할 정책의 유형을 지정해야 합니다. 포함할 각 정책 유형에 대해 명령을 반복합니다.

```
$ aws organizations list-policies \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDK: ListPolicies

루트, OU, 계정에 연결된 정책 나열

> **최소 권한**
>
> 조직 내 루트, 조직 단위(OU) 또는 계정에 연결된 정책을 나열하려면 다음과 같은 권한이 있어야 합니다.
>
> - 동일한 정책 명령문에서 지정된 대상의 Amazon 리소스 이름(ARN)(또는 "*")을 포함하는 `Resource` 요소를 가진 `organizations:ListPoliciesForTarget`

AWS Management Console

지정된 루트, OU 또는 계정에 직접 연결된 모든 정책을 나열하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 정책을 보려는 루트, OU 또는 계정의 이름을 선택합니다. 원하는 OU를 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 루트, OU 또는 계정 페이지에서 정책(Policies) 탭을 선택합니다.

   정책 탭에는 해당 루트, OU 또는 계정에 연결된 모든 정책이 정책 유형별로 그룹화되어 표시됩니다.

AWS CLI & AWS SDKs

지정된 루트, OU 또는 계정에 직접 연결된 모든 정책 나열

다음 명령 중 하나를 사용하여 개체에 연결된 정책을 나열할 수 있습니다.

- AWS CLI: list-policies-for-target

  다음 예제에서는 지정된 OU에 연결된 모든 서비스 제어 정책을 나열합니다. 루트, OU 또는 계정의 ID와 나열할 정책 유형을 모두 지정해야 합니다.

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
```

```
}
```

- AWS SDK: ListPoliciesForTarget

정책이 연결된 모든 루트, OU, 계정 나열

> 최소 권한
>
> 정책이 연결된 개체를 나열하려면 다음과 같은 권한이 있어야 합니다.
>
> - 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 `Resource` 요소를 가진 `organizations:ListTargetsForPolicy`

AWS Management Console

지정된 정책이 연결된 모든 루트, OU, 계정을 나열하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 정책(Policies) 페이지에서 정책 유형을 선택한 다음 연결을 검토하려는 정책의 이름을 선택합니다.
3. 대상(Targets) 탭을 선택하여 선택한 정책이 연결된 모든 루트, OU, 계정의 테이블을 표시합니다.

AWS CLI & AWS SDKs

지정된 정책이 연결된 모든 루트, OU, 계정을 나열하려면

다음 명령 중 하나를 사용하여 정책이 있는 개체를 나열할 수 있습니다.

- AWS CLI: list-targets-for-policy

  다음 예제에서는 지정된 정책이 연결된 모든 루트, OU, 계정을 보여 줍니다.

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
```

```
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```


- AWS SDK: ListTargetsForPolicy

정책 세부 정보 확인

> **최소 권한**
>
> 정책 세부 정보를 표시하려면 다음과 같은 권한이 있어야 합니다.
>
> - 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 organizations:DescribePolicy

AWS Management Console

정책에 대한 세부 정보를 얻으려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 정책(Policies) 페이지에서 검토하려는 정책의 정책 유형을 선택한 다음 정책의 이름을 선택합니다.

   정책 페이지에는 ARN, 설명, 연결된 대상을 비롯해 정책에 대해 제공되는 정보가 표시됩니다.

   - 내용(Content) 탭은 정책의 현재 내용을 JSON 형식으로 보여 줍니다.
   - 대상(Targets) 탭에는 정책이 연결된 루트, OU, 계정의 목록이 표시됩니다.
   - 태그(Tags) 탭에는 정책에 연결된 태그가 표시됩니다. 참고: AWS 관리형 정책은 태그(Tags) 탭을 이용할 수 없습니다.

   정책을 편집하려면 정책 편집(Edit policy)을 선택합니다. 정책 유형마다 편집 요구 사항이 다르기 때문에 지정된 정책 유형의 정책 생성 및 업데이트에 대한 지침을 참조하세요.

AWS CLI & AWS SDKs

정책에 대한 세부 정보를 얻으려면

다음 명령 중 하나를 사용하여 정책에 대한 세부 정보를 확인할 수 있습니다.

- AWS CLI: describe-policy

  다음 예제에서는 지정된 정책의 세부 정보를 표시합니다.

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
```

```
            "AwsManaged": true
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*
\"\n    }\n  ]\n}"
    }
}
```

- AWS SDK: DescribePolicy

에 대한 위임 관리자 AWS Organizations

AWS Organizations 관리 계정과 해당 사용자 및 역할은 해당 계정으로 수행해야 하는 작업에만 사용하는 것이 좋습니다. 또한 AWS 리소스를 조직의 다른 멤버 계정에 저장하고 관리 계정에는 저장하지 않는 것이 좋습니다. 이는 Organizations 서비스 제어 정책(SCP)과 같은 보안 기능이 관리 계정의 사용자나 역할을 제한하지 않기 때문입니다.

조직의 관리 계정에서, Organizations의 정책 관리를 지정된 멤버 계정에 위임하여 기본적으로 관리 계정에서만 사용할 수 있는 정책 작업을 수행할 수 있습니다.

리소스 기반 위임 정책 생성 또는 업데이트

관리 계정에서, 조직의 리소스 기반 위임 정책을 생성하거나 업데이트하고, 정책과 관련한 작업을 수행할 권한이 부여된 멤버 계정을 지정하는 명령문을 추가합니다. 정책에 여러 명령문을 추가하여 멤버 계정마다 다양하게 구성된 권한을 부여할 수 있습니다.

최소 권한

리소스 기반 위임 정책을 생성하거나 업데이트하려면 다음 작업을 실행할 권한이 필요합니다.

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

또한 위임된 관리자 계정의 역할과 사용자에게, 필요한 작업에 해당하는 IAM 권한을 부여해야 합니다. IAM 권한이 없으면 통화 주체에게는 정책을 관리하는 AWS Organizations 데 필요한 권한이 없는 것으로 간주됩니다.

AWS Management Console

AWS Management Console 에서 다음 방법 중 하나를 사용하여 리소스 기반 위임 정책에 명령문을 추가합니다.

- JSON 정책 - 예제 리소스 기반 위임 정책을 붙여 넣고 계정에서 사용하기에 적합하도록 수정하거나, JSON 편집기에서 직접 JSON 정책 문서를 입력합니다.
- 시각적 편집기 - 시각적 편집기에서 새 위임 정책을 구성합니다. 시각적 편집기는 사용자가 JSON 구문을 작성하지 않고도 위임 정책을 만들 수 있도록 안내합니다.

JSON 정책 편집기를 사용하여 위임 정책을 생성하거나 업데이트하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 설정을 선택합니다.
3. Delegated administrator for AWS Organizations(의 위임된 관리자) 섹션에서 Delegate(위임)를 선택하여 Organizations 위임 정책을 생성합니다. 기존 위임 정책을 업데이트하려면 Edit(편집)를 선택합니다.
4. JSON 정책 문서를 입력하거나 붙여 넣습니다. IAM 정책 언어에 대한 자세한 내용은 IAM JSON 정책 참조를 참조하세요.
5. 정책을 검증하는 동안 생성된 모든 보안 경고, 오류 또는 일반 경고를 해결한 다음 Create policy(정책 생성)를 선택하여 작업 내용을 저장합니다.

시각적 편집기를 사용하여 위임 정책을 생성하거나 업데이트하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 설정을 선택합니다.
3. Delegated administrator for AWS Organizations(의 위임된 관리자) 섹션에서 Delegate(위임)를 선택하여 Organizations 위임 정책을 생성합니다. 기존 위임 정책을 업데이트하려면 Edit(편집)를 선택합니다.
4. Create Delegation policy(위임 정책 생성) 페이지에서 Add new statement(새 명령문 추가)를 선택합니다.
5. Effect(효과)를 `Allow`로 설정합니다.

6. `Principal`을 추가하여, 작업을 위임하려는 멤버 계정을 정의합니다. 구문에 대한 자세한 내용은 리소스 기반 위임 정책 예제 섹션을 참조하세요.
7. Actions(작업) 목록에서 위임하려는 작업을 선택합니다. Filter actions(작업 필터링)를 사용하여 선택 범위를 좁힐 수 있습니다.
8. 위임된 멤버 계정이 조직 루트 또는 조직 단위(OU)에 정책을 연결할 수 있도록 할지 여부를 지정하려면, `Resources`를 설정합니다. 또한 리소스 유형으로 `policy`를 선택해야 합니다. 자세한 내용은 리소스 기반 위임 정책 예제 섹션을 참조하세요. 다음과 같은 방법으로 리소스를 지정할 수 있습니다.

   - Add a resource(리소스 추가)를 선택하고 대화 상자에 나타나는 지시에 따라 Amazon 리소스 이름(ARN)을 구성합니다.
   - 편집기에서 리소스 ARN을 수동으로 나열합니다. ARN 구문에 대한 자세한 내용은 일반 참조 안내서의 Amazon 리소스 이름 (ARN) 을 AWS 참조하십시오. 정책의 Resource 요소에 ARN을 사용하는 방법에 대한 자세한 내용은 IAM JSON 정책 요소: Resource를 참조하세요.
9. Add a condition(조건 추가)을 선택하여 위임하려는 정책 유형을 비롯한 다른 조건을 지정합니다. 조건의 Condition key(조건 키), Tag key(태그 키), Qualifier(한정어), Operator(연산자)를 선택한 후 **`Value`**를 입력합니다. 자세한 내용은 리소스 기반 위임 정책 예제섹션을 참조하세요. 마치면 Add condition(조건 추가)을 선택합니다. Condition 요소에 대한 자세한 내용은 IAM JSON 정책 참조에서 IAM JSON 정책 요소: Condition을 참조하세요.
10. 권한 블록을 더 추가하려면 Add new statement(새 명령문 추가)를 선택합니다. 각 블록마다 5~9단계를 반복합니다.
11. 정책을 검증하는 동안 생성된 모든 보안 경고, 오류 또는 일반 경고를 해결한 다음 Create policy(정책 생성)를 선택하여 작업 내용을 저장합니다.

AWS CLI & AWS SDKs

위임 정책 생성 또는 업데이트

위임 정책을 생성하거나 업데이트하려면 다음 명령을 사용합니다.

- AWS CLI: put-resource-policy

  다음 예제에서는 위임 정책을 생성하거나 업데이트합니다.

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            }
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

지원되는 위임 정책 작업

위임 정책과 관련하여 지원되는 작업은 다음과 같습니다.

- `AttachPolicy`

- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource

- `UntagResource`
- `UpdatePolicy`

지원되는 조건 키

에서 지원하는 조건 키만 위임 정책에 사용할 AWS Organizations 수 있습니다. 자세한 내용은 서비스 권한 부여 AWS Organizations참조의 조건 키를 참조하십시오.

리소스 기반 위임 정책 보기

관리 계정에서, 조직의 리소스 기반 위임 정책을 보면서 위임된 관리자별로 어떤 정책 유형을 관리할 권한이 부여되어 있는지 파악합니다.

> 최소 권한
>
> 리소스 기반 위임 정책을 보려면 `organizations:DescribeResourcePolicy` 작업을 실행할 권한이 필요합니다.

AWS Management Console

위임 정책을 보려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 설정을 선택합니다.
3. Delegated administrator for AWS Organizations(의 위임된 관리자) 섹션에서 스크롤하여 전체 위임 정책을 봅니다.

AWS CLI & AWS SDKs

위임 정책 보기

위임 정책을 보려면 다음 명령을 사용합니다.

- AWS CLI: describe-resource-policy

  다음 예제에서는 정책을 검색합니다.

```
$ aws organizations describe-resource-policy
```

- AWS SDK: DescribeResourcePolicy

리소스 기반 위임 정책 삭제

조직의 정책 관리 작업을 더 이상 위임할 필요가 없는 경우, 조직의 관리 계정에서 리소스 기반 위임 정책을 삭제할 수 있습니다.

> **Important**
>
> 삭제한 리소스 기반 위임 정책은 복구할 수 없습니다.

> **최소 권한**
>
> 리소스 기반 위임 정책을 삭제하려면 `organizations:DeleteResourcePolicy` 작업을 실행할 권한이 필요합니다.

AWS Management Console

위임 정책을 삭제하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 설정을 선택합니다.
3. Delegated administrator for AWS Organizations(의 위임된 관리자) 섹션에서 Delete(삭제)를 선택합니다.
4. Delete policy(정책 삭제) 확인 대화 상자에 **delete**를 입력합니다. 그런 다음 Delete policy(정책 삭제)를 선택합니다.

AWS CLI & AWS SDKs

위임 정책 삭제

위임 정책을 삭제하려면 다음 명령을 사용합니다.

- AWS CLI: delete-resource-policy

  다음 예제에서는 정책을 삭제합니다.

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS SDK: DeleteResourcePolicy

리소스 기반 위임 정책 예제

다음 코드 예제는 리소스 기반 위임 정책을 사용하는 방법을 보여줍니다.

예제

- 예: 조직, OU, 계정 및 정책 보기
- 예: 조직의 백업 정책을 관리하기 위한 통합 권한

예: 조직, OU, 계정 및 정책 보기

정책 관리 작업을 위임하기 전에 먼저 조직 구조를 탐색하고, 조직 단위(OU)와 계정, 그리고 거기에 연결된 정책을 확인할 수 있는 권한을 위임해야 합니다.

이 예에서는 *AccountId*라는 멤버 계정에 대한 리소스 기반 위임 정책에 이 권한을 포함하는 방법을 보여줍니다.

> **Important**
>
> 이 정책을 사용하면 어떠한 Organizations 읽기 전용 작업이든 위임할 수 있지만, 이 예에서 보듯이 최소한의 필수 작업에 대한 권한만 포함하는 것이 좋습니다.

이 예제 위임 정책은 AWS API 또는 AWS CLI에서 프로그래밍 방식으로 작업을 수행하는 데 필요한 권한을 부여합니다. 이 위임 정책을 사용하려면 *AccountId*의 AWS 자리 표시자 텍스트를 사용자의 실제 정보로 바꿉니다. 그런 다음 에 대한 위임 관리자 AWS Organizations의 지침을 따릅니다.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

예: 조직의 백업 정책을 관리하기 위한 통합 권한

이 예에서는 `create`, `read`, `update`, `delete` 작업 권한 등 조직 내에서 백업 정책을 관리하는 데 필요한 모든 권한과 `attach` 및 `detach` 정책 작업 권한을 관리 계정에서 위임할 수 있도록 하는 리소스 기반 위임 정책을 생성하는 방법을 보여줍니다. 각 작업, 리소스 및 조건의 중요성에 대해서는 리소스 기반 위임 정책 예제 섹션을 참조하세요.

> **Important**
>
> 위임된 관리자는 이 정책을 통해, 관리 계정을 비롯하여 조직의 모든 계정에서 생성한 정책에 대해 지정된 작업을 수행할 수 있습니다.

이 예제 위임 정책은 AWS API 또는 에서 프로그래밍 방식으로 작업을 완료하는 데 필요한 권한을 부여합니다. AWS CLI이 위임 정책을 사용하려면, *ManagementAccountIdOrganizationId*, 및 의 AWS 자리 표시자 텍스트를 사용자 고유의 *MemberAccountIdRootId*정보로 바꾸십시오. 그런 다음 에 대한 위임 관리자 AWS Organizations의 지침을 따릅니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
```

```
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

관리 정책

관리 정책을 사용하면 AWS 서비스와 해당 기능을 중앙에서 구성하고 관리할 수 있습니다. 정책이 해당 정책을 상속하는 OU 및 계정에 미치는 영향은 AWS Organizations에 적용되는 관리 정책 유형에 따라 달라집니다. 이 섹션의 주제를 검토하여 관리 정책에 대한 관련 용어 및 개념을 이해하세요.

주제

- 관리 정책 상속에 대한 이해
- AI 서비스 옵트아웃 정책
- 백업 정책
- 태그 정책

관리 정책 상속에 대한 이해

> **Note**
>
> SCP는 IAM 작업의 허용 및 거부를 모두 관리하기 때문에 이 섹션의 정보는 SCP에는 적용되지 않습니다. SCP는 루트, OU 및 계정에 연결되어 있지만 작업을 허용하려면 루트에서 각 OU에

이르는 모든 수준의 SCP에서 계정 직접 경로(대상 계정 자체 포함)에 명시적인 `allow` 설명이 필요합니다. AWS Organizations 계층의 SCP 작업 방법에 대한 자세한 내용은 의 SCP 평가을(를) 참조하세요.

조직에 속한 조직 엔터티(조직 루트, OU(조직 단위) 또는 계정)에 관리 정책을 연결할 수 있습니다.

- 정책을 조직 루트에 연결하면 조직의 모든 OU 및 계정이 해당 정책을 상속합니다.
- 정책을 특정 OU에 연결하면 해당 OU 또는 하위 OU 바로 아래에 있는 계정이 관리 정책을 상속합니다.
- 관리 정책을 특정 계정에 연결하면 해당 계정에만 영향을 미칩니다.

조직의 여러 수준에 관리 정책을 연결할 수 있으므로 계정은 여러 정책을 상속할 수 있습니다.

이 단원에서는 상위 정책과 하위 정책이 계정의 유효 정책으로 처리되는 방법을 설명합니다.

주제

- 상속 용어
- 관리 정책 유형에 대한 정책 구문 및 상속
- 상속 연산자
- 상속 사례

상속 용어

이 주제에서는 관리 정책 상속을 설명할 때 다음 용어를 사용합니다.

정책 상속

조직의 최상위 루트에서 OU(조직 단위) 계층 그리고 개별 계정으로 이동하며 조직의 서로 다른 수준에서 이루어지는 정책의 상호 작용입니다.

조직 루트, OU, 개별 계정 및 이러한 조직 엔터티의 조합에 정책을 연결할 수 있습니다. 관리 정책 상속은 조직 루트 또는 OU에 연결된 정책을 말합니다. 관리 정책이 연결된 조직 루트 또는 OU의 멤버인 모든 계정은 해당 정책을 상속 합니다.

예를 들어 관리 정책이 조직 루트에 연결되면 조직의 모든 계정이 해당 정책을 상속합니다. 조직의 모든 계정이 항상 조직 루트 아래에 있기 때문입니다. 정책을 특정 OU에 연결하면 해당 OU 또는 하

위 OU 바로 아래에 있는 계정이 정책을 상속합니다. 조직의 여러 수준에 정책을 연결할 수 있으므로 계정은 단일 정책 유형에 대해 여러 정책 문서를 상속할 수 있습니다.

상위 정책

조직 트리에서 트리 아래쪽에 있는 엔터티에 연결된 정책보다 높은 수준에 연결된 정책입니다.

예를 들어 관리 정책 A를 조직 루트에 연결하는 경우 단지 정책일 뿐입니다. 정책 B도 해당 루트 아래 OU에 연결하는 경우 정책 A는 정책 B의 상위 정책입니다. 정책 B는 정책 A의 하위 정책입니다. 정책 A와 정책 B는 병합되어 OU의 계정에 대한 유효 태그 정책을 생성합니다.

하위 정책

조직 트리에서 상위 정책보다 하위 수준에 연결된 정책입니다.

유효 정책

계정에 적용되는 규칙을 지정하는 최종 단일 정책 문서입니다. 유효 정책은 계정이 상속하는 모든 정책과 계정에 직접 연결된 정책을 집계한 것입니다. 예를 들어 태그 정책을 사용하면 계정에 적용되는 유효 태그 정책을 볼 수 있습니다. 자세한 정보는 유효 태그 정책 보기 섹션을 참조하세요.

상속 연산자

상속된 정책이 단일 유효 정책으로 병합되는 방법을 제어하는 연산자입니다. 이러한 연산자는 고급 기능으로 간주됩니다. 숙련된 정책 작성자는 이러한 연산자를 사용하여 하위 정책이 변경할 수 있는 내용과 정책의 설정이 병합되는 방법을 제한할 수 있습니다. 자세한 내용은 상속 연산자 섹션을 참조하세요.

관리 정책 유형에 대한 정책 구문 및 상속

정책이 해당 정책을 상속하는 OU 및 계정에 미치는 영향은 선택한 관리 정책 유형에 따라 달라집니다. 관리 정책 유형은 다음과 같습니다.

- 인공 지능(AI) 서비스 옵트아웃 정책
- 백업 정책
- 태그 정책

관리 정책 유형의 구문에는 상속 연산자이(가) 포함되어 있습니다. 이 연산자를 사용하면 상위 정책의 어떤 요소가 적용되는지, 그리고 요소가 하위 OU 및 계정에 의해 상속될 때 어떤 요소가 무시되거나 수정될 수 있는지 세밀하게 지정할 수 있습니다.

유효 정책은 조직 루트 및 OU에서 상속되는 규칙과 계정에 직접 연결된 규칙의 집합입니다. 유효 정책은 계정에 적용되는 최종 규칙 집합을 지정합니다. 적용되는 정책의 모든 상속 연산자가 미치는 영향을 포함한 계정의 유효 정책을 볼 수 있습니다. 자세한 내용은 유효 태그 정책 보기 섹션을 참조하세요.

상속 연산자

상속 연산자는 상속된 정책과 계정 정책이 계정의 유효 정책으로 병합되는 방법을 제어합니다. 이러한 연산자에는 값 설정 연산자와 하위 제어 연산자가 포함됩니다.

AWS Organizations 콘솔에서 시각적 편집기를 사용하는 경우 `@@assign` 연산자만 사용할 수 있습니다. 기타 연산자는 고급 기능으로 간주됩니다. 기타 연산자를 사용하려면 JSON 정책을 수동으로 작성해야 합니다. 숙련된 정책 작성자는 상속 연산자를 사용하여 유효 정책에 적용되는 값을 제어하고 하위 정책에 따라 변경할 수 있는 내용을 제한할 수 있습니다.

값 설정 연산자

다음 값 설정 연산자를 사용하여 정책이 상위 정책과 상호 작용하는 방식을 제어할 수 있습니다.

- `@@assign` – 상속된 정책 설정을 지정된 설정으로 덮어씁니다. 지정된 설정이 상속되지 않은 경우 이 연산자는 해당 설정을 유효 정책에 추가합니다. 이 연산자는 모든 유형의 정책 설정에 적용할 수 있습니다.
  - 단일 값 설정의 경우 이 연산자는 상속된 값을 지정된 값으로 바꿉니다.
  - 다중 값 설정(JSON 배열)의 경우 이 연산자는 상속된 값을 모두 제거하고 이 정책에 지정된 값으로 바꿉니다.
- `@@append` – 지정된 설정을 제거하지 않고 상속된 설정에 추가합니다. 지정된 설정이 상속되지 않은 경우 이 연산자는 해당 설정을 유효 정책에 추가합니다. 이 연산자는 다중 값 설정에서만 사용할 수 있습니다.
  - 이 연산자는 상속된 배열의 값에 지정된 값을 추가합니다.
- `@@remove` – 상속된 지정된 설정(있는 경우)을 유효 정책에서 제거합니다. 이 연산자는 다중 값 설정에서만 사용할 수 있습니다.
  - 이 연산자는 상위 정책에서 상속된 값 배열에서 지정된 값만 제거합니다. 다른 값은 배열에 계속 존재할 수 있으며 하위 정책이 상속할 수 있습니다.

하위 제어 연산자

하위 제어 연산자를 사용하는 것은 선택 사항입니다.
`@@operators_allowed_for_child_policies` 연산자를 사용하여 하위 정책에서 사용할 수 있는

값 설정 연산자를 제어할 수 있습니다. 모든 연산자를 허용하거나, 일부 특정 연산자를 허용하거나, 연산자를 허용하지 않을 수 있습니다. 기본적으로 모든 연산자(@@all) 가 허용됩니다.

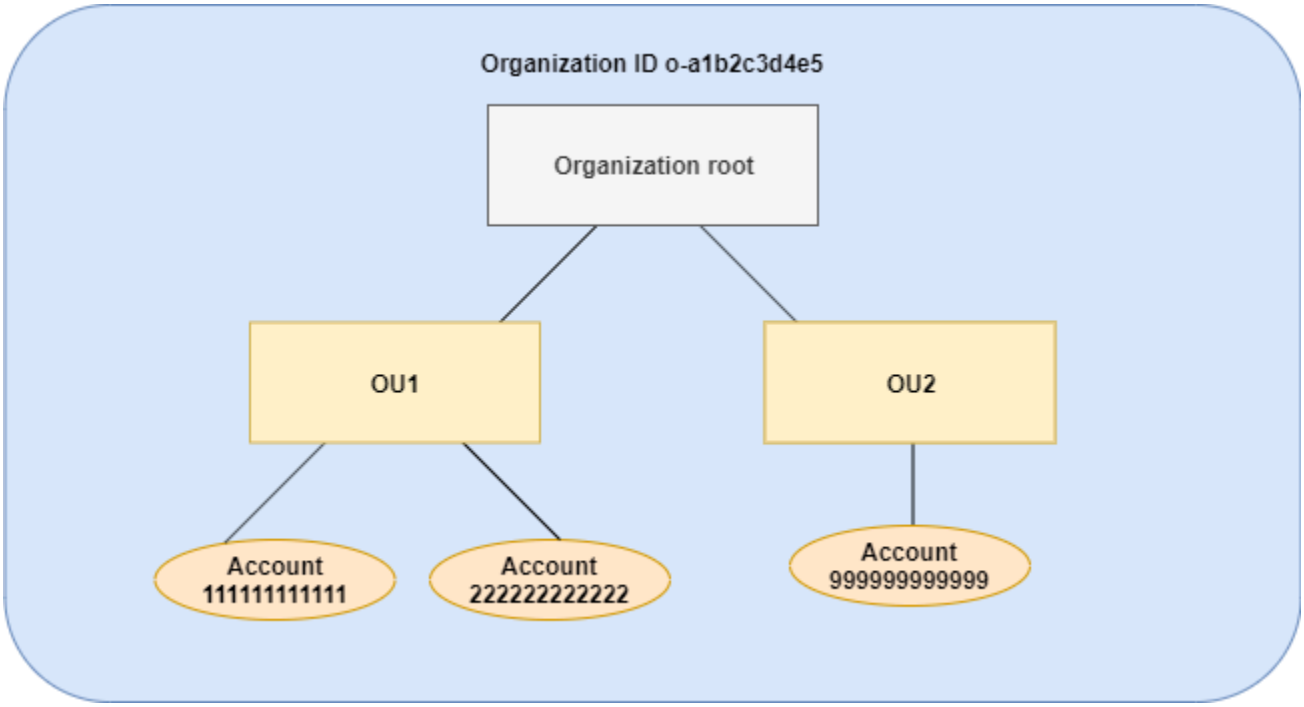
- `"@@operators_allowed_for_child_policies":["@@all"]` – 하위 OU와 계정은 정책에서 어떤 연산자든지 사용할 수 있습니다. 기본적으로 모든 연산자가 하위 정책에서 허용됩니다.
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` – 하위 OU 및 계정은 하위 정책에서 지정된 연산자만 사용할 수 있습니다. 이 하위 제어 연산자에서 값 설정 연산자를 하나 이상 지정할 수 있습니다.
- `"@@operators_allowed_for_child_policies":["@@none"]` – 하위 OU와 계정은 정책에서 연산자를 사용할 수 없습니다. 이 연산자를 사용하여 하위 정책에서 해당 값을 추가, 첨부 또는 제거할 수 없도록 상위 정책에서 정의된 값을 효과적으로 잠글 수 있습니다.

> **Note**
>
> 상속된 하위 제어 연산자가 연산자 사용을 제한하는 경우 하위 정책에서 해당 규칙을 되돌릴 수 없습니다. 상위 정책에 하위 제어 연산자를 포함하면 이러한 연산자는 모든 하위 정책에서 값 설정 연산자를 제한합니다.

상속 사례

다음 예제에서는 상위 및 하위 태그 정책이 계정의 유효 태그 정책으로 병합되는 과정을 설명하여 정책 상속이 작동하는 방식을 보여 줍니다.

이 예에서는 다음 다이어그램에 표시된 조직 구조가 있다고 가정합니다.



예시

- 예제 1: 하위 정책이 태그 값만 덮어쓰도록 허용
- 예제 2: 상속된 태그에 새 값 추가
- 예제 3: 상속된 태그에서 값 제거
- 예제 4: 하위 정책의 변경 제한
- 예제 5: 하위 제어 연산자와 충돌
- 예제 6: 동일한 계층 수준에서 값 추가와 충돌

예제 1: 하위 정책이 태그 값만 덮어쓰도록 허용

다음 태그 정책은 CostCenter 태그 키와 허용 가능한 두 값 Development 및 Support를 정의합니다. 이 태그 정책을 조직 루트에 연결하면 태그 정책은 조직의 모든 계정에 적용됩니다.

정책 A - 조직 루트 태그 정책

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
```

```
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

OU1의 사용자가 키에 다른 태그 값을 사용하도록 하고 특정 리소스 유형에 대해 해당 태그 정책을 적용하려고 한다고 가정합니다. 정책 A는 어떤 하위 제어 연산자가 허용되는지를 지정하지 않으므로 모든 연산자가 허용됩니다. `@@assign` 연산자를 사용하고 다음과 같은 태그 정책을 생성하여 OU1에 연결할 수 있습니다.

정책 B - OU1 태그 정책

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

태그에 대해 `@@assign` 연산자를 지정하면 정책 A와 정책 B가 병합되어 계정의 유효 태그 정책을 형성할 때 다음이 수행됩니다.

- 정책 B는 상위 정책에서 지정된 두 개의 태그 값을 덮어씁니다. 따라서 Sandbox는 CostCenter 태그 키의 유일한 정책 준수 값입니다.
- enforced_for를 추가하면 CostCenter 태그가 모든 Amazon Redshift 리소스와 Amazon DynamoDB 테이블에서 지정된 태그 값을 사용해야 합니다.

그림과 같이 OU1에는 111111111111 및 222222222222라는 두 개의 계정이 포함되어 있습니다.

계정 111111111111 및 222222222222에 대해 생성된 유효 태그 정책

> **Note**
>
> 표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

예제 2: 상속된 태그에 새 값 추가

조직의 모든 계정에서 허용 가능한 값의 짧은 목록이 있는 태그 키를 지정하려는 경우가 있을 수 있습니다. 한 OU에 있는 계정의 경우 리소스를 생성할 때 해당 계정만 지정할 수 있는 추가 값을 허용하려고 할 수 있습니다. 이 예제에서는 @@append 연산자를 사용하여 이 작업을 수행하는 방법을 설명합니다. @@append 연산자는 고급 기능입니다.

예제 1과 마찬가지로, 이 예제는 조직 루트 태그 정책에 대한 정책 A로 시작합니다.

정책 A - 조직 루트 태그 정책

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

이 예제에서는 정책 C를 OU2에 연결합니다. 이 예제의 차이점은 정책 C에서 @@append 연산자를 사용할 경우 허용 값 목록과 enforced_for 규칙을 덮어쓰지 않고 해당 항목에 추가한다는 것입니다.

정책 C - 값을 추가하기 위한 OU2 태그 정책

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
```

```
}
```

정책 C를 OU2에 연결하면 정책 A와 정책 C가 병합되어 계정의 유효 태그 정책을 형성할 때 다음과 같은 효과가 발생합니다.

- 정책 C에는 @@append 연산자가 포함되어 있으므로 이 정책은 정책 A에서 지정된 허용 가능한 태그 값의 목록을 덮어쓰지 않고 이 목록에 값을 추가하도록 허용 합니다.
- 정책 B와 같이, enforced_for를 추가하면 CostCenter 태그가 모든 Amazon Redshift 리소스와 Amazon DynamoDB 테이블에서 지정된 태그 값으로 사용되어야 합니다. 상위 정책에 하위 정책이 지정할 수 있는 항목을 제한하는 하위 제어 연산자가 포함되지 않으면 덮어쓰기(@@assign)와 추가(@@append)는 동일한 효과를 나타냅니다.

다이어그램과 같이 OU2에는 999999999999라는 계정 하나가 포함되어 있습니다. 정책 A와 정책 C가 병합되어 계정 999999999999에 대한 유효 태그 정책을 생성합니다.

계정 999999999999에 대한 유효 태그 정책

> **Note**
>
> 표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
                "Support",
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
```

```
}
```

예제 3: 상속된 태그에서 값 제거

조직에 연결된 태그 정책이 계정에서 사용하려는 것보다 더 많은 태그 값을 정의하는 경우가 있을 수 있습니다. 이 예에서는 `@@remove` 연산자를 사용하여 태그 정책을 수정하는 방법을 설명합니다. `@@remove`는 고급 기능입니다.

다른 예제와 마찬가지로, 이 예제는 조직 루트 태그 정책에 대한 정책 A로 시작합니다.

정책 A - 조직 루트 태그 정책

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

이 예제에서는 계정 999999999999에 정책 D를 연결합니다.

정책 D - 값을 제거하는 계정 999999999999 태그 정책

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
```

```
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

정책 D를 계정 9999999999999에 연결하면 정책 A, 정책 C 및 정책 D가 병합되어 유효 태그 정책을 형성할 때 다음과 같은 효과가 발생합니다.

- 이전의 예제를 모두 수행했다고 가정하면 정책 B, C 및 C는 A의 하위 정책입니다. 정책 B는 OU1에만 연결되므로 계정 9999999999999에 영향을 미치지 않습니다.
- 계정 9999999999999의 경우 `CostCenter` 태그 키에 허용 가능한 유일한 값은 `Support`입니다.
- 정책 준수는 `CostCenter` 태그 키에 적용되지 않습니다.

계정 9999999999999에 대한 새로운 유효 태그 정책

> **Note**
>
> 표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

나중에 OU2에 계정을 더 추가하는 경우 해당 계정의 유효 태그 정책은 계정 999999999999와 다릅니다. 더 제한적인 정책 D는 계정 수준에서만 연결되고 OU에는 연결되지 않기 때문입니다.

예제 4: 하위 정책의 변경 제한

하위 정책의 변경을 제한하려는 경우가 있을 수 있습니다. 이 예제에서는 하위 제어 연산자를 사용하여 이 작업을 수행하는 방법에 대해 설명합니다.

이 예제에서는 새 조직 루트 태그 정책으로 시작하며 태그 정책이 조직 엔터티에 아직 연결되어 있지 않다고 가정합니다.

정책 E - 하위 정책의 변경을 제한하는 조직 루트 태그 정책

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

조직 루트에 정책 E를 연결하면 하위 정책이 `Project` 태그 키를 변경할 수 없습니다. 하지만 하위 정책은 태그 값을 덮어쓰거나 추가할 수 있습니다.

그런 다음 OU에 다음과 같은 정책 F를 연결한다고 가정합니다.

정책 F - OU 태그 정책

```
{
    "tags": {
        "project": {
            "tag_key": {
```

```
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

정책 E와 정책 F를 병합하면 OU의 계정에 다음과 같은 영향을 미칩니다.

- 정책 F는 정책 E의 하위 정책입니다.
- 정책 F는 사례 처리를 변경하려고 시도하지만 그렇게 할 수 없습니다. 정책 E에는 태그 키에 대한 `"@@operators_allowed_for_child_policies": ["@@none"]` 연산자가 포함되어 있기 때문입니다.
- 하지만 정책 F는 키의 태그 값을 추가할 수 있습니다. 정책 E에는 태그 값에 대한 `"@@operators_allowed_for_child_policies": ["@@append"]`가 포함되어 있기 때문입니다.

OU의 계정에 대한 유효 정책

> **Note**
>
> 표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
```

```
        }
    }
}
```

예제 5: 하위 제어 연산자와 충돌

하위 제어 연산자는 조직 계층의 동일한 수준에서 연결된 태그 정책에 존재할 수 있습니다. 이러한 경우 정책이 병합되어 계정의 유효 정책을 형성할 때 허용된 연산자의 교집합이 사용됩니다.

정책 G와 정책 H가 조직 루트에 연결되어 있다고 가정합니다.

정책 G - 조직 루트 태그 정책 1

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

정책 H - 조직 루트 태그 정책 2

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

이 예제에서 조직 루트에 있는 한 정책은 태그 키의 값을 추가만 할 수 있도록 정의합니다. 조직 루트에 연결된 다른 정책은 하위 정책이 값을 추가하고 제거할 수 있도록 허용합니다. 이러한 두 가지 권한의 교집합이 하위 정책에 사용됩니다. 결과적으로 하위 정책은 값을 추가할 수 있지만 값을 제거할 수 없

습니다. 따라서 하위 정책은 태그 값 목록에 값을 추가할 수 있지만 Maintenance 값을 제거할 수 없습니다.

예제 6: 동일한 계층 수준에서 값 추가와 충돌

각 조직 엔터티에 여러 태그 정책을 연결할 수 있습니다. 이렇게 하면 동일한 조직 엔터티에 연결된 태그 정책에 충돌하는 정보가 포함될 수 있습니다. 정책은 조직 엔터티에 연결된 순서를 기준으로 평가됩니다. 어떤 정책이 먼저 평가되는지를 변경하려면 정책을 분리한 다음 다시 연결하면 됩니다.

정책 J가 조직 루트에 먼저 연결된 다음, 정책 K가 조직 루트에 연결된다고 가정합니다.

정책 J - 조직 루트에 연결된 첫 번째 태그 정책

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

정책 K - 조직 루트에 연결된 두 번째 태그 정책

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

이 예제에서는 태그 키를 정의한 정책이 조직 루트에 먼저 연결되었기 때문에 유효 태그 정책에서 태그 키 PROJECT가 사용됩니다.

정책 JK - 계정의 유효 태그 정책

계정의 유효 정책은 다음과 같습니다.

> **Note**
>
> 표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

AI 서비스 옵트아웃 정책

Amazon Rekognition, Amazon CodeWhisperer, Amazon Transcribe, Amazon Connect용 콘택트 렌즈와 같은 AWS 인공 지능(AI) 서비스는 다른 AWS 서비스를 개발하고 지속적으로 개선하기 위해 해당 서비스에서 처리되는 고객 콘텐츠를 저장하고 사용할 수 있습니다. AWS 고객은 서비스 개선을 위해 자신의 콘텐츠가 저장, 사용되지 않도록 옵트아웃할 수 있습니다.

> **Note**
>
> AWS 인공 지능(AI) 서비스는 사용자가 서비스 개선을 위한 AWS의 데이터 사용을 옵트아웃한 경우에도 데이터를 저장해야 할 수 있습니다. 자세한 내용은 사용 중인 AI 서비스의 설명서를 참조하세요.

조직에서 사용하는 각 AWS 계정에 대해 이 설정을 개별적으로 구성하는 대신 조직의 멤버인 모든 계정에 대해 설정 선택을 적용하는 조직 정책을 구성할 수 있습니다. 개별 AI 서비스의 콘텐츠 저장 및 사용을 옵트아웃하거나 적용되는 서비스 모두에 대해 한 번에 옵트아웃하도록 선택할 수 있습니다. 각 계정에 적용되는 유효 정책을 쿼리하여 설정 선택의 효과를 확인할 수 있습니다.

Important

- 서비스에 대해 옵트인 또는 옵트아웃 기본 설정을 지정하면 해당 설정은 전역 설정으로서, 모든 AWS 리전에 적용됩니다. 한 AWS 리전 내에서 값을 설정하면 다른 모든 리전에 복제됩니다.
- AWS AI 서비스의 콘텐츠 사용을 옵트아웃하면 해당 서비스는 이 옵션을 설정하기 전에 AWS와 공유했던 과거의 관련된 콘텐츠를 모두 삭제합니다. 이 삭제는 서비스 기능을 제공하는 데 필요하지 않은 저장된 데이터로 제한되어야 합니다.

AI 서비스 옵트아웃 정책 시작하기

다음 단계에 따라 인공 지능(AI) 서비스 옵트아웃 정책을 시작합니다.

1. 조직에 대해 AI 서비스 옵트아웃 정책을 활성화합니다.
2. AI 서비스 옵트아웃 정책을 만듭니다.
3. AI 서비스 옵트아웃 정책을 조직의 루트, OU 또는 계정에 연결합니다.
4. 계정에 적용되는 결합된 유효 AI 서비스 옵트아웃 정책을 확인합니다.

위의 모든 단계를 수행하려면 조직의 관리 계정에서 AWS Identity and Access Management(IAM) 사용자로 로그인하거나, IAM 역할을 맡거나, 루트 사용자로 로그인(권장되지 않음)합니다.

기타 정보

- AI 서비스 옵트아웃 정책에 대한 정책 구문 알아보기 및 정책 예제 보기

AI 서비스 옵트아웃 정책의 생성, 업데이트, 삭제

이 주제에서 수행할 작업

- 조직에 대해 AI 서비스 옵트아웃 정책을 활성화한 후에 정책을 생성할 수 있습니다.
- 옵트아웃 요구 사항이 변경되면 기존 정책을 업데이트할 수 있습니다.
- 정책이 더 이상 필요하지 않은 경우 모든 조직 단위(OU) 및 계정에서 정책을 분리한 후 삭제할 수 있습니다.

AI 서비스 옵트아웃 정책 만들기

> **최소 권한**
>
> AI 서비스 옵트아웃 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.
>
> - `organizations:CreatePolicy`

AWS Management Console

AI 서비스 옵트아웃 정책을 만들려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AI 서비스 옵트아웃 정책(AI services opt-out policies) 페이지에서 정책 생성(Create policy)을 선택합니다.
3. 새 AI 서비스 옵트아웃 정책 생성(Create new AI services opt-out policy) 페이지에서 정책 이름과 정책 설명을 입력합니다. 정책 설명은 선택 사항입니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 `null`이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 정보는 AWS Organizations 리소스에 태그 지정을 참조하세요.
5. JSON 탭에 정책 텍스트를 입력하거나 붙여 넣습니다. AI 서비스 옵트아웃 정책 구문에 대한 자세한 내용은 AI 서비스 옵트아웃 정책 구문 및 예제 단원을 참조하세요. 시작점으로 사용할 수 있는 정책 예제를 보려면 AI 서비스 옵트아웃 정책 예제 단원을 참조하세요.
6. 정책 편집을 마쳤으면 페이지의 오른쪽 아래 모서리에 있는 정책 생성(Create policy)을 선택합니다.

AWS CLI & AWS SDKs

AI 서비스 옵트아웃 정책을 만들려면

다음 중 하나를 사용하여 태그 정책을 생성할 수 있습니다.

- AWS CLI: create-policy

1. 다음과 같은 AI 서비스 옵트아웃 정책을 작성하여 텍스트 파일에 저장합니다. “optOut“과 “optIn“는 대소문자를 구분합니다.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

이 AI 서비스 옵트아웃 정책은 정책의 영향을 받는 모든 계정이 Amazon Rekognition을 제외한 모든 AI 서비스에서 옵트아웃되도록 지정합니다.

2. JSON 정책 파일을 가져와 조직에 새 정책을 생성합니다. 이 예제에서 이전 JSON 파일의 이름은 policy.json이었습니다.

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
```

```
    }
}
```

- AWS SDK: CreatePolicy

다음에 수행할 작업

AI 서비스 옵트아웃 정책을 생성한 후 옵트아웃 옵션을 적용할 수 있습니다. 이를 위해 조직 루트, 조직 단위(OU), 조직 내 AWS 계정, 또는 이들의 조합에 정책을 연결할 수 있습니다.

AI 서비스 옵트아웃 정책 업데이트

> 최소 권한
>
> AI 서비스 옵트아웃 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 `Resource` 요소를 가진 `organizations:UpdatePolicy`
> - 동일한 정책 명령문에서 지정된 정책의 Amazon Resource Name(ARN)(또는 "*")을 포함하는 `Resource` 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

AI 서비스 옵트아웃 정책을 업데이트하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AI 서비스 옵트아웃 정책(AI services opt-out policies) 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책의 세부 정보 페이지에서 정책 편집(Edit policy)을 선택합니다.
4. 새 정책 이름, 정책 설명을 입력하거나, JSON 정책 텍스트를 편집할 수 있습니다. AI 서비스 옵트아웃 정책 구문에 대한 자세한 내용은 AI 서비스 옵트아웃 정책 구문 및 예제 단원을 참조하세요. 시작점으로 사용할 수 있는 정책 예제를 보려면 AI 서비스 옵트아웃 정책 예제 단원을 참조하세요.
5. 백업 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

다음 중 하나를 사용하여 정책을 업데이트할 수 있습니다.

- AWS CLI: update-policy

  다음 예제에서는 AI 서비스 옵트아웃 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

  다음 예제에서는 AI 서비스 옵트아웃 정책에 대한 설명을 추가하거나 변경합니다.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
```

```
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

다음 예제에서는 AI 서비스 옵트아웃 정책에 연결된 JSON 정책 문서를 변경합니다. 이 예제에서 콘텐츠는 다음 텍스트를 포함한 `policy.json`이라는 파일에서 가져옵니다.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
```

```
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"    ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n"}
}
```

- AWS SDK: UpdatePolicy

AI 서비스 옵트아웃 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하면 AI 서비스 옵트아웃 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요AWS Organizations 리소스에 태그 지정

최소 권한

AWS 조직의 AI 서비스 옵트아웃 정책에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:DescribePolicy` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

AI 서비스 옵트아웃 정책에 연결된 태그를 편집하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AI 서비스 옵트아웃 정책(AI services opt-out policies) 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 선택한 정책의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.

- 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
- 제거(Remove)를 선택하여 기존 태그를 제거합니다.
- 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 `null`이 아닌 빈 문자열이 됩니다.

5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

AI 서비스 옵트아웃 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 AI 서비스 옵트아웃 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: tag-resource 및 untag-resource
- AWS SDK: TagResource 및 UntagResource

AI 서비스 옵트아웃 정책 삭제

조직의 관리 계정에 로그인하면 조직에서 더 이상 필요 없는 정책을 삭제할 수 있습니다.

정책을 삭제하기 전에 먼저 연결된 모든 개체에서 정책을 분리해야 합니다.

> 최소 권한
>
> 백업 정책을 삭제하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - `organizations:DescribePolicy`(콘솔만 해당 - 정책으로 이동하기 위해)
> - `organizations:DeletePolicy`

AWS Management Console

AI 서비스 옵트아웃 정책을 삭제하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. AI 서비스 옵트아웃 정책(AI services opt-out policies) 페이지에서 삭제할 정책의 이름을 선택합니다.
3. 먼저 모든 루트, OU, 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제(Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제(Delete)를 선택합니다.

AWS CLI & AWS SDKs

AI 서비스 옵트아웃 정책을 삭제하려면

다음 중 하나를 사용하여 정책을 삭제할 수 있습니다.

- AWS CLI: delete-policy

  다음은 지정된 정책을 삭제하는 예제입니다. 정책이 루트, OU 또는 계정에 연결되지 않은 경우에만 작동합니다.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: DeletePolicy

AI 서비스 옵트아웃 정책 연결 및 분리

전체 조직뿐 아니라 OU(조직 단위) 및 개별 계정에서도 인공 지능(AI) 서비스 옵트아웃 정책을 사용할 수 있습니다. AI 서비스 옵트아웃 정책이 적용되는 대상은 정책을 연결하는 조직 요소에 따라 다릅니다.

- AI 서비스 옵트아웃 정책을 조직 루트에 연결하면 정책은 해당 루트의 모든 멤버 OU 및 계정에 모두 적용됩니다.
- AI 서비스 옵트아웃 정책을 OU에 연결하면 해당 정책은 OU 또는 해당 자식 OU에 속한 계정에 적용됩니다. 이러한 계정에는 조직 루트에 연결된 정책이 모두 적용됩니다.

- AI 서비스 옵트아웃 정책을 계정에 연결하면 정책이 해당 계정에만 적용됩니다. 또한 계정에는 조직 루트 및 해당 계정이 속한 OU에 연결된 정책이 적용됩니다.

계정이 루트 및 상위 OU로부터 상속하는 AI 서비스 옵트아웃 정책과 계정에 직접 연결된 모든 정책의 집계가 유효 정책입니다. 정책이 유효 정책에 병합되는 방법에 대한 자세한 내용은 관리 정책 상속에 대한 이해 단원을 참조하세요.

> 최소 권한
>
> AI 서비스 옵트아웃 정책을 연결하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - `organizations:AttachPolicy`

AWS Management Console

정책을 탐색하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 AI 서비스 옵트아웃 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 AI 서비스 옵트아웃 정책을 연결하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책(Policies) 탭의 AI 서비스 옵트아웃 정책에 대한 항목에서 연결(Attach)을 선택합니다.
4. 원하는 정책을 찾아 정책 연결(Attach policy)을 선택합니다.

   정책(Policies) 탭의 연결된 AI 서비스 옵트아웃 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 AI 서비스 옵트아웃 정책을 연결하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. AI 서비스 옵트아웃 정책(AI services opt-out policies) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
5. 정책 연결(Attach policies)을 선택합니다.

   대상(Targets) 탭의 연결된 AI 서비스 옵트아웃 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

AWS CLI & AWS SDKs

AI 서비스 옵트아웃 정책을 조직 루트, OU 또는 계정에 연결하려면

다음 중 하나를 사용하여 AI 서비스 옵트아웃 정책을 연결할 수 있습니다.

- AWS CLI: attach-policy

  다음 예제에서는 정책을 OU에 연결합니다.

```
$ aws organizations attach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: AttachPolicy

정책 변경은 즉시 적용됩니다.

AI 서비스 옵트아웃 정책 분리

조직의 관리 계정에 로그인하면 연결된 조직 루트, OU 또는 계정에서 AI 서비스 옵트아웃 정책을 분리할 수 있습니다. 엔터티에서 AI 서비스 옵트아웃 정책을 분리하면 해당 정책은 현재 분리된 엔터티의 영향을 받던 모든 계정에 더 이상 적용되지 않습니다. 정책을 분리하려면 다음 단계를 완료하세요.

최소 권한

조직 루트, OU 또는 계정에서 AI 서비스 옵트아웃 정책을 분리하려면 다음 작업을 실행할 권한이 있어야 합니다.

- `organizations:DetachPolicy`

AWS Management Console

정책으로 이동하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 AI 서비스 옵트아웃 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 AI 서비스 옵트아웃 정책을 분리하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책(Policies) 탭에서, 분리할 AI 서비스 옵트아웃 정책 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

   연결된 AI 서비스 옵트아웃 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 AI 서비스 옵트아웃 정책을 분리하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AI 서비스 옵트아웃 정책(AI services opt-out policies) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).

4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

   연결된 AI 서비스 옵트아웃 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

AWS CLI & AWS SDKs

조직 루트, OU 또는 계정에서 AI 서비스 옵트아웃 정책을 분리하려면

다음 중 하나를 사용하여 AI 서비스 옵트아웃 정책을 분리할 수 있습니다.

- AWS CLI: detach-policy

  다음 예제에서는 OU로부터 정책을 분리합니다.

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: DetachPolicy

정책 변경은 즉시 적용됩니다.

유효 AI 서비스 옵트아웃 정책 보기

조직의 계정에 대한 유효 인공 지능(AI) 서비스 옵트아웃 정책을 결정합니다.

유효 AI 서비스 옵트아웃 정책이란 무엇입니까?

유효 AI 서비스 옵트아웃 정책은 AWS 계정에 적용되는 최종 규칙을 지정합니다. 이는 계정이 상속하는 모든 AI 서비스 옵트아웃 정책과 계정에 직접 연결된 AI 서비스 옵트아웃 정책을 집계한 것입니다. AI 서비스 옵트아웃 정책을 조직의 루트에 연결하면 해당 정책은 조직의 모든 계정에 적용됩니다. AI 서비스 옵트아웃 정책을 OU에 연결하면 해당 정책은 OU에 속한 모든 계정 및 OU에 적용됩니다. 정책을 계정에 직접 연결하면 정책이 해당 AWS 계정에만 적용됩니다.

예를 들어 조직 루트에 연결된 AI 서비스 옵트아웃 정책은 조직의 모든 계정이 모든 AWS 기계 학습 서비스에 의한 콘텐츠 사용을 옵트아웃하도록 지정할 수 있습니다. 여기서, 한 멤버 계정에 직접 연결된

개별적 AI 서비스 옵트아웃 정책이 Amazon Rekognition에 대해서만 콘텐츠 사용을 옵트인하도록 지정되어 있습니다. 이 AI 서비스 옵트아웃 정책들의 조합이 유효 AI 서비스 옵트아웃 정책을 구성하고 있습니다. 이 정책의 결과로, Amazon Rekognition에 옵트인한 하나의 계정을 제외하고 조직의 모든 계정이 모든 AWS 서비스에서 옵트아웃됩니다.

AI 서비스 옵트아웃 정책이 최종 유효 정책으로 결합되는 방식에 대한 자세한 내용은 관리 정책 상속에 대한 이해 단원을 참조하세요.

유효 AI 서비스 옵트아웃 정책을 보는 방법

AWS Management Console, AWS API 또는 AWS Command Line Interface에서 계정에 대한 유효 AI 서비스 옵트아웃 정책을 볼 수 있습니다.

> 최소 권한
>
> 계정에 대한 유효 AI 서비스 옵트아웃 정책을 보려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

계정에 대한 유효 AI 서비스 옵트아웃 정책을 보는 방법

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 유효 AI 서비스 옵트아웃 정책을 보려는 계정의 이름을 선택합니다. 원하는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책 탭의 AI 서비스 옵트아웃 정책 섹션에서 이 AWS 계정에 대한 유효 AI 정책 보기를 선택합니다.

   지정한 계정에 적용되는 유효 정책이 콘솔에 표시됩니다.

> **Note**
>
> 중요한 변경 없이 유효 정책을 복사하여 붙여넣고 다른 AI 서비스 옵트아웃 정책의 JSON으로 사용할 수는 없습니다. AI 서비스 옵트아웃 정책 문서에는 각 설정이 최종 유효 정책으로 병합되는 방법을 지정하는 상속 연산자가 포함되어야 합니다.

AWS CLI & AWS SDKs

계정에 대한 유효 AI 서비스 옵트아웃 정책을 보려면

다음 중 하나를 사용하여 유효 AI 서비스 옵트아웃 정책을 볼 수 있습니다.

- AWS CLI: describe-effective-policy

  다음 예제에서는 계정에 대한 유효 AI 서비스 옵트아웃 정책을 보여 줍니다.

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWS SDK: DescribeEffectivePolicy

AI 서비스 옵트아웃 정책 구문 및 예제

이 주제에서는 AI(인공 지능) 서비스 옵트아웃 정책 구문에 대해 설명하고 예제를 제공합니다.

AI 서비스 옵트아웃 정책의 구문

AI 서비스 옵트아웃 정책은 JSON 규칙에 따라 구성된 일반 텍스트 파일입니다. AI 서비스 옵트아웃 정책 구문은 관리 정책 유형에 대한 구문을 따릅니다. 해당 구문에 대한 자세한 내용은 관리 정책 상속에

대한 이해 단원을 참조하세요. 이 주제에서는 AI 서비스 옵트아웃 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 방법을 중점적으로 설명합니다.

> **Important**
>
> 이 섹션에 설명된 값의 대소문자 사용은 중요합니다. 이 주제에 제시된 대로 대문자와 소문자로 값을 입력해야 합니다. 잘못된 대소문자를 사용하면 정책이 작동하지 않습니다.

다음 정책은 기본적인 AI 서비스 옵트아웃 정책 구문을 보여 줍니다. 이 예제를 계정에 직접 연결하면 해당 계정은 한 서비스를 명시적으로 옵트아웃하고 다른 한 서비스에는 옵트인합니다. 다른 서비스들은 상위 수준(OU 또는 루트 정책)으로부터 상속된 정책에 의해 옵트인되거나 옵트아웃될 수 있습니다.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

다음은 조직의 루트에 연결된 정책의 예입니다. 이 예제는 조직에서 모든 AI 서비스를 옵트아웃하는 기본값을 설정합니다. 여기에는 명시적으로 제외되지 않은 한 AWS 가 향후 배포할 수 있는 모든 AI 서비스를 비롯해 모든 AI 서비스가 자동으로 포함됩니다. 하위 정책을 OU에 연결하거나 계정에 직접 연결하여 Amazon Comprehend를 제외한 모든 AI 서비스에 대해 이 설정을 재정의할 수 있습니다. 다음 예제의 두 번째 항목은 `@@operators_allowed_for_child_policies`를 `none`으로 설정하여 설정이 재정의되지 않도록 합니다. 예제의 세 번째 항목은 Amazon Rekognition에 대해 조직 전체를 제외합니다. 이에 따라 전체 조직이 해당 서비스를 옵트인합니다. 그러나 적절한 경우 해당 정책은 하위 정책의 재정의를 허용합니다.

```
{
    "services": {
        "default": {
```

```
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

AI 서비스 옵트아웃 정책 구문에는 다음 요소가 포함됩니다.

- `services` 요소. AI 서비스 옵트아웃 정책은 이 고정 이름에 의해 가장 바깥쪽 JSON 포함 요소로 식별됩니다.

  AI 서비스 옵트아웃 정책은 `services` 요소에 하나 이상의 문을 가질 수 있습니다. 각 문에는 다음 요소가 포함됩니다.

  - AWS AI 서비스를 식별하는 서비스 이름 키입니다. 다음의 키 이름은 이 필드에 유효한 값입니다.
    - **`default`** – 현재 사용 가능한 모든 AI 서비스를 나타내며, 향후 추가될 수 있는 AI 서비스를 묵시적으로 자동 포함시킵니다.
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`
    - `codeguruprofiler`
    - `codewhisperer`
    - `comprehend`
    - `connectamd`
    - `connectoptimization`
    - `contactlens`

- datazone
- entityresolution
- frauddetector
- glue
- guardduty
- lex
- polly
- q
- quicksightq
- rekognition
- securitylake
- textract
- transcribe
- translate

서비스 이름 키로 식별되는 각 정책 문에는 다음 요소가 포함될 수 있습니다.

- opt_out_policy 키. 이 키는 반드시 있어야 합니다. 이 키는 서비스 이름 키 아래에 배치할 수 있는 유일한 키입니다.

  opt_out_policy 키는 다음 값 중 하나를 가진 @@assign 연산자만 포함할 수 있습니다

  - optOut - 지정된 AI 서비스의 콘텐츠 사용을 옵트아웃하도록 선택합니다.
  - optIn - 지정된 AI 서비스의 콘텐츠 사용을 옵트인하도록 선택합니다.

  > **참고**
  >
  > - @@append 및 @@remove 상속 연산자는 AI 서비스 옵트아웃 정책에 사용할 수 없습니다.
  > - @@enforced_for 연산자는 AI 서비스 옵트아웃 정책에 사용할 수 없습니다.

- 어떤 레벨에서든 @@operators_allowed_for_child_policies 연산자를 지정하면 상위 정책에서 부과한 설정을 재정의하기 위해 하위 정책이 실행할 수 있는 동작을 제어할 수 있습니다. 다음 값 중 하나를 지정할 수 있습니다.
  - @@assign – 해당 정책의 하위 정책이 @@assign 연산자를 사용하여 상속된 값을 다른 값으로 재정의할 수 있습니다.

- @@none - 해당 정책의 하위 정책이 값을 변경할 수 없습니다.

@@operators_allowed_for_child_policies가 동작하는 방식은 배치하는 위치에 따라 다릅니다. 다음의 위치를 사용할 수 있습니다.

- services 키 아래에 배치 - 하위 정책이 유효 정책의 서비스 목록을 추가하거나 변경할 수 있는지 여부를 제어합니다.
- 특정 AI 서비스 또는 default 키에 대한 키 아래에 배치 - 하위 정책이 이 특정 항목 아래의 키 목록에 키를 추가하거나 키 목록을 변경할 수 있는지 여부를 제어합니다.
- 특정 서비스에 대한 opt_out_policies 키 아래에 배치 - 하위 정책이 이 특정 서비스에 대한 설정만을 변경할 수 있는지 여부를 제어합니다.

AI 서비스 옵트아웃 정책 예제

다음 정책 예제는 정보 제공 용도로만 제공됩니다.

예제 1: 조직의 모든 계정에 대해 모든 AI 서비스를 옵트아웃

다음 예제에서는 조직의 루트에 연결하여 조직의 계정에 대해 AI 서비스를 옵트아웃할 수 있는 정책을 보여 줍니다.

> **Tip**
>
> 예제의 오른쪽 위 모서리에 있는 복사 버튼을 사용하여 다음 예제를 복사하면 복사본에 행 번호가 포함되지 않습니다. 붙여 넣을 준비가 되었습니다.

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] – "@@operators_allowed_for_child_policies": ["@@none"]를 services 아래에 배치하면 모든 하위 정책이 이미 존재하는 default 섹션 외에 개별 서비스의 새 섹션을 추가하지 못합니다. Default는 “모든 AI 서비스”를 나타내는 자리표시자입니다.
- [2] – "@@operators_allowed_for_child_policies": ["@@none"]를 default 아래에 배치하면 모든 하위 정책이 이미 존재하는 opt_out_policy 섹션 외에 개별 서비스에 대한 새 섹션을 추가하지 못합니다.
- [3] - "@@operators_allowed_for_child_policies": ["@@none"]를 opt_out_policy 아래에 배치하면 하위 정책이 optOut 설정의 값을 변경하거나 다른 설정을 추가하지 못합니다.

예제 2: 모든 서비스에 대해 조직 기본 설정을 설정하되 하위 정책이 개별 서비스에 대한 설정을 재정의할 수 있도록 허용

다음 정책 예제는 모든 AI 서비스에 대해 조직 전반의 기본값을 설정합니다. 값이 default이면 하위 정책이 서비스 default(모든 AI 서비스에 대한 자리표시자)의 optOut 값을 변경하지 못합니다. 이 정책을 루트 또는 OU에 연결하여 상위 정책으로 적용하더라도 하위 정책은 두 번째 정책에서처럼 개별 서비스에 대한 옵트아웃 설정을 변경할 수 있습니다.

- services 키 아래에 "@@operators_allowed_for_child_policies": ["@@none"]가 없으므로 하위 정책이 개별 서비스에 대한 새 섹션을 추가할 수 있습니다.
- "@@operators_allowed_for_child_policies": ["@@none"]를 default 아래에 배치하면 모든 하위 정책이 이미 존재하는 opt_out_policy 섹션 외에 새 섹션을 추가하지 못합니다.
- "@@operators_allowed_for_child_policies": ["@@none"]를 opt_out_policy 아래에 배치하면 하위 정책이 optOut 설정의 값을 변경하거나 다른 설정을 추가하지 못합니다.

조직 루트 사용자AI 서비스 옵트아웃 상위 정책

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

다음 정책 예제는 앞의 정책 예제가 조직 루트 또는 상위 OU에 연결되며 이 예제를 상위 정책의 영향을 받는 계정에 연결한다고 가정합니다. 이 정책은 기본 옵트아웃 설정을 재정의하고 Amazon Lex 서비스만 명시적으로 옵트인합니다.

AI 서비스 옵트아웃 하위 정책

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

이에 대한 효과적인 정책은 상위 정책에서 상속된 옵트아웃 설정으로 인해 계정이 Amazon Lex만 옵트인하고 다른 모든 AWS AI 서비스는 `default` 옵트아웃하는 것입니다. AWS 계정

예제 3: 한 서비스에 대해 조직 전체의 AI 서비스 옵트아웃 정책 정의

다음 예제에서는 하나의 AI 서비스에 대해 `optOut` 설정을 정의하는 AI 서비스 옵트아웃 정책을 보여 줍니다. 이 정책이 조직의 루트에 연결되면 하위 정책이 해당 서비스에 대한 `optOut` 설정을 재정의할 수 없습니다. 다른 서비스는 이 정책으로 처리되지 않지만 다른 OU 또는 계정의 하위 정책이 영향을 미칠 수 있습니다.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

백업 정책

AWS Backup을 사용하면 백업 계획을 작성해 AWS 리소스를 백업하는 방법을 정의할 수 있습니다. 계획의 규칙에는 백업 빈도, 백업이 수행되는 기간, 백업할 리소스가 있는 AWS 리전, 백업을 저장할 볼

트와 같은 다양한 설정이 포함됩니다. 그런 다음 태그를 사용하여 식별된 AWS 리소스 그룹에 백업 계획을 적용할 수 있습니다. 또한 사용자를 대신하여 백업 작업을 수행할 AWS Backup 권한을 부여하는 AWS Identity and Access Management(IAM) 역할도 식별해야 합니다.

AWS Organizations의 백업 정책은 이러한 부분을 모두 JSON 텍스트 문서로 결합합니다. 정의된 백업 정책은 조직의 구조에 존재하는 모든 요소(루트, 조직 단위(OU), 개별 계정 등)에 연결할 수 있습니다. Organizations는 상속 규칙을 적용하여 조직의 루트, 상위 OU 또는 계정에 연결된 정책을 결합합니다. 이렇게 하면 각 계정에 대해 유효 백업 정책이 생성됩니다. 이 유효 정책은 AWS Backup에 AWS 리소스를 자동으로 백업하는 방법을 지시합니다.

백업 정책을 사용하면 조직에 필요한 수준의 리소스 백업을 세부적으로 제어할 수 있습니다. 예를 들어 조직의 루트에 연결된 정책에서 모든 Amazon DynamoDB 테이블을 백업하도록 지정할 수 있습니다. 이 정책에는 기본 백업 빈도가 포함될 수 있습니다. 그런 다음 각 OU의 요구 사항에 따라 백업 빈도를 재정의하는 백업 정책을 OU에 연결할 수 있습니다. 예를 들어 `Developers` OU는 백업 빈도를 일주일에 한 번으로 지정하고 `Production` OU는 하루에 한 번으로 지정할 수 있습니다.

리소스를 성공적으로 백업하는 데 필요한 정보의 일부만 개별적으로 포함하는 부분 백업 정책을 생성할 수 있습니다. 하위 수준 OU 및 계정에서 이러한 부분 정책을 상속하도록 루트 또는 상위 OU와 같은 조직 트리의 다양한 부분에 이러한 정책을 연결할 수 있습니다. Organizations가 상속 규칙을 사용하여 계정에 대한 모든 정책을 결합하는 경우 최종 유효 정책은 필수 요소를 모두 포함해야 합니다. 그렇지 않으면 AWS Backup은 정책이 유효하지 않은 것으로 간주하여 영향을 받는 리소스를 백업하지 않습니다.

> **Important**
>
> AWS Backup은 필수 요소가 모두 포함된 완전한 유효 정책에 의해 호출된 경우에만 성공적인 백업을 수행할 수 있습니다.
> 앞서 설명한 부분 정책 전략이 작동할 수 있지만 계정에 대한 유효 정책이 불완전하면 오류가 발생하거나 리소스가 백업되지 않습니다. 대체 전략으로 모든 백업 정책이 자체적으로 완전하고 유효하도록 요구하는 것이 좋습니다. 상위 계층에 연결된 정책에서 제공하는 기본값을 사용하고 상속 하위 제어 연산자를 포함하여 하위 정책에서 필요에 따라 재정의합니다.

조직의 각 AWS 계정에 대한 유효 백업 계획은 AWS Backup 콘솔에 해당 계정에 대한 변경 불가능한 계획으로 표시됩니다. 볼 수는 있지만 변경할 수는 없습니다.

AWS Backup이 정책에서 생성한 백업 계획에 따라 백업을 시작하면 AWS Backup 콘솔에서 백업 작업의 상태를 볼 수 있습니다. 멤버 계정의 사용자는 해당 멤버 계정의 백업 작업에 대한 상태 및 오류를 볼 수 있습니다. AWS Backup에서 신뢰할 수 있는 서비스 액세스도 활성화하면 조직의 관리 계정 사용자

가 조직의 모든 백업 작업에 대한 상태 및 오류를 볼 수 있습니다. 자세한 내용은 AWS Backup 개발자 안내서의 교차 계정 관리 활성화를 참조하세요.

백업 정책 시작하기

다음 단계에 따라 백업 정책 사용을 시작합니다.

1. 백업 정책 작업을 수행하는 데 필요한 권한에 대해 알아봅니다.
2. 백업 정책을 사용할 때 권장되는 몇 가지 모범 사례에 대해 알아봅니다.
3. 조직에 대해 백업 정책을 활성화합니다.
4. 백업 정책을 생성합니다.
5. 백업 정책을 조직의 루트, OU 또는 계정에 연결합니다.
6. 계정에 적용되는 결합된 유효 백업 정책을 확인합니다.

위의 모든 단계를 수행하려면 조직의 관리 계정에서 IAM 사용자로 로그인하거나, IAM 역할을 맡거나, 루트 사용자로 로그인(권장되지 않음)합니다.

기타 정보

- 백업 정책 구문 알아보기 및 정책 예제 보기

백업 정책 관리를 위한 사전 조건 및 권한

이 페이지에서는 AWS Organizations에서 백업 정책을 관리하기 위한 사전 조건 및 필수 권한에 대해 설명합니다.

주제

- 백업 정책 관리를 위한 사전 조건
- 백업 정책 관리를 위한 권한

백업 정책 관리를 위한 사전 조건

조직에서 백업 정책을 관리하려면 다음이 필요합니다.

- 조직의 모든 기능을 활성화해야 합니다.
- 조직의 관리 계정에 로그인해야 합니다.

- AWS Identity and Access Management(IAM) 사용자 또는 역할에는 다음 섹션에 나열된 권한이 있어야 합니다.

백업 정책 관리를 위한 권한

다음 IAM 정책 예제는 조직에서 백업 정책의 모든 측면을 관리할 수 있는 권한을 제공합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

IAM 정책 및 권한에 대한 자세한 내용은 IAM 사용 설명서를 참조하세요.

백업 정책 사용 모범 사례

AWS에서는 백업 정책 사용에 대해 다음과 같은 모범 사례를 권장합니다.

백업 정책 전략 결정

상속 및 병합되는 불완전한 부분으로 백업 정책을 생성하여 각 멤버 계정에 대해 완전한 정책을 생성할 수 있습니다. 이렇게 하면 변경 내용이 하위 수준의 모든 계정에 미치는 영향을 신중하게 고려하지 않고 특정 수준에서 정책을 변경하면 불완전한 유효 정책이 될 위험이 있습니다. 이를 방지하려면 모든 수준에서 구현하는 백업 정책이 자체적으로 완전하도록 하는 것이 좋습니다. 상위 정책을 하위 정책에 지정된 설정으로 재정의할 수 있는 기본 정책으로 취급합니다. 이렇게 하면 하위 정책이 존재하지 않더라도 상속된 정책이 완전하고 기본값을 사용합니다. 하위 제어 상속 연산자를 사용하여 하위 정책에 의해 추가, 변경 또는 제거될 수 있는 설정을 제어할 수 있습니다.

`GetEffectivePolicy`를 사용하여 백업 정책 확인에 대한 변경 사항 유효성 검사

백업 정책을 변경한 후 정책이 변경된 수준보다 낮은 대표 계정에 대한 유효 정책을 확인합니다. AWS Management Console을 사용하거나 GetEffectivePolicy API 작업 또는 해당 AWS CLI 또는 AWS SDK 변형 중 하나를 사용하여 유효 정책을 볼 수 있습니다. 변경한 내용이 유효 정책에 의도한 영향을 미쳤는지 확인합니다.

간단하게 시작하고 소규모로 변경

디버깅을 단순화하려면 간단한 정책으로 시작하여 한 번에 한 항목씩 변경합니다. 다음 변경을 수행하기 전에 각 변경의 동작 및 영향을 검증합니다. 이러한 접근 방식은 오류 또는 예기치 않은 결과가 발생할 때 고려해야 할 변수를 줄입니다.

조직의 다른 AWS 리전 및 계정에 백업의 복사본 저장

재해 복구 위치를 개선하기 위해 백업의 복사본을 저장할 수 있습니다.

- 다른 리전 - 백업의 복사본을 다른 AWS 리전에 추가로 저장하면 원래 리전에서 실수로 손상되거나 삭제되는 경우에 대비하여 백업을 보호할 수 있습니다. 정책의 `copy_actions` 섹션을 사용해, 백업 계획이 실행되는 해당 계정에 속한 리전 하나 이상에서 볼트를 지정합니다. 이를 위해 백업의 복사본을 저장할 백업 볼트의 ARN을 지정할 때 `$account` 변수를 사용하여 계정을 식별합니다. `$account` 변수는 실행 시점에 백업 정책이 실행되는 계정 ID로 대체됩니다.

- 다른 계정 - 백업 복사본을 다른 AWS 계정에 추가로 저장하면 계정 중 하나를 손상시키는 악의적인 행위자를 막는 데 도움이 되는 보안 장벽이 더해집니다. 정책의 `copy_actions` 섹션을 사용해, 백업 계획이 실행되는 계정과 별도로 조직에 속한 계정 하나 이상에서 볼트를 지정합니다. 이를 위해 백업의 복사본을 저장할 백업 볼트의 ARN을 지정할 때 실제 계정 ID 번호를 사용해 계정을 식별합니다.

정책당 계획 수를 제한

여러 계획이 포함된 정책은 모두 유효성을 검사해야 하는 출력 수가 많아지기 때문에 문제를 해결하는 것이 더 복잡합니다. 대신, 각 정책에 하나의 백업 계획만 포함하여 디버깅 및 문제 해결을 단순화하도록 하세요. 그런 다음 다른 요구 사항을 충족하도록 다른 계획을 사용하여 정책을 추가할 수 있습니다. 이 방식은 특정 계획의 모든 문제를 하나의 정책으로 격리할 수 있으며 다른 정책 및 해당 계획 때문에 문제 해결이 복잡해지는 것을 방지할 수 있습니다.

스택 세트를 사용하여 필요한 백업 볼트 및 IAM 역할 생성

AWS CloudFormation 스택 세트와 Organizations 간 통합을 사용하여 조직의 각 멤버 계정에서 필요한 백업 볼트 및 AWS Identity and Access Management(IAM) 역할을 자동으로 생성합니다. 조직의 모든 AWS 계정에서 자동으로 사용할 수 있는 리소스를 포함하는 스택 세트를 생성할 수 있습니다. 이 방식을 통해 종속성이 이미 충족되었음이 보장된 상태에서 백업 계획을 실행할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 자체 관리 권한으로 스택 세트 만들기를 참조하세요.

각 계정에서 생성된 첫 번째 백업을 검토하여 결과를 확인합니다.

정책을 변경할 때 변경 이후에 생성된 다음 백업을 확인하여 변경 사항이 원하는 영향을 미치는지 확인합니다. 이 단계는 유효 정책을 확인하는 것을 넘어 AWS Backup이 정책을 해석하고 의도한 대로 백업 계획을 구현하기 위한 것입니다.

백업 정책 생성, 업데이트 및 삭제

이 주제에서 수행할 작업

- 조직에 대해 백업 정책을 활성화한 후 정책을 생성할 수 있습니다.
- 백업 요구 사항이 변경되면 기존 정책을 업데이트할 수 있습니다.
- 정책이 더 이상 필요하지 않은 경우 모든 조직 단위(OU) 및 계정에서 정책을 분리한 후 삭제할 수 있습니다.

백업 정책 생성

> **최소 권한**
>
> 백업 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.
>
> - `organizations:CreatePolicy`

AWS Management Console

다음 두 가지 방법 중 하나를 사용하여 AWS Management Console에서 백업 정책을 생성할 수 있습니다.

- 사용자가 옵션을 선택하면 자동으로 JSON 정책 텍스트를 생성하는 시각적 편집기.
- 사용자가 직접 JSON 정책 텍스트를 작성할 수 있는 텍스트 편집기.

시각적 편집기를 사용하면 프로세스를 쉽게 수행할 수 있지만 유연성은 제한됩니다. 이는 처음 정책을 생성하여 편안하게 사용할 수 있는 좋은 방법입니다. 정책이 어떻게 작동하는지 이해하고 시각적 편집기가 제공하는 기능에 의해 제한되기 시작하면 JSON 정책 텍스트를 직접 편집하여 정책에 고급 기능을 추가할 수 있습니다. 시각적 편집기는 @@assign value-setting 연산자만 사용하며, 하위 제어 연산자에 대한 액세스 권한을 제공하지 않습니다. 하위 제어 연산자는 JSON 정책 텍스트를 수동으로 편집하는 경우에만 추가할 수 있습니다.

백업 정책을 생성하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 백업 정책(Backup policies) 페이지에서 정책 생성(Create policy)을 선택합니다.
3. 정책 생성(Create policy) 페이지에서 정책 이름과 정책 설명(선택 사항)을 입력합니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요AWS Organizations 리소스에 태그 지정
5. 이 절차의 설명과 같이 시각적 편집기를 사용하여 정책을 작성할 수 있습니다. JSON 탭에서 정책 텍스트를 입력하거나 붙여 넣을 수도 있습니다. 백업 정책 구문에 대한 자세한 내용은 백업 정책 구문 및 예제 단원을 참조하세요.

시각적 편집기를 사용하기로 선택한 경우 시나리오에 적합한 백업 옵션을 선택합니다. 백업 계획은 세 부분으로 구성됩니다. 이러한 백업 계획 요소에 대한 자세한 내용은 AWS Backup 개발자 안내서의 백업 계획 생성 및 리소스 할당을 참조하세요.

a. 백업 계획 일반 세부 정보

- 백업 계획 이름은 영숫자, 하이픈, 밑줄 문자로만 구성할 수 있습니다.
- 목록에서 하나 이상의 백업 계획 영역을 선택해야 합니다. 계획은 선택한 AWS 리전에서만 리소스를 백업할 수 있습니다.

b. AWS Backup이 작동하는 방법 및 시기를 지정하는 하나 이상의 백업 규칙이 있습니다. 각 백업 규칙은 다음 사항을 정의합니다.

- 백업 빈도 및 백업을 수행할 수 있는 기간을 포함하는 일정.
- 사용할 백업 볼트의 이름입니다. 백업 볼트 이름은 영숫자, 하이픈, 밑줄 문자로만 구성할 수 있습니다. 백업 볼트가 있어야 계획을 성공적으로 실행할 수 있습니다. AWS Backup 콘솔 또는 AWS CLI 명령을 사용하여 볼트를 생성합니다.
- (선택 사항) 하나 이상의 리전에 복사(Copy to region) 규칙을 사용하여 백업을 다른 AWS 리전의 볼트에 복사합니다.
- 이 백업 계획이 실행될 때마다 생성된 백업 복구 지점에 연결할 하나 이상의 태그 키/값 페어.
- 백업이 콜드 스토리지로 전환되는 시기와 백업이 만료되는 시기를 지정하는 수명 주기 옵션.

규칙 추가(Add rule)를 선택해 필요한 모든 규칙을 추가합니다.

백업 규칙에 대한 자세한 내용은 AWS Backup 개발자 안내서의 백업 규칙을 참조하세요.

c. AWS Backup이 이 계획을 통해 백업해야 하는 리소스를 지정하는 리소스 할당. 할당은 AWS Backup이 리소스를 찾아서 매칭하는 데 사용할 태그 페어를 지정하여 수행됩니다.

- 리소스 할당 이름은 영숫자, 하이픈, 밑줄 문자로만 구성될 수 있습니다.
- AWS Backup이 이름을 기준으로 백업을 수행하는 데 사용할 IAM 역할을 지정합니다.

  콘솔에서는 전체 Amazon 리소스 이름(ARN)을 지정하지 않습니다. 역할 이름과 역할 유형을 지정하는 접두사를 모두 포함해야 합니다. 접두사는 일반적으로 `role` 또는 `service-role`이며, 슬래시('/')로 역할 이름과 구분합니다. 예를 들어 `role/MyRoleName` 또는 `service-role/MyManagedRoleName`을 입력할 수 있습니다. 이는 기본 JSON에 저장될 때 전체 ARN으로 변환됩니다.

> **Important**
>
> 지정된 IAM 역할은 정책이 적용되는 계정에 이미 존재해야 합니다. 그렇지 않으면 백업 계획이 백업 작업을 성공적으로 시작할 수 있지만 이러한 백업 작업은 실패합니다.

- 백업할 리소스를 식별하기 위해 하나 이상의 리소스 태그 키 및 태그 값 페어를 지정합니다. 태그 값이 두 개 이상인 경우 쉼표로 값을 구분합니다.

할당 추가(Add assignment)를 선택해, 구성된 각 리소스 할당을 백업 계획에 추가합니다.

자세한 내용은 AWS Backup 개발자 안내서의 백업 계획에 리소스 할당을 참조하세요.

6. 정책 작성을 마쳤으면 정책 생성(Create policy)을 선택합니다. 정책이 사용 가능한 백업 정책 목록에 나타납니다.

AWS CLI & AWS SDKs

백업 정책을 생성하려면

다음 중 하나를 사용하여 백업 정책을 생성할 수 있습니다.

- AWS CLI: create-policy

백업 계획을 다음과 유사한 JSON 텍스트로 생성해서 텍스트 파일에 저장합니다. 구문의 전체 규칙은 백업 정책 구문 및 예제 단원을 참조하세요.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
```

```
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

이 백업 계획은 영향을 받는 AWS 계정에서 지정된 AWS 리전에 있고 태그 `dataType`의 값이 `PII`인 모든 리소스를 AWS Backup이 백업하도록 지정합니다.

다음으로, JSON 정책 파일 백업 계획을 가져와 조직에 새 백업 정책을 생성합니다. 출력에서 정책 ARN의 끝에 있는 정책 ID를 확인합니다.

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
```

```
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWS SDK: CreatePolicy

다음에 수행할 작업

백업 정책을 생성한 후 정책을 적용할 수 있습니다. 이를 위해 조직 루트, 조직 단위(OU), 조직 내 AWS 계정, 또는 이들의 조합에 정책을 연결할 수 있습니다.

백업 정책 업데이트

조직의 관리 계정에 로그인하면 조직에서 변경이 필요한 정책을 편집할 수 있습니다.

> 최소 권한
>
> 백업 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - 동일한 정책 명령문에서 업데이트할 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 organizations:UpdatePolicy
> - 동일한 정책 명령문에서 업데이트할 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 organizations:DescribePolicy

AWS Management Console

백업 정책을 업데이트하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 백업 정책 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책 편집을 선택합니다.
4. 새로운 정책 이름, 정책 설명을 입력할 수 있습니다. 정책 내용은 시각적 편집기를 사용하거나 JSON을 직접 편집해 변경할 수 있습니다.
5. 백업 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

백업 정책을 업데이트하려면

다음 중 하나를 사용하여 백업 정책을 업데이트할 수 있습니다.

- AWS CLI: update-policy

  다음 예제에서는 백업 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

  다음 예제에서는 백업 정책에 대한 설명을 추가하거나 변경합니다.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
```

```
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}}"
    }
}
```

다음 예제에서는 백업 정책에 연결된 JSON 정책 문서를 변경합니다. 이 예제에서 콘텐츠는 다음 텍스트를 포함한 `policy.json`이라는 파일에서 가져옵니다.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
```

```
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- AWS SDK: UpdatePolicy

태그 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하여 백업 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요AWS Organizations 리소스에 태그 지정

최소 권한

AWS 조직의 백업 정책에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- organizations:DescribeOrganization(콘솔만 해당 - 정책으로 이동하기 위해)
- organizations:DescribePolicy(콘솔만 해당 - 정책으로 이동하기 위해)
- organizations:TagResource
- organizations:UntagResource

AWS Management Console

백업 정책에 연결된 태그를 편집하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 백업 정책 페이지
3. 편집할 태그가 있는 정책의 이름을 선택합니다.

   정책 세부 정보 페이지가 나타납니다.
4. 태그 탭에서 태그 관리를 선택합니다.
5. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.

   - 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
   - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
   - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 `null`이 아닌 빈 문자열이 됩니다.
6. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

백업 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 백업 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: tag-resource 및 untag-resource
- AWS SDK: TagResource 및 UntagResource

백업 정책 삭제

조직의 관리 계정에 로그인하면 조직에서 더 이상 필요 없는 정책을 삭제할 수 있습니다.

정책을 삭제하기 전에 먼저 연결된 모든 개체에서 정책을 분리해야 합니다.

최소 권한

백업 정책을 삭제하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- 동일한 정책 명령문에서 삭제할 정책의 ARN(또는 "*")을 포함하는 `Resource` 요소를 가진 `organizations:DeletePolicy`

AWS Management Console

백업 정책을 삭제하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 백업 정책 페이지에서 삭제할 백업 정책의 이름을 선택합니다.
3. 먼저 모든 루트, OU와 계정에서 삭제하려는 백업 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제(Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제(Delete)를 선택합니다.

AWS CLI & AWS SDKs

백업 정책을 삭제하려면

다음 중 하나를 사용하여 정책을 삭제할 수 있습니다.

- AWS CLI: delete-policy

  다음은 지정된 정책을 삭제하는 예제입니다. 정책이 루트, OU 또는 계정에 연결되지 않은 경우에만 작동합니다.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: DeletePolicy

백업 정책 연결 및 분리

전체 조직뿐 아니라 OU(조직 단위) 및 개별 계정에서도 백업 정책을 사용할 수 있습니다. 다음 사항에 유의하세요.

- 백업 정책을 조직 루트에 연결하면 정책은 해당 루트의 모든 멤버 OU 및 계정에 모두 적용됩니다.
- 백업 정책을 OU에 연결하면 해당 정책은 OU 또는 해당 자식 OU에 속한 계정에 적용됩니다. 이러한 계정에는 조직 루트에 연결된 정책이 모두 적용됩니다.
- 백업 정책을 계정에 연결하면 정책이 해당 계정에만 적용됩니다. 또한 계정에는 조직 루트 및 해당 계정이 속한 OU에 연결된 정책이 적용됩니다.

계정이 루트 및 상위 OU로부터 상속하는 백업 정책과 계정에 직접 연결된 모든 정책의 집계가 유효 정책입니다. 정책이 유효 정책에 병합되는 방법에 대한 자세한 내용은 관리 정책 상속에 대한 이해 단원을 참조하세요.

백업 정책 연결

조직의 관리 계정에 로그인하면 백업 정책을 조직의 루트, OU 또는 계정에 직접 연결할 수 있습니다.

> **최소 권한**
>
> 백업 정책을 연결하려면 다음 작업을 실행할 권한이 있어야 합니다.
>
> - `organizations:AttachPolicy`

AWS Management Console

정책을 탐색하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 백업 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 백업 정책을 연결하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).

3. 정책(Policies) 탭의 백업 정책에 대한 항목에서 연결(Attach)을 선택합니다.
4. 원하는 정책을 찾아 정책 연결(Attach policy)을 선택합니다.

   정책(Policies) 탭의 연결된 백업 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 백업 정책을 연결하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 백업 정책 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
5. 정책 연결(Attach policies)을 선택합니다.

   대상(Targets) 탭의 연결된 백업 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

AWS CLI & AWS SDKs

백업 정책을 조직 루트, OU 또는 계정에 연결하려면

백업 정책을 연결하려면 다음 명령 중 한 가지를 사용합니다.

- AWS CLI: attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- AWS SDK: AttachPolicy

정책 변경은 즉시 적용됩니다.

백업 정책 분리

조직의 관리 계정에 로그인하면 연결된 조직 루트, OU 또는 계정에서 백업 정책을 분리할 수 있습니다. 엔터티에서 백업 정책을 분리하면 해당 정책은 현재 분리된 엔터티의 영향을 받던 모든 계정에 더 이상 적용되지 않습니다. 정책을 분리하려면 다음 단계를 완료하세요.

> **최소 권한**
>
> 조직 루트, OU 또는 계정에서 백업 정책을 분리하려면 다음 작업을 실행할 권한이 있어야 합니다.
>
> - `organizations:DetachPolicy`

AWS Management Console

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 백업 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 백업 정책을 분리하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책(Policies) 탭에서, 분리할 백업 정책 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

   연결된 백업 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 백업 정책을 분리하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 백업 정책(Backup policies) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.

3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

   연결된 백업 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

AWS CLI & AWS SDKs

조직 루트, OU 또는 계정에서 백업 정책을 분리하려면

백업 정책을 분리하려면 다음 명령 중 한 가지를 사용합니다.

- AWS CLI: detach-policy

  다음 예제에서는 OU로부터 정책을 분리합니다.

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS SDK: DetachPolicy

정책 변경은 즉시 적용됩니다.

유효 백업 정책 보기

AWS 관리 콘솔, AWS API 또는 AWS Command Line Interface에서 계정의 유효 백업 정책을 볼 수 있습니다. 다음 섹션에서는 하나의 예제와 함께 유효 백업 정책에 대한 간략한 개요를 제공합니다.

유효 백업 정책이란 무엇입니까?

유효 백업 정책은 AWS 계정에 적용되는 최종 백업 계획 설정을 지정합니다. 이는 계정이 상속하는 모든 백업 정책과 계정에 직접 연결된 백업 정책을 집계한 것입니다. 백업 정책을 조직 루트에 연결하면 해당 정책은 조직의 모든 계정에 적용됩니다. 백업 정책을 조직 단위(OU)에 연결하면 해당 정책은 OU

에 속한 모든 계정 및 OU에 적용됩니다. 정책을 계정에 직접 연결하면 정책이 해당 AWS 계정에만 적용됩니다.

예를 들어 조직 루트에 연결된 백업 정책은 조직의 모든 계정이 기본 백업 빈도인 일주일에 한 번씩 모든 Amazon DynamoDB 테이블을 백업하도록 지정할 수 있습니다. 테이블에 중요한 정보가 있는 한 멤버 계정에 직접 연결된 별도의 백업 정책은 하루에 한 번으로 빈도를 재정의할 수 있습니다. 이러한 백업 정책의 조합이 유효 백업 정책을 구성합니다. 이 유효 백업 정책은 조직의 각 계정에 대해 개별적으로 결정됩니다. 이 예제를 실행하면 결과적으로 DynamoDB 테이블을 매일 백업하는 한 계정을 제외하고 조직의 모든 계정이 일주일에 한 번씩 테이블을 백업합니다.

백업 정책이 최종 유효 백업 정책으로 결합되는 방법에 대한 자세한 내용은 관리 정책 상속에 대한 이해 단원을 참조하세요.

유효 백업 정책 보기

AWS Management Console, AWS API 또는 AWS Command Line Interface를 사용하여 계정에 대한 유효 백업 정책을 볼 수 있습니다.

> 최소 권한
>
> 계정에 대한 유효 백업 정책을 보려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

계정에 대한 유효 백업 정책을 보려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 유효 백업 정책을 보려는 계정의 이름을 선택합니다. 원하는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책(Policies) 탭의 백업 정책(Backup policies) 섹션에서 이 AWS 계정에 대한 유효 백업 정책 보기(View the effective AI policy for this AWS 계정)를 선택합니다.

지정한 계정에 적용되는 유효 정책이 콘솔에 표시됩니다.

> **Note**
>
> 중요한 변경 없이 유효 정책을 복사하여 붙여넣고 다른 백업 정책의 JSON으로 사용할 수는 없습니다. 백업 정책 문서에는 각 설정이 최종 유효 정책으로 병합되는 방법을 지정하는 상속 연산자가 포함되어야 합니다.

AWS CLI & AWS SDKs

계정에 대한 유효 백업 정책을 보려면

다음 명령 중 하나를 사용하여 유효 백업 정책을 볼 수 있습니다.

- AWS CLI: describe-effective-policy

  다음 예제에서는 백업 정책의 세부 정보를 표시합니다.

```
$ aws organizations describe-effective-policy \
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::
$account:role/MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes
\":\"10080\",\"target_backup_vault_name\
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},
\"copy_actions\":{\"arn:aws:backup:us-east-1:$accou
nt:backup-vault:secondary-vault\":{\"lifecycle\":
{\"move_to_cold_storage_after_days\":\"10\",\"delete_after_days\":\"100\"
}}}}}}}"
    }
}
```

- AWS SDK: DescribeEffectivePolicy

AWS CloudTrail 이벤트를 사용하여 조직의 백업 정책을 모니터링하기

AWS CloudTrail 이벤트를 사용하여 AWS 조직의 계정에서 백업 정책이 생성, 업데이트 또는 삭제되는 경우와 잘못된 조직 백업 계획이 있는 경우를 모니터링할 수 있습니다. 자세한 내용은 AWS Backup 개발자 안내서의 교차 계정 관리 이벤트 로깅을 참조하세요.

백업 정책 구문 및 예제

이 페이지에서는 백업 정책 구문에 대해 설명하고 예제를 제공합니다.

백업 정책 구문

백업 정책은 JSON 규칙에 따라 구성된 일반 텍스트 파일입니다. 백업 정책 구문은 모든 관리 정책 유형에 대한 구문을 따릅니다. 해당 구문에 대한 자세한 내용은 관리 정책 유형에 대한 정책 구문 및 상속을 참조하세요. 이 항목에서는 백업 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 방법을 중점적으로 설명합니다.

백업 정책의 대부분은 백업 계획과 그 규칙입니다. 백업 정책 내의 백업 계획 구문은 에서 사용하는 구문과 구조적으로 AWS Backup동일하지만 키 이름은 다릅니다. AWS Organizations 아래 정책 키 이름에 대한 설명에는 각 정책 키 이름에 해당하는 AWS Backup 계획 키 이름이 포함되어 있습니다. AWS Backup 플랜에 대한 자세한 내용은 AWS Backup 개발자 안내서를 참조하십시오 CreateBackupPlan.

> **Note**
>
> JSON을 사용할 때 중복된 키 이름은 거부됩니다. 단일 정책에 여러 계획, 규칙 또는 선택 항목을 포함하려면 각 키의 이름이 고유해야 합니다.

완전하고 제대로 작동하는 유효 백업 정책은 일정 및 규칙이 포함된 백업 계획 이상을 포함해야 합니다. 또한 정책은 백업할 대상 AWS 리전 및 리소스, 백업을 수행하는 데 사용할 AWS Backup 수 있는 AWS Identity and Access Management (IAM) 역할을 식별해야 합니다.

다음의 기능적으로 완전한 정책은 기본 백업 정책 구문을 보여 줍니다. 이 예제를 계정에 직접 연결한 경우 값이 `PII` 또는 `RED` 인 AWS Backup 태그가 `dataType` 있는 `us-east-1` 및 `eu-north-1` 지역에서 해당 계정의 모든 리소스를 백업합니다. 이러한 리소스를 매일 오전 5시에 `My_Backup_Vault`로 백업하고 복제본을 `My_Secondary_Vault`에 저장합니다. 두 볼트는 모두 리소스와 동일한 계정에 있

습니다. 정책은 명시적으로 지정한 다른 계정의 My_Tertiary_Vault에도 백업의 복사본을 저장합니다. 유효한 정책을 받는 각 저장소의 지정된 AWS 리전 저장소에는 저장소가 AWS 계정 이미 있어야 합니다. 백업된 리소스가 EC2 인스턴스인 경우 해당 인스턴스의 백업에 대해 Microsoft Volume Shadow Copy Service(VSS) 지원이 활성화됩니다. 백업은 각 복구 지점에 태그 Owner:Backup을 적용합니다.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
```

```
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
}
```

백업 정책 구문에는 다음 구성 요소가 포함됩니다.

- $account 변수 - 정책의 특정 텍스트 문자열에서 $account 변수를 사용하여 현재 AWS 계정을 나타낼 수 있습니다. 유효 정책에서 계획을 실행하면 이 변수가 유효 정책 및 해당 계획이 AWS Backup 실행되고 있는 현재 AWS 계정 변수로 자동 대체됩니다.

  > **Important**
  >
  > Amazon 리소스 이름(ARN)을 포함할 수 있는 정책 요소(예: 백업을 저장할 백업 볼트를 지정하는 요소 또는 백업을 수행할 권한이 있는 IAM 역할)에서만 $account 변수를 사용할 수 있습니다.

  예를 들어, 다음과 같은 경우에는 정책이 AWS 계정 적용되는 각 저장소에 이름이 지정된 저장소가 My_Vault 있어야 합니다.

  ```
  arn:aws:backup:us-west-2:$account:vault:My_Vault"
  ```

  AWS CloudFormation 스택 세트 및 Organization과의 통합을 사용하여 조직의 각 구성원 계정에 대한 백업 저장소와 IAM 역할을 자동으로 생성하고 구성하는 것이 좋습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 자체 관리 권한으로 스택 세트 만들기를 참조하세요.
- 상속 연산자 - 백업 정책은 상속 값-설정(value-setting) 연산자와 하위 제어 연산자를 모두 사용할 수 있습니다.
- plans

  정책의 최상위 키에는 plans 키가 있습니다. 백업 정책은 항상 정책 파일의 맨 위에 있는 이 고정 키 이름으로 시작해야 합니다. 이 키 아래에 하나 이상의 백업 계획을 둘 수 있습니다.
- plans 최상위 키 아래의 각 계획은 사용자가 할당한 백업 계획 이름으로 구성된 키 이름을 갖습니다. 위의 예제에서 백업 계획 이름은 PII_Backup_Plan입니다. 한 정책에 각각 고유한 rules, regions, selections, tags를 가진 여러 계획을 둘 수 있습니다.

  백업 정책의 이 백업 계획 키 이름은 계획의 BackupPlanName 키 값에 매핑됩니다. AWS Backup

  각 객체에는 다음의 요소가 포함될 수 있습니다.

  - rules - 이 키에는 규칙 모음이 들어 있습니다. 각 규칙은 예약된 작업으로 변환되며, 유효 백업 정책의 selections 및 regions 요소로 식별된 리소스를 백업할 시작 시간 및 기간이 포함됩니다.

- regions- 이 키에는 이 정책으로 리소스를 백업할 수 있는 AWS 리전 사람의 배열 목록이 들어 있습니다.
- selections – 이 키에는 지정된 rules에 의해 백업되는 리소스 모음(지정된 regions에 있음)이 하나 이상 들어 있습니다.
- advanced_backup_settings- 이 키에는 특정 리소스에서 실행되는 백업에 특정한 설정이 포함되어 있습니다.
- backup_plan_tags - 백업 계획 자체에 연결되는 태그를 지정합니다.

- rules

  rules 정책 키는 AWS Backup 계획의 Rules 키에 매핑됩니다. rules 키 아래에 하나 이상의 규칙을 포함할 수 있습니다. 각 규칙은 선택한 리소스에 대한 백업을 수행하는 예약된 작업이 됩니다.

  각 규칙에는 이름이 규칙 이름인 키가 포함됩니다. 위의 예제에서 규칙 이름은 “My_Hourly_Rule”입니다. 규칙 키의 값은 다음과 같은 규칙 요소의 모음입니다.

  - schedule_expression— 이 정책 키는 AWS Backup 계획의 ScheduleExpression 키에 매핑됩니다.

    백업의 시작 시간을 지정합니다. 이 키에는 @@assign상속 값 연산자와 백업 작업 시작 시기를 AWS Backup 지정하는 CRON 표현식이 있는 문자열 값이 들어 있습니다. CRON 문자열의 일반적인 형식은 "cron( )"입니다. 각각은 숫자 또는 와일드카드입니다. 예를 들어 cron(0 5 ? * 1,3,5 *)는 매주 월요일, 수요일 및 금요일 오전 5시에 백업을 시작합니다. cron(0 0/1 ? * * *)는 매일 매시 정각에 백업을 시작합니다.

  - target_backup_vault_name— 이 정책 키는 계획의 키에 TargetBackupVaultName 매핑됩니다. AWS Backup

    백업을 저장할 백업 볼트의 이름을 지정합니다. 를 사용하여 가치를 AWS Backup창출합니다. 이 키에는 @@assign 상속 값 연산자와 볼트 이름이 포함된 문자열 값이 들어 있습니다.

    > **Important**
    >
    > 백업 계획을 처음 시작할 때 볼트가 이미 있어야 합니다. AWS CloudFormation 스택 세트 및 Organization과의 통합을 사용하여 조직의 각 구성원 계정에 대한 백업 저장소와 IAM 역할을 자동으로 생성하고 구성하는 것이 좋습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 자체 관리 권한으로 스택 세트 만들기를 참조하세요.

  - start_backup_window_minutes— 이 정책 키는 계획의 키에 StartWindowMinutes 매핑됩니다. AWS Backup

(선택 사항) 성공적으로 시작되지 않은 작업을 취소하기 전에 대기할 시간(분)을 지정합니다. 이 키에는 @@assign 상속 값 연산자와 정수 값(분)이 들어 있습니다.

- complete_backup_window_minutes – 이 정책 키는 AWS Backup 계획의 CompletionWindowMinutes 키에 매핑됩니다.

  (선택 사항) 백업 작업이 성공적으로 시작된 후 완료되거나 AWS Backup에 의해 취소되기 전까지 시간(분)을 지정합니다. 이 키에는 @@assign 상속 값 연산자와 정수 값(분)이 들어 있습니다.

- enable_continuous_backup— 이 정책 키는 AWS Backup 계획의 EnableContinuousBackup 키에 매핑됩니다.

  (선택 사항) 연속 백업을 AWS Backup 생성할지 여부를 지정합니다. True point-in-time 복원 가능한 연속 백업 (PITR) AWS Backup 을 생성하는 원인. False(또는 지정되지 않음) 원인은 AWS Backup 스냅샷 백업을 생성합니다.

  > **Note**
  >
  > PITR 지원 백업은 최대 35일 동안 유지할 수 있으므로 만약 다음 옵션 중 하나를 설정했다면 False를 선택하거나 값을 지정하지 않아야 합니다.
  >
  > - delete_after_days를 35보다 큰 값으로 설정.
  > - move_to_cold_storage_after_days를 임의의 값으로 설정.

  연속 백업에 대한 자세한 내용은 AWS Backup 개발자 안내서의 P oint-in-time 복구를 참조하십시오.

- lifecycle— 이 정책 키는 AWS Backup 계획의 Lifecycle 키에 매핑됩니다.

  (선택 사항) 이 백업을 콜드 스토리지로 AWS Backup 전환하는 시기와 만료일을 지정합니다.

  - move_to_cold_storage_after_days - 이 정책 키는 계획의 키에 MoveToColdStorageAfterDays 매핑됩니다. AWS Backup

    AWS Backup 이 백업 후 복구 지점을 콜드 스토리지로 이동할 때까지 경과할 기간(일)을 지정합니다. 이 키에는 @@assign 상속 값 연산자와 정수 값(일)이 들어 있습니다.

  - delete_after_days— 이 정책 키는 AWS Backup 계획의 DeleteAfterDays 키에 매핑됩니다.

AWS Backup 이 백업 후 복구 지점을 삭제할 때까지 경과할 기간(일)을 지정합니다. 이 키에는 @@assign 상속 값 연산자와 정수 값(일)이 들어 있습니다. 백업을 콜드 스토리지로 전환하는 경우 백업을 최소 90일 동안 유지해야 하므로 이 값은 move_to_cold_storage_after_days보다 90일 이상 커야 합니다.

- copy_actions— 이 정책 키는 AWS Backup 계획의 CopyActions 키에 매핑됩니다.

  (선택 사항) 백업을 하나 이상의 추가 위치에 복사하도록 AWS Backup 지정합니다. 각 백업 복사본 위치는 아래에 설명되어 있습니다.

  - 이름으로 해당 복사 작업을 고유하게 식별할 수 있는 키입니다. 이때 키 이름은 백업 볼트의 Amazon 리소스 이름(ARN)이어야 합니다. 이 키는 두 항목을 포함합니다.
    - target_backup_vault_arn – 이 정책 키는 AWS Backup 계획의 DestinationBackupVaultArn 키에 매핑됩니다.

      (선택 사항) 백업의 추가 복사본을 AWS Backup 저장하는 저장소를 지정합니다. 이 키의 값은 @@assign 상속 값 연산자와 볼트의 ARN을 포함합니다.
      - 백업 정책이 실행되는 저장소를 참조하려면 계정 ID 번호 대신 ARN의 $account 변수를 사용하십시오. AWS 계정 백업 계획을 실행하면 변수가 정책이 AWS Backup 실행되는 계정의 계정 ID 번호로 자동 대체됩니다. AWS 계정 이렇게 하면 백업 정책을 조직의 둘 이상의 계정에 적용할 때 백업이 올바르게 실행됩니다.
      - 동일한 조직에 있는 다른 AWS 계정 의 볼트를 참조하려면 ARN에 실제 계정 ID 번호를 사용합니다.

      > **Important**
      > - 이 키가 없으면 상위 키 이름에 있는 모든 소문자 버전의 ARN이 사용됩니다. ARN은 대소문자를 구분하므로 이 문자열은 오류의 실제 ARN과 일치하지 않을 수 있으며 계획이 실패합니다. 따라서 항상 이 키 및 값을 제공하는 것이 좋습니다.
      > - 백업 계획을 처음 시작할 때 백업을 복사하려는 백업 볼트가 사전에 존재해야 합니다. AWS CloudFormation 스택 세트 및 Organizations와의 통합을 사용하여 조직의 각 멤버 계정에 대한 백업 볼트 및 IAM 역할을 자동으로 생성하고 구성하는 것이 좋습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 자체 관리 권한으로 스택 세트 만들기를 참조하세요.

    - lifecycle— 이 정책 키는 AWS Backup 계획의 Lifecycle 키 아래에 있는 CopyAction 키에 매핑됩니다.

(선택 사항) 이 백업 복사본을 콜드 스토리지로 AWS Backup 전환하는 시기와 만료일을 지정합니다.

- `move_to_cold_storage_after_days` – 이 정책 키는 AWS Backup 계획의 `MoveToColdStorageAfterDays` 키에 매핑됩니다.

  백업이 발생한 후 복구 지점을 콜드 스토리지로 AWS Backup 이동하기 전까지 경과할 일수를 지정합니다. 이 키에는 @@assign 상속 값 연산자와 정수 값(일)이 들어 있습니다.

- `delete_after_days` – 이 정책 키는 AWS Backup 계획의 `DeleteAfterDays` 키에 매핑됩니다.

  백업이 발생한 후 복구 지점을 AWS Backup 삭제하기 전까지 경과할 일수를 지정합니다. 이 키에는 @@assign 상속 값 연산자와 정수 값(일)이 들어 있습니다. 백업을 콜드 스토리지로 전환하는 경우 백업을 최소 90일 동안 유지해야 하므로 이 값은 `move_to_cold_storage_after_days`보다 90일 이상 커야 합니다.

- `recovery_point_tags`- 이 정책 키는 AWS Backup 계획의 `RecoveryPointTags` 키에 매핑됩니다.

  (선택 사항) 이 계획에서 생성하는 각 백업에 AWS Backup 첨부되는 태그를 지정합니다. 이 키의 값에는 다음 요소 중 하나 이상이 포함됩니다.

  - 이 키 이름/값 페어의 식별자. `tag_key`의 대/소문자 처리가 다르더라도 `recovery_point_tags` 아래의 각 요소에 대한 이 이름은 모두 소문자로 표시된 태그 키 이름입니다. 이 식별자는 대소문자를 구분하지 않습니다. 위의 예제에서 이 키 페어는 이름 `Owner`로 식별되었습니다. 각 키 페어에는 다음 요소가 들어 있습니다.

    - `tag_key` – 백업 계획에 연결할 태그 키 이름을 지정합니다. 이 키에는 @@assign 상속 값 연산자와 문자열 값이 들어 있습니다. 값은 대소문자를 구분합니다.
    - `tag_value` - 백업 계획에 연결되고 `tag_key`와 연결되는 값을 지정합니다. 이 키에는 상속 값 연산자와 유효 정책에서 대체, 추가 또는 제거할 하나 이상의 값이 들어 있습니다. 이러한 값은 대소문자를 구분합니다.

- `regions`

  `regions`정책 키는 키의 조건에 맞는 리소스를 찾기 위해 검색할 대상을 지정합니다. AWS 리전 AWS Backup `selections` 이 키에는 모든 상속 값 연산자와 하나 이상의 AWS 리전 코드 문자열 값이 포함됩니다 (예:`["us-east-1", "eu-north-1"]`.

- `selections`

selections 정책 키는 이 정책의 계획 규칙에 의해 백업되는 리소스를 지정합니다. 이 키는 대략 의 BackupSelection 객체에 해당합니다 AWS Backup. 리소스는 태그 키 이름 및 값을 일치시키는 쿼리에 의해 지정됩니다. selections 키는 그 아래에 하나의 키(tags)를 포함합니다.

- tags – 리소스를 식별하는 태그와, 리소스를 쿼리해서 백업할 수 있는 권한이 있는 IAM 역할을 지정합니다. 이 키의 값에는 다음 요소 중 하나 이상이 포함됩니다.
  - 이 태그 요소의 식별자. 쿼리할 태그의 대/소문자 처리가 다르더라도 tags 아래의 이 식별자는 모두 소문자로 표시된 태그 키 이름입니다. 이 식별자는 대소문자를 구분하지 않습니다. 위의 예제에서 한 요소가 이름 My_Backup_Assignment로 식별되었습니다. tags의 각 식별자에는 다음 요소가 들어 있습니다.
    - iam_role_arn – regions 키로 지정된 AWS 리전 에서 태그 쿼리로 식별된 리소스에 액세스할 수 있는 권한이 있는 IAM 역할을 지정합니다. 이 값에는 @@assign상속 값 연산자와 역할의 ARN이 포함된 문자열 값이 포함됩니다. AWS Backup 이 역할을 사용하여 리소스를 쿼리 및 검색하고 백업을 수행합니다.

      계정 ID 번호 대신 ARN의 $account 변수를 사용할 수 있습니다. 에서 백업 계획을 실행하면 변수가 정책이 실행되고 있는 실제 계정 ID 번호로 자동 대체됩니다. AWS Backup AWS 계정

      > **Important**
      >
      > 백업 계획을 처음 시작할 때 역할이 이미 존재해야 합니다. AWS CloudFormation 스택 세트 및 Organization과의 통합을 사용하여 조직의 각 구성원 계정에 대한 백업 저장소와 IAM 역할을 자동으로 생성하고 구성하는 것이 좋습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 자체 관리 권한으로 스택 세트 만들기를 참조하세요.

    - tag_key - 검색할 태그 키 이름을 지정합니다. 이 키에는 @@assign 상속 값 연산자와 문자열 값이 들어 있습니다. 값은 대소문자를 구분합니다.
    - tag_value- 일치하는 키 이름과 연결되어야 하는 값을 지정합니다. tag_key AWS Backup 와 가 모두 tag_value 일치하는 경우에만 백업에 tag_key 리소스를 포함합니다. 이 키에는 상속 값 연산자와 유효 정책에서 대체, 추가 또는 제거할 하나 이상의 값이 들어 있습니다. 이러한 값은 대소문자를 구분합니다.
- advanced_backup_settings – 특정 백업 시나리오에 대한 설정을 지정합니다. 이 키에는 하나 이상의 설정이 있습니다. 각 설정은 다음 요소를 포함하는 JSON 객체 문자열입니다.
  - 객체 키 이름 - 다음 고급 설정이 적용되는 리소스 유형을 지정하는 문자열입니다.
  - 객체 값 - 연관된 리소스 유형에 특정한 하나 이상의 백업 설정을 포함하는 JSON 객체 문자열입니다.

현재 지원되는 유일한 고급 백업 설정은 Amazon EC2 인스턴스에서 실행 중인 Windows 또는 SQL Server에 대해 Microsoft Volume Shadow Copy Service(VSS) 백업을 사용하는 것입니다. 키 이름은 "ec2" 리소스 유형이어야 하며, 값은 Amazon EC2 인스턴스에서 실행되는 백업에 대해 "windows_vss" 지원을 enabled, 아니면 disabled 여부를 지정합니다. 이 기능에 대한 자세한 내용은 AWS Backup 개발자 안내서의 VSS 지원 Windows 백업 생성을 참조하세요.

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
}
```

- backup_plan_tags – 백업 계획 자체에 연결되는 태그를 지정합니다. 규칙 또는 선택 사항에 지정된 태그에는 영향을 주지 않습니다.

  (선택 사항) 백업 계획에 태그를 연결할 수 있습니다. 이 키의 값은 요소의 모음입니다.

  쿼리할 태그의 대/소문자 처리가 다르더라도 backup_plan_tags 아래의 각 요소에 대한 키 이름은 모두 소문자로 표시된 태그 키 이름입니다. 이 식별자는 대소문자를 구분하지 않습니다. 이러한 각 항목의 값은 다음 키로 구성됩니다.

  - tag_key – 백업 계획에 연결할 태그 키 이름을 지정합니다. 이 키에는 @@assign 상속 값 연산자와 문자열 값이 들어 있습니다. 이 값은 대소문자를 구분합니다.
  - tag_value - 백업 계획에 연결되고 tag_key와 연결되는 값을 지정합니다. 이 키에는 @@assign 상속 값 연산자와 문자열 값이 들어 있습니다. 이 값은 대소문자를 구분합니다.

백업 정책 예제

다음 백업 정책 예제는 정보 제공 용도로만 제공됩니다. 다음 예제 중 일부에서는 공간을 절약하기 위해 JSON 공백 서식이 압축되었을 수 있습니다.

예제 1: 상위 노드에 할당된 정책

다음 예제에서는 계정의 상위 노드 중 하나에 할당된 백업 정책을 보여 줍니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 의도된 계정의 상위 OU에 연결할 수 있습니다.

```
{
```

```
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
```

```
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        }                   }
            }
        },
        "selections": {
            "tags": {
                "datatype": {
                    "iam_role_arn": {
                        "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                    },
                    "tag_key": {
                        "@@assign": "dataType"
                    },
                    "tag_value": {
                        "@@assign": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        },
        "advanced_backup_settings": {
            "ec2": {
                "windows_vss": {
                    "@@assign": "enabled"
                }
            }
```

```
            }
        }
    }
}
```

계정에 상속되거나 계정에 연결된 다른 정책이 없는 경우 각 적용 가능한 정책에서 렌더링된 유효 정책은 다음 예와 AWS 계정 같습니다. CRON 식은 백업을 한 시간에 한 번 실행합니다. 계정 ID 123456789012는 각 계정의 실제 계정 ID입니다.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
```

```
                            "to_delete_after_days": "28",
                            "move_to_cold_storage_after_days": "180"
                        }
                    }
                }
            }
        },
        "selections": {
            "tags": {
                "datatype": {
                    "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                    "tag_key": "dataType",
                    "tag_value": [
                        "PII",
                        "RED"
                    ]
                }
            }
        },
        "advanced_backup_settings": {
            "ec2": {
                "windows_vss": "enabled"
            }
        }
     }
  }
}
```

예제 2: 상위 정책이 하위 정책과 병합

다음 예에서는 상속된 상위 정책과 하위 정책을 상속하거나 AWS 계정 병합에 직접 연결하여 효과적인 정책을 구성합니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 상위 OU에 연결할 수 있습니다.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
```

```
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII", "RED" ] }
                    }
                }
            }
        }
    }
}
```

하위 정책 – 이 정책은 상위 정책이 연결된 수준보다 낮은 수준에서 계정 또는 OU에 직접 연결할 수 있습니다.

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
```

```
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "to_delete_after_days": { "@@assign": "365" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "MonthlyDatatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                            "tag_key": { "@@assign": "BackupType" },
                            "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                        }
                    }
                }
            }
        }
}
```

최종 유효 정책 – 계정에 적용되는 유효 정책에는 각각 자체 규칙 집합과 규칙을 적용할 리소스 집합이 있는 두 개의 계획이 포함됩니다.

```
{
    "plans": {
       "PII_Backup_Plan": {
```

```
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
```

```
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "to_delete_after_days": "365"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "monthlydatatype": {
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
    }
}
```

예제 3: 상위 정책이 하위 정책에 의한 모든 변경을 금지

다음 예제에서 상속된 상위 정책은 하위 제어 연산자를 사용하여 모든 설정을 강제 적용하고 하위 정책이 설정을 변경 또는 재정의하는 것을 금지합니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 상위 OU에 연결할 수 있습니다. 정책의 모든 노드에 `"@@operators_allowed_for_child_policies": ["@@none"]`이 존재한다는 것은 하위 정책이 계획을 변경할 수 없음을 의미합니다. 또한 하위 정책은 유효 정책에 추가 계획을 추가할 수 없습니다. 이 정책은 연결된 OU 아래의 모든 OU 및 계정에 대해 유효한 정책이 됩니다.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
```

```
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "to_delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
```

```
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "to_delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
["@@none"],
                                    "@@assign": "180"
                                }
                            }
                        }
                    }
                },
                "selections": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "tags": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "datatype": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "iam_role_arn": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                            },
                            "tag_key": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": "dataType"
                            },
                            "tag_value": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": [
                                    "PII",
                                    "RED"
                                ]
                            }
                        }
                    }
                },
                "advanced_backup_settings": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                "ec2": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "windows_vss": {
                        "@@assign": "enabled",
                        "@@operators_allowed_for_child_policies": ["@@none"]
                    }
                }
            }
        }
    }
}
```

최종 유효 정책 – 하위 백업 정책이 존재하면 해당 정책이 무시되고 상위 정책이 유효 정책이 됩니다.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
```

```
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

예제 4: 상위 정책이 하위 정책에 의한 한 백업 계획의 변경을 금지

다음 예제에서 상속된 상위 정책은 하위 제어 연산자를 사용하여 단일 계획의 설정을 강제 적용하고 하위 정책이 해당 설정을 변경 또는 재정의하는 것을 금지합니다. 하위 정책은 여전히 추가 계획을 추가할 수 있습니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 상위 OU에 연결할 수 있습니다. 이 예제는 plans 최상위 수준을 제외하고 모든 하위 상속 연산자가 차단된 이전 예제와 유사합니다. 이 수준에서 @@append 설정을 사용하면 하위 정책이 유효 정책의 모음에 다른 계획을 추가할 수 있습니다. 상속된 계획에 대한 변경 사항은 여전히 모두 차단됩니다.

명확성을 위해 계획 섹션은 잘렸습니다.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

하위 정책 – 이 정책은 상위 정책이 연결된 수준보다 낮은 수준에서 계정 또는 OU에 직접 연결할 수 있습니다. 이 하위 정책은 새 계획을 정의합니다.

명확성을 위해 계획 섹션은 잘렸습니다.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

최종 유효 정책 – 유효 정책에는 두 계획이 모두 포함됩니다.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

예제 5: 하위 정책이 상위 정책의 설정을 재정의

다음 예제에서 하위 정책은 값-설정(value-setting) 연산자를 사용하여 상위 정책에서 상속된 설정 일부를 재정의합니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 상위 OU에 연결할 수 있습니다. 해당 작업을 금지하는 하위 제어 연산자가 없는 경우 기본 동작은 하위 정책에 `@@assign`, `@@append` 또는 `@@remove`를 허용하는 것이므로 하위 정책은 모든 설정을 재정의할 수 있습니다. 상위 정책에는 유효한 백업 계획에 필요한 모든 요소가 포함되어 있으므로 정책이 있는 그대로 상속되면 리소스가 성공적으로 백업됩니다.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
```

```
                    }
                }
            }
        }
    }
}
```

하위 정책 – 하위 정책에는 상속된 상위 정책과 달라야 하는 설정만 포함됩니다. 유효 정책으로 병합될 때 다른 필수 설정을 제공하는 상속된 상위 정책이 있어야 합니다. 그렇지 않으면 예상대로 리소스를 백업하지 않는 잘못된 백업 계획이 유효 백업 정책에 포함됩니다.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

최종 유효 정책 – 유효 정책에는 두 정책의 설정이 모두 포함되며 하위 정책이 제공하는 설정은 상위 정책에서 상속된 설정을 재정의합니다. 이 예제에서는 다음과 같이 변경됩니다.

- 리전 목록이 완전히 다른 목록으로 바뀝니다. 상속된 목록에 리전을 추가하려면 하위 정책에 `@@assign` 대신 `@@append`를 사용합니다.
- AWS Backup 매시간이 아닌 격주로 수행합니다.

- AWS Backup 60분이 아닌 80분 동안 백업을 시작할 수 있습니다.
- AWS Backup 대신 `Default` 볼트를 사용합니다`FortKnox`.
- 백업을 콜드 스토리지로 이전 및 최종 삭제하기 위한 수명 주기가 모두 연장됩니다.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
```

```
                }
            }
        }
    }
}
```

태그 정책

태그 정책을 사용하여 태그 키와 태그 값의 기본 대소문자 처리를 포함한 태그를 일관적으로 유지 관리할 수 있습니다.

태그란 무엇입니까?

태그는 사용자 또는 AWS가 AWS 리소스에 할당하는 사용자 지정 속성 레이블입니다. 각 태그에는 다음 두 가지 부분이 있습니다.

- 태그 키(예: `CostCenter`, `Environment` 또는 `Project`) 태그 키는 대/소문자를 구별합니다.
- 태그 값(예: `111122223333` 또는 `Production`)으로 알려진 선택적 필드 태그 값을 생략하는 것은 빈 문자열을 사용하는 것과 같습니다. 태그 키처럼 태그 값은 대/소문자를 구별합니다.

이 페이지의 나머지 부분에서는 태그 정책에 대해 설명합니다. 태그에 대한 자세한 내용은 다음과 같은 소스를 참조하세요.

- 이름 지정 및 사용 규칙을 비롯한 태깅에 대한 일반 정보는 태깅 AWS 리소스 사용 설명서를 참조하십시오.
- 태그 사용을 지원하는 서비스 목록은 Resource Groups Tagging API 참조를 참조하세요.
- 태그를 사용하여 리소스를 분류하는 방법에 대한 자세한 내용은 리소스 태깅 모범 사례 백서를 참조하십시오. AWS
- Organizations 리소스 태그 지정에 대한 자세한 내용은 AWS Organizations 리소스에 태그 지정 단원을 참조하세요.
- 다른 AWS 서비스의 리소스에 태그를 지정하는 방법에 대한 자세한 내용은 해당 서비스의 설명서를 참조하십시오.

태그 정책이란 무엇입니까?

태그 정책은 조직의 계정에 있는 리소스 전체에서 태그를 표준화하는 데 도움이 될 수 있는 정책의 한 유형입니다. 태그 정책에서 리소스에 태그를 지정할 때 리소스에 적용할 수 있는 태그 지정 규칙을 지정합니다.

예를 들어, 태그 정책은 `CostCenter` 태그가 리소스에 연결될 때 태그 정책에 정의된 대소문자 처리 및 태그 값을 사용해야 하도록 지정할 수 있습니다. 태그 정책은 지정된 리소스 유형에 대한 정책 미준수 태그 지정 작업이 적용되도록 지정할 수도 있습니다. 다시 말해서, 지정된 리소스 유형에 대한 정책 미준수 태그 지정 요청은 완료할 수 없습니다. 태그 없는 리소스 또는 태그 정책에서 정의되지 않은 태그는 태그 정책 준수 여부가 평가되지 않습니다.

태그 정책을 사용하려면 다음과 같은 여러 AWS 서비스에서 작업해야 합니다.

- AWS Organizations를 사용하여 태그 정책을 관리합니다. 조직의 관리 계정에 로그인하고 Organizations를 사용하여 태그 정책 기능을 활성화합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다. 그런 다음 태그 정책을 생성하고 조직 엔터티에 연결하여 해당 태그 규칙을 적용할 수 있습니다.
- AWS Resource Groups를 사용하여 태그 정책 준수를 관리합니다. 조직의 계정에 로그인하고 Resource Groups를 사용하여 계정의 리소스에서 정책 미준수 태그를 찾습니다. 리소스를 생성한 AWS 서비스에서 정책 미준수 태그를 수정할 수 있습니다.

  조직의 관리 계정에 로그인하면 조직의 모든 계정에 대한 정책 준수 정보를 볼 수 있습니다.

태그 정책은 모든 기능이 활성화된 조직에서만 사용할 수 있습니다. 태그 정책을 사용하는 데 필요한 항목에 대한 자세한 내용은 태그 정책 관리를 위한 사전 조건 및 권한 단원을 참조하세요.

> **Important**
>
> 태그 정책을 시작하려면 AWS에서 고급 태그 정책으로 이동하기 전에 태그 정책 시작하기에서 설명하는 예제 워크플로우를 따르는 것이 좋습니다. 태그 정책을 전체 OU 또는 조직으로 확장하기 전에 간단한 태그 정책을 단일 계정에 연결하는 효과를 이해하는 것이 가장 좋습니다. 태그 정책 준수를 적용하기 전에 태그 정책의 효과를 이해하는 것이 특히 중요합니다. 태그 정책 시작하기 페이지의 표에는 고급 정책 관련 작업에 대한 지침의 링크도 제공됩니다.

태그 정책 관리를 위한 사전 조건 및 권한

이 페이지에서는 AWS Organizations에서 태그 정책을 관리하기 위한 사전 조건 및 필수 권한에 대해 설명합니다.

주제

태그 정책 관리를 위한 사전 조건

태그 정책을 사용하려면 다음이 필요합니다.

- 조직의 모든 기능을 활성화해야 합니다.
- 조직의 관리 계정에 로그인해야 합니다.
- 태그 정책 관리 권한에 나열된 권한이 필요합니다.

태그 정책 준수 여부를 평가하려면 AWS Resource Groups를 사용합니다. 규정 준수 평가에 대한 요구 사항에 대한 자세한 내용은 AWS Resource Groups 사용 설명서의 사전 조건 및 권한을 참조하세요.

태그 정책 관리 권한

다음 IAM 정책 예제는 태그 정책을 관리하기 위한 권한을 제공합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
```

```
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM 정책 및 권한에 대한 자세한 내용은 IAM 사용 설명서를 참조하세요.

태그 정책 사용에 대한 모범 사례

AWS에서는 태그 정책 사용에 대해 다음과 같은 모범 사례를 권장합니다.

태그 대소문자 전략 결정

태그를 대문자로 전환하고 모든 리소스 유형에서 해당 정책을 일관적으로 구현하는 방법을 결정합니다. 예를 들어, `Costcenter`, `costcenter` 또는 `CostCenter`를 사용할지 결정하고 모든 태그에 대해 동일한 규칙을 사용합니다. 정책 준수 보고서에서 일관된 결과를 얻으려면 일관되지 않은 대소문자 처리와 비슷한 태그를 사용하지 마세요. 이 전략은 조직의 태그 정책을 정의하는 데 도움이 됩니다.

권장 워크플로우 사용

간단한 태그 정책을 생성하여 소규모로 시작합니다. 그런 다음 테스트용으로 사용할 수 있는 멤버 계정에 연결합니다. 태그 정책 시작하기에서 설명하는 워크플로우를 사용합니다.

태그 지정 규칙 결정

이 항목은 조직의 필요에 따라 결정됩니다. 예를 들어 `CostCenter` 보안 암호에 AWS Secrets Manager 태그가 연결될 때 지정된 대소문자 처리를 사용하도록 지정할 수 있습니다. 정책 준수 태그를 정의하는 태그 정책을 생성하고 해당 태그 지정 규칙을 적용할 조직 엔터티에 태그 정책을 연결합니다.

계정 관리자 교육

태그 정책 사용을 확장할 준비가 되면 계정 관리자를 다음과 같이 교육합니다.

- 태그 지정 전략을 전달합니다.
- 관리자가 특정 리소스 유형에서 태그를 사용해야 한다는 점을 강조합니다.

  태그가 없는 리소스는 정책 준수 결과에서 정책 미준수로 표시되지 않으므로 이렇게 하는 것이 중요합니다.
- 태그 정책 준수 확인에 대한 지침을 제공합니다. 관리자에게 AWS Resource Groups 사용 설명서의 계정 정책 준수 평가에 설명된 절차를 사용하여 계정의 리소스에서 정책 미준수 태그를 찾고 수정할 수 있는 지침을 제시합니다. 정책 준수 여부를 확인할 빈도를 관리자에게 알려줍니다.

정책 준수 적용 시 주의

정책 준수를 적용하면 조직의 계정에 있는 사용자가 필요한 리소스에 태그를 지정할 수 없습니다. 적용 이해의 정보를 검토합니다. 태그 정책 시작하기에서 설명하는 워크플로우도 참조합니다.

리소스 생성 요청에 대한 가드레일을 설정하는 SCP 생성 고려

태그가 연결되지 않은 리소스는 보고서에서 정책 미준수로 표시되지 않습니다. 계정 관리자는 여전히 태그 없는 리소스를 생성할 수 있습니다. 경우에 따라, SCP(서비스 제어 정책)를 사용하여 리소스 생성 요청에 대한 가드레일을 설정할 수 있습니다. SCP 예제는 생성되는 특정 리소스에 대한 태그 요구 단원을 참조하세요. AWS 서비스가 태그를 사용한 액세스 제어를 지원하는지 여부를 알아보려면 IAM 사용 설명서의 IAM과 함께 작업하는 AWS 서비스를 참조하세요. 태그 기반 권한 부여(Authorization based on tags) 열이 예(Yes)로 표시된 서비스를 찾습니다. 서비스의 이름을 선택하여 해당 서비스에 대한 권한 부여 및 액세스 제어 문서를 봅니다.

태그 정책 시작하기

태그 정책을 사용하려면 여러 AWS 서비스를 사용해야 합니다. 시작하려면 다음 페이지를 검토하세요. 그런 다음 이 페이지의 워크플로우에 따라 태그 정책 및 해당 효과에 대해 잘 알아두세요.

- 태그 정책 관리를 위한 사전 조건 및 권한

- 태그 정책 사용에 대한 모범 사례

처음으로 태그 정책 사용

다음 단계에 따라 처음으로 태그 정책 사용을 시작합니다.

작업	로그인할 계정	AWS 사용할 서비스 콘솔
1단계: 조직에 대해 태그 정책을 활성화합니다.	조직의 관리 계정.[1]	AWS Organizations
2단계: 태그 정책을 생성합니다. 첫 번째 태그 정책을 간단하게 유지합니다. 사용할 대소문자 처리에 태그 키 하나를 입력하고 다른 모든 옵션은 기본값으로 둡니다.	조직의 관리 계정.[1]	AWS Organizations
3단계: 테스트에 사용할 수 있는 단일 멤버 계정에 태그 정책을 연결합니다. 다음 단계에서 이 계정에 로그인해야 합니다.	조직의 관리 계정.[1]	AWS Organizations
4단계: 정책 준수 태그가 있는 일부 리소스와 정책 미준수 태그가 있는 일부 리소스를 생성합니다.	테스트 용도로 사용하는 멤버 계정.	편안하게 이용할 수 있는 모든 AWS 서비스. 예를 들어, AWS Secrets Manager을 사용하고 기본 암호 생성의 절차를 따라 정책 준수 암호 및 정책 미준수 암호를 포함한 암호를 생성합니다.
5단계: 유효 태그 정책을 보고 계정의 정책 준수 상태를 평가합니다.	테스트 용도로 사용하는 멤버 계정.	Resource Groups 및 리소스가 생성된 AWS 서비스.

작업	로그인할 계정	AWS 사용할 서비스 콘솔
		정책 준수 태그와 정책 미준수 태그를 사용하여 리소스를 생성한 경우 결과에 정책 미준수 태그가 표시되어야 합니다.
6단계: 테스트 계정의 리소스가 태그 정책을 준수할 때까지 정책 준수 문제를 찾아서 수정하는 프로세스를 반복합니다.	테스트 용도로 사용하는 멤버 계정.	Resource Groups 및 리소스가 생성된 AWS 서비스.
언제든지 조직 전체의 정책 준수 여부를 평가할 수 있습니다.	조직의 관리 계정.[1]	Resource Groups

[1] 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

태그 정책 사용 확장

다음 작업을 어떤 순서로든 수행하여 태그 정책 사용을 확장할 수 있습니다.

고급 작업	로그인할 계정	AWS 사용할 서비스 콘솔
고급 태그 정책을 생성합니다. 처음 사용자와 동일한 프로세스를 따르지만, 다른 작업을 시도해 봅니다. 예를 들어, 추가 키 또는 값을 정의하거나 태그 키에 다른 대소문자 처리를 지정합니다. 관리 정책 상속에 대한 이해 및 태그 정책 구문의 정보를 사용하여 더 세부적인 태그 정책을 생성할 수 있습니다.	조직의 관리 계정.[1]	AWS Organizations

고급 작업	로그인할 계정	AWS 사용할 서비스 콘솔
추가 계정 또는 OU에 태그 정책을 연결합니다. 추가 정책을 계정에 연결하거나 계정이 멤버로 속한 OU에 연결한 후 계정에 대한 유효 태그 정책을 확인합니다.	조직의 관리 계정.[1]	AWS Organizations
다른 사람이 새 리소스를 생성할 때 태그를 반드시 사용하도록 하는 SCP를 생성합니다. 예시는 생성되는 특정 리소스에 대한 태그 요구단원을 참조하세요.	조직의 관리 계정.[1]	AWS Organizations
변경하는 동안 유효 태그 정책에 대해 계정의 정책 준수 상태를 계속 평가합니다. 정책 미준수 태그를 수정합니다.	유효한 태그 정책이 있는 멤버 계정.	Resource Groups 및 리소스가 생성된 AWS 서비스.
조직 전체의 정책 준수를 평가합니다.	조직의 관리 계정.[1]	Resource Groups

[1] 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

처음으로 태그 정책 적용

태그 정책을 처음 적용하려면 태그 정책을 처음 사용하는 것과 비슷한 워크플로우를 따르고 테스트 계정을 사용합니다.

> **Warning**
>
> 정책 준수를 적용할 때는 주의하세요. 태그 정책 사용의 효과를 이해하고 권장 워크플로우를 따라야 합니다. 추가 계정으로 확장하기 전에 테스트 계정에서 적용이 어떻게 작동하는지 테스

트합니다. 그렇지 않으면 조직의 계정에 있는 사용자가 필요한 리소스에 태그를 지정하지 못하도록 할 수 있습니다. 자세한 정보는 적용 이해 섹션을 참조하세요.

적용 작업	로그인할 계정	AWS 사용할 서비스 콘솔
1단계: 태그 정책을 생성합니다. 첫 번째 적용된 태그 정책을 간단하게 유지합니다. 사용할 대소문자 처리에 태그 키 하나를 입력하고 이 태그에 대해 정책 미준수 작업 금지 옵션을 선택합니다. 그런 다음 적용할 리소스 유형 하나를 지정합니다. 이전의 예제를 계속 사용하여 Secrets Manager 암호에 태그 정책을 적용하도록 선택할 수 있습니다.	조직의 관리 계정.[1]	AWS Organizations
2단계: 단일 테스트 계정에 태그 정책을 연결합니다.	조직의 관리 계정.[1]	AWS Organizations
3단계: 정책 준수 태그가 있는 일부 리소스와 정책 미준수 태그가 있는 일부 리소스를 생성해 봅니다. 정책 미준수 태그를 사용하여 태그 정책에서 지정된 유형의 리소스에 태그를 생성할 수 없습니다.	테스트 용도로 사용하는 멤버 계정.	편안하게 이용할 수 있는 모든 AWS 서비스. 예를 들어, AWS Secrets Manager을 사용하고 기본 암호 생성의 절차를 따라 정책 준수 암호 및 정책 미준수 암호를 포함한 암호를 생성합니다.
4단계: 유효 태그 정책에 대해 계정의 정책 준수 상태를 평가하고 정책 미준수 태그를 수정합니다.	테스트 용도로 사용하는 멤버 계정.	Resource Groups 및 리소스가 생성된 AWS 서비스.

적용 작업	로그인할 계정	AWS 사용할 서비스 콘솔
5단계: 테스트 계정의 리소스가 태그 정책을 준수할 때까지 정책 준수 문제를 찾아서 수정하는 프로세스를 반복합니다.	테스트 용도로 사용하는 멤버 계정.	Resource Groups 및 리소스가 생성된 AWS 서비스.
언제든지 조직 전체의 정책 준수 여부를 평가할 수 있습니다.	조직의 관리 계정.[1]	Resource Groups

[1] 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

태그 정책 생성, 업데이트 및 삭제

이 주제에서 수행할 작업

- 조직에 대해 태그 정책을 활성화한 후에 태그 정책을 생성할 수 있습니다.
- 태그 지정 요구 사항이 변경되면 기존 정책을 업데이트할 수 있습니다.
- 정책이 더 이상 필요하지 않은 경우 모든 조직 단위(OU) 및 계정에서 정책을 분리한 후 삭제할 수 있습니다.

> **Important**
> 태그가 지정되지 않은 리소스는 결과에 정책 미준수로 나타나지 않습니다.

태그 정책 생성

> **최소 권한**
> 태그 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.
>
> - `organizations:CreatePolicy`

다음 두 가지 방법 중 하나를 사용하여 AWS Management Console에서 태그 정책을 생성할 수 있습니다.

- 사용자가 옵션을 선택하면 자동으로 JSON 정책 텍스트를 생성하는 시각적 편집기.
- 사용자가 직접 JSON 정책 텍스트를 작성할 수 있는 텍스트 편집기.

시각적 편집기를 사용하면 프로세스를 쉽게 수행할 수 있지만 유연성은 제한됩니다. 이는 처음 정책을 생성하여 편안하게 사용할 수 있는 좋은 방법입니다. 정책이 어떻게 작동하는지 이해하고 시각적 편집기가 제공하는 기능에 의해 제한되기 시작하면 JSON 정책 텍스트를 직접 편집하여 정책에 고급 기능을 추가할 수 있습니다. 시각적 편집기는 @@assign value-setting 연산자만 사용하며, 하위 제어 연산자에 대한 액세스 권한을 제공하지 않습니다. 하위 제어 연산자는 JSON 정책 텍스트를 수동으로 편집하는 경우에만 추가할 수 있습니다.

AWS Management Console

태그 정책을 생성하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 태그 정책(Tag policies) 페이지에서 정책 생성(Create policy)을 선택합니다.
3. 정책 생성(Create policy) 페이지에서 정책 이름(Policy name) 및 정책 설명(Policy description)(선택 사항)을 입력합니다.
4. (선택 사항) 정책 객체 자체에 하나 이상의 태그를 추가할 수 있습니다. 이러한 태그는 정책에 포함되지 않습니다. 이렇게 하려면 태그 추가(Add tag)를 선택한 다음 키 및 값(선택 사항)을 입력합니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 정보는 AWS Organizations 리소스에 태그 지정 섹션을 참조하세요.
5. 이 절차의 설명과 같이 시각적 편집기를 사용하여 태그 정책을 빌드할 수 있습니다. JSON 탭에서 태그 정책을 입력하거나 붙여 넣을 수도 있습니다. 태그 정책 구문에 대한 자세한 내용은 태그 정책 구문 단원을 참조하세요.

   새 태그 키 1(New tag key 1)에서 추가할 태그 키의 이름을 지정합니다.
6. 태그 키 대소문자 정책 준수(Tag key capitalization compliance)에서, 상속된 상위 태그 정책이 있는 경우 해당 정책이 태그 키의 대/소문자 처리를 정의하도록 지정하려면 이 옵션을 선택 취소된(기본값) 상태로 둡니다.

   이 정책을 사용하여 태그 키에 특정 대소문자를 강제하려면 이 옵션을 활성화합니다. 이 옵션을 선택하면 태그 키에 대해 지정한 대소문자 처리가 상속된 상위 정책에 지정된 대소문자 처리를 재정의합니다.

상위 정책이 존재하지 않고 이 옵션을 활성화하지 않으면 모든 소문자의 태그 키만 정책을 준수하는 것으로 간주됩니다. 상위 정책으로부터의 상속에 관한 자세한 내용은 관리 정책 상속에 대한 이해 단원을 참조하세요.

> **Tip**
>
> 태그 키와 해당 대소문자 처리를 정의하는 태그 키를 생성할 때 예제 1: 조직 전체의 태그 키 사례 정의에 표시된 태그 정책 예제를 가이드로 사용할 수 있습니다. 이 태그 정책을 조직 루트에 연결합니다. 나중에 추가 태그 정책을 생성하고 OU 또는 계정에 연결하여 추가 태그 규칙을 생성할 수 있습니다.

7. 태그 값 정책 준수(Tag value compliance)의 경우 해당 태그 키에 허용되는 값을 상위 정책에서 상속된 모든 값에 추가하려면 이 옵션을 활성화합니다.

   기본적으로 이 옵션은 선택 취소되어 있으므로 상위 정책에서 정의되고 상속된 값만 정책을 준수하는 것으로 간주됩니다. 상위 정책이 없거나 태그 값을 지정하지 않는 경우 모든 값(값 없음 포함)이 정책을 준수하는 것으로 간주됩니다.

   허용 가능한 태그 값 목록을 업데이트하려면 이 태그 키에 허용되는 값 지정(Specify allowed values for this tag key)을 선택한 다음 값 지정(Specify values)을 선택합니다. 메시지가 표시되면 새 값(상자당 하나의 값)을 입력하고 변경 사항 저장(Save changes)을 선택합니다.

8. 이 태그에 대한 정책 미준수 작업 금지(Prevent noncompliant operations for this tag)의 경우 태그 정책을 사용한 경험이 없으면 이 옵션을 선택 취소(기본값)된 상태로 두는 것이 좋습니다. 적용 이해에서 권장 사항을 검토했는지 확인하고 철저히 테스트합니다. 그렇지 않으면 조직의 계정에 있는 사용자가 필요한 리소스에 태그를 지정하지 못하도록 할 수 있습니다.

   이 태그 키에 정책 준수를 적용하지 않으려면 확인란을 선택한 다음 리소스 유형 지정(Specify resource types)을 선택합니다. 메시지가 표시되면 정책에 포함할 리소스 유형을 선택합니다. 변경 사항 저장(Save changes)을 선택합니다.

   > **Important**
   >
   > 이 옵션을 선택하면 지정된 유형의 리소스에 대한 태그를 조작하는 모든 작업은 해당 작업의 결과로 태그가 정책을 준수하게 되는 경우에만 성공합니다.

9. (선택 사항) 이 태그 정책에 다른 태그 키를 추가하려면 태그 키 추가를 선택합니다. 그런 다음 6~9단계를 수행하여 태그 키를 정의합니다.

10. 태그 정책 빌드를 완료하면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

태그 정책을 생성하려면

다음 중 하나를 사용하여 태그 정책을 생성할 수 있습니다.

- AWS CLI: create-policy

  어떤 텍스트 편집기든 사용하여 태그 정책을 생성할 수 있습니다. JSON 구문을 사용하여 태그 정책을 선택한 위치에 어떤 이름과 확장명으로든 파일로 저장합니다. 태그 정책은 공백을 포함하여 최대 2,500자를 사용할 수 있습니다. 태그 정책 구문에 대한 자세한 내용은 태그 정책 구문 단원을 참조하세요.

  태그 정책을 생성하려면

  1. 텍스트 파일에 다음과 유사한 태그 정책을 만듭니다.

     `testpolicy.json`의 콘텐츠:

     ```
     {
         "tags": {
             "CostCenter": {
                 "tag_key": {
                     "@@assign": "CostCenter"
                 }
             }
         }
     }
     ```

     이 태그 정책은 `CostCenter` 태그 키를 정의합니다. 태그는 어떠한 값이든 수락하거나 값을 수락하지 않을 수 있습니다. 이와 같은 정책은 값이 있거나 없는 CostCenter 태그가 연결된 리소스가 규정을 준수함을 의미합니다.
  2. 파일의 정책 콘텐츠를 담은 정책을 생성합니다. 읽기 쉽도록 출력의 여분의 공백을 잘랐습니다.

     ```
     $ aws organizations create-policy \
         --name "MyTestTagPolicy" \
         --description "My Test policy" \
         --content file://testpolicy.json \
     ```

```
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

- AWS SDK: CreatePolicy

다음에 수행할 작업

태그 정책을 생성한 후에는 태그 지정 규칙을 적용할 수 있습니다. 이를 위해 조직 루트, 조직 단위(OU), 조직 내 AWS 계정, 또는 조직 엔터티의 조합에 정책을 연결합니다.

태그 정책 업데이트

> 최소 권한
>
> 태그 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 organizations:UpdatePolicy
> - 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 organizations:DescribePolicy

AWS Management Console

태그 정책을 업데이트하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 태그 정책(Tag policies) 페이지에서 업데이트할 태그 정책을 선택합니다.
3. 정책 편집을 선택합니다.
4. 새로운 정책 이름, 정책 설명을 입력할 수 있습니다. 정책 내용은 시각적 편집기를 사용하거나 JSON을 편집해 변경할 수 있습니다.
5. 태그 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

다음 중 하나를 사용하여 정책을 업데이트할 수 있습니다.

- AWS CLI: update-policy

  다음 예제에서는 태그 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

다음 예제에서는 태그 정책에 대한 설명을 추가하거나 변경합니다.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

다음 예제에서는 AI 서비스 옵트아웃 정책에 연결된 JSON 정책 문서를 변경합니다. 이 예제에서 콘텐츠는 다음 텍스트를 포함한 `policy.json`이라는 파일에서 가져옵니다.

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWS SDK: UpdatePolicy

태그 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하여 태그 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

최소 권한

AWS 조직의 태그 정책에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization`(콘솔만 해당 - 정책으로 이동하기 위해)
- `organizations:DescribePolicy`(콘솔만 해당 - 정책으로 이동하기 위해)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

AI 서비스 옵트아웃 정책에 연결된 태그를 편집하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. 태그 정책(Tag policies) 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 선택한 정책의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.
   - 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
   - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
   - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 `null`이 아닌 빈 문자열이 됩니다.
5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

태그 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 태그 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: tag-resource 및 untag-resource
- AWS SDK: TagResource 및 UntagResource

태그 정책 삭제

조직의 관리 계정에 로그인하면 조직에서 더 이상 필요 없는 정책을 삭제할 수 있습니다.

정책을 삭제하기 전에 먼저 연결된 모든 개체에서 정책을 분리해야 합니다.

> 최소 권한
>
> 태그 정책을 삭제하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - `organizations:DeletePolicy`

AWS Management Console

태그 정책을 삭제하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2.
3. 태그 정책(Tag policies) 페이지에서 삭제할 정책을 선택합니다.
4. 먼저 모든 루트, OU와 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다.
5. 페이지 상단에서 삭제(Delete)를 선택합니다.
6. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제(Delete)를 선택합니다.

AWS CLI & AWS SDKs

태그 정책을 삭제하려면

다음 중 하나를 사용하여 정책을 삭제할 수 있습니다.

- AWS CLI: delete-policy

  다음 예제에서는 지정한 정책을 삭제합니다. 정책이 루트, OU 또는 계정에 연결되지 않은 경우에만 작동합니다.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: DeletePolicy

태그 정책 연결 및 분리

전체 조직뿐 아니라 OU(조직 단위) 및 개별 계정에서도 태그 정책을 사용할 수 있습니다.

- 태그 정책을 조직 루트에 연결하면 태그 정책은 해당 루트의 모든 멤버 OU 및 계정에 모두 적용됩니다.

- 태그 정책을 OU에 연결하면 해당 태그 정책은 OU에 속한 계정에 적용됩니다. 이러한 계정에는 조직 루트에 연결된 태그 정책이 적용됩니다.
- 태그 정책을 계정에 연결하면 해당 태그 정책은 계정에 적용됩니다. 또한 해당 계정에는 조직 루트에 연결된 태그 정책 외에도 계정이 속한 OU에 연결된 모든 태그 정책이 적용됩니다.

계정이 상속하는 태그 정책과 계정에 직접 연결된 태그 정책을 집계한 것이 유효 태그 정책입니다. 자세한 내용은 관리 정책 상속에 대한 이해 섹션을 참조하세요.

Important

태그가 지정되지 않은 리소스는 결과에 정책 미준수로 나타나지 않습니다.

최소 권한

태그 정책을 연결하려면 다음 작업을 실행할 권한이 있어야 합니다.

- `organizations:AttachPolicy`

AWS Management Console

정책을 탐색하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 태그 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 태그 정책을 연결하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책(Policies) 탭의 태그 정책에 대한 항목에서 연결(Attach)을 선택합니다.
4. 원하는 정책을 찾아서 정책 연결(Attach policy)을 선택합니다.

   정책(Policies) 탭의 연결된 태그 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 태그 정책을 연결하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 태그 정책(Tag policies) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
5. 정책 연결(Attach policies)을 선택합니다.

   대상(Targets) 탭의 연결된 태그 정책 목록이 업데이트되어 새 추가 기능이 목록에 포함됩니다. 정책 변경은 즉시 적용됩니다.

AWS CLI & AWS SDKs

태그 정책을 조직 루트, OU 또는 계정에 연결하려면

다음 중 하나를 사용하여 태그 정책을 연결할 수 있습니다.

- AWS CLI: attach-policy

  다음 절차에서는 방금 생성한 태그 정책을 단일 테스트 계정에 연결하는 방법을 보여 줍니다.

  - 다음과 같이 명령을 실행하여 태그 정책을 테스트 계정에 연결합니다.

    ```
    $ aws organizations attach-policy \
        --target-id <account-id> \
        --policy-id p-a1b2c3d4e5
    ```

    성공하면 이 명령에 출력이 없습니다.

- AWS SDK: AttachPolicy

정책 변경은 즉시 적용됩니다.

다음에 수행할 작업

태그 정책을 연결한 후 자신의 리소스가 해당 태그 정책을 얼마나 준수하는지 알아볼 수 있습니다. 이를 위해 Resource Groups 콘솔을 사용합니다. 자세한 내용은 AWS Resource Groups 사용 설명서에서 계정의 규정 준수 평가를 참조하세요.

태그 정책 분리

조직의 관리 계정에 로그인하면 연결된 루트, OU 또는 계정에서 태그 정책을 분리할 수 있습니다. 엔터티에서 태그 정책을 분리한 후 해당 정책은 현재 분리된 엔터티의 영향을 받았던 모든 계정에 더 이상 적용되지 않습니다. 정책을 분리하려면 다음 단계를 완료하세요.

> **최소 권한**
>
> 조직 루트, OU 또는 계정에서 태그 정책을 분리하려면 다음 작업을 실행할 권한이 있어야 합니다.
>
> - `organizations:DetachPolicy`

AWS Management Console

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 태그 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 태그 정책을 분리하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책(Policies) 탭에서, 분리할 태그 정책 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

   연결된 태그 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 태그 정책을 분리하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 태그 정책(Tag policies) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

   연결된 태그 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

AWS CLI & AWS SDKs

조직 루트, OU 또는 계정에서 태그 정책을 분리하려면

다음 중 하나를 사용하여 태그 정책을 분리할 수 있습니다.

- AWS CLI: detach-policy
- AWS SDK: DetachPolicy

정책 변경은 즉시 적용됩니다.

유효 태그 정책 보기

계정에서 태그가 지정된 리소스의 정책 준수 상태를 확인하려면 먼저 계정에 대한 유효 태그 정책을 확인하는 것이 좋습니다.

유효 태그 정책이란 무엇입니까?

유효 태그 정책은 계정에 적용되는 태그 지정 규칙을 지정합니다. 유효 태그 정책은 계정이 상속하는 태그 정책과 계정에 직접 연결된 태그 정책을 집계한 것입니다. 태그 정책을 조직 루트에 연결하면 해당 태그 정책은 조직의 모든 계정에 적용됩니다. 태그 정책을 OU에 연결하면 해당 태그 정책은 OU에 속한 모든 계정과 OU에 적용됩니다.

예를 들어, 조직 루트에 연결된 태그 정책은 4개의 정책 준수 값이 있는 CostCenter 태그를 정의할 수 있습니다. 계정에 연결된 별도의 태그 정책은 CostCenter 키를 4개의 정책 준수 값 중 두 개로만 제한할 수 있습니다. 이러한 태그 정책의 조합으로 유효 태그 정책이 구성됩니다. 결과적으로 조직 루트 태그 정책에 정의된 4개의 정책 준수 태그 값 중 두 개만 계정에 대해 호환됩니다.

유효 태그 정책을 생성하는 방법에 대한 자세한 내용과 고급 예제는 관리 정책 상속에 대한 이해 단원을 참조하세요.

유효 태그 정책을 보는 방법

AWS Management Console, AWS API 또는 AWS Command Line Interface에서 계정에 대한 유효 태그 정책을 볼 수 있습니다.

> 최소 권한
>
> 계정에 대한 유효 태그 정책을 보려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization`

AWS Management Console

계정에 대한 유효 태그 정책을 보려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 유효 태그 정책을 보려는 계정의 이름을 선택합니다. 원하는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책(Policies) 탭의 태그 정책(Tag policies) 섹션에서 이 AWS 계정 계정에 대한 유효 태그 정책 보기(View the effective tag policy for this AWS 계정)를 선택합니다.

   지정한 계정에 적용되는 유효 정책이 콘솔에 표시됩니다.

> **Note**
>
> 중요한 변경 없이 유효 태그 정책을 복사하여 붙여넣고 다른 백업 정책의 JSON으로 사용할 수는 없습니다. 태그 정책 문서에는 각 설정이 최종 유효 정책으로 병합되는 방법을 지정하는 상속 연산자가 포함되어야 합니다.

AWS CLI & AWS SDKs

계정에 대한 유효 태그 정책을 보려면

다음 중 하나를 사용하여 유효 태그 정책을 볼 수 있습니다.

- AWS CLI: describe-effective-policy

  어떤 태그 지정 규칙이 계정에 상속되거나 연결되는지를 확인하려면 계정에서 다음을 실행하고 결과를 파일에 저장합니다.

```
$ aws organizations describe-effective-policy \
    --policy-type TAG_POLICY
{
    "EffectivePolicy": {
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],
\"tag_key\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
}
```

  태그 정책이 계정뿐 아니라 루트 또는 OU에도 연결되는 경우 상속된 모든 정책의 조합으로 계정의 유효 태그 정책이 정의됩니다. 이러한 경우 계정에서 `describe-effective-policy`를 실행하면 계정의 계층 구조 내에 있는 모든 태그 정책을 병합한 내용이 반환됩니다.

- AWS SDK: DescribeEffectivePolicy

Amazon EventBridge를 사용하여 정책 미준수 태그 모니터링

Amazon EventBridge(이전 Amazon CloudWatch Events)를 사용하여 정책 미준수 태그가 언제 도입되는지 모니터링할 수 있습니다. 다음 예제 이벤트에서 `tag-policy-compliant`의 `"false"` 값은 새 태그가 유효 태그 정책을 준수하지 않음을 나타냅니다.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

이벤트를 구독하고 모니터링할 문자열이나 패턴을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.

적용 이해

태그 정책은 지정된 리소스 유형에 대한 정책 미준수 태그 지정 작업이 적용되도록 지정할 수 있습니다. 다시 말해서, 지정된 리소스 유형에 대한 정책 미준수 태그 지정 요청은 완료할 수 없습니다.

> **Important**
>
> 태그 없이 생성된 리소스는 적용의 영향을 받지 않습니다.

태그 정책 준수를 적용하려면 태그 정책을 생성할 때 다음 중 하나를 수행하세요.

- Visual editor(시각적 편집기) 탭에서 Prevent noncompliant operations for this tag(이 태그의 정책 미준수 작업 금지)를 선택합니다.
- JSON 탭에서 `enforced_for` 필드를 사용합니다. 태그 정책 구문에 대한 자세한 내용은 태그 정책 구문 및 예제 단원을 참조하세요.

태그 정책 준수를 적용하려면 다음 모범 사례를 따르세요.

- 정책 준수 적용 시 주의 – 태그 정책 사용의 효과를 이해하고 태그 정책 시작하기에서 설명하는 권장 워크플로우를 따라야 합니다. 추가 계정으로 확장하기 전에 테스트 계정에서 적용이 어떻게 작동하는지 테스트합니다. 그렇지 않으면 조직의 계정에 있는 사용자가 필요한 리소스에 태그를 지정하지 못하도록 할 수 있습니다.
- 적용할 수 있는 리소스 유형에 유의 – 지원되는 리소스 유형에 대해서만 태그 정책 준수를 적용할 수 있습니다. 시각적 편집기를 사용하여 태그 정책을 빌드할 때 정책 준수 적용을 지원하는 리소스 유형이 나열됩니다.
- 일부 서비스와의 상호 작용 이해 — 일부 AWS 서비스에는 리소스를 자동으로 생성하는 컨테이너와 같은 리소스 그룹이 있으며 태그는 한 서비스의 리소스에서 다른 리소스로 전파될 수 있습니다. 예를 들어 Amazon EC2 Auto Scaling 그룹 및 Amazon EMR 클러스터의 태그는 포함된 Amazon EC2 인스턴스에 자동으로 전파될 수 있습니다. Auto Scaling 그룹 또는 EMR 클러스터보다 엄격한 Amazon EC2에 대한 태그 정책이 있을 수 있습니다. 적용을 활성화하면 태그 정책에 따라 리소스에 태그가 지정되지 않으며 동적 조정 및 프로비저닝이 차단될 수 있습니다.

다음 단원에서는 정책 미준수 리소스를 찾아서 올바르게 수정하는 방법을 보여 줍니다.

계정의 정책 미준수 리소스 찾기

각 계정에 대해 정책 미준수 리소스에 대한 정보를 가져올 수 있습니다. 계정에 리소스가 있는 모든 리전에서 이 명령을 실행해야 합니다.

태그 정책을 사용하는 계정의 비준수 리소스를 찾으려면 다음 명령어를 실행하여 결과를 파일에 저장하세요.

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

리소스에서 정책 미준수 태그 수정

정책 미준수 태그를 찾은 후에는 다음 방법 중 하나를 사용하여 수정합니다. 정책 미준수 태그가 포함된 리소스가 있는 계정에 로그인해야 합니다.

- 비준수 리소스를 생성한 AWS 서비스의 콘솔 또는 태깅 API 작업을 사용하십시오.
- AWS Resource Groups TagResources및 UntagResources작업을 사용하여 효과적인 정책을 준수하는 태그를 추가하거나 규정을 준수하지 않는 태그를 제거할 수 있습니다.

추가 정책 미준수 문제 찾기 및 수정

정책 준수 문제를 찾아서 수정하는 것은 반복적인 프로세스입니다. 관리하는 리소스가 태그 정책을 준수할 때까지 이전 두 단원의 단계를 반복합니다.

조직 전체의 정책 준수 보고서 생성

언제든지 조직 전체에서 태그가 지정된 모든 리소스를 나열하는 보고서를 생성할 수 있습니다. AWS 계정 보고서에는 각 리소스가 유효 태그 정책을 준수하는지 여부가 표시됩니다. 태그 정책 또는 리소스에 대한 변경 사항이 조직 전체의 정책 준수 보고서에 반영되려면 최대 48시간까지 걸릴 수 있습니다. 예를 들어, 한 리소스 유형에 대해 표준화된 새 태그를 정의하는 태그 정책이 있다고 가정합니다. 이 태그가 없는 해당 유형의 리소스는 최대 48시간 동안 보고서에서 정책을 준수하는 것으로 표시됩니다.

Amazon S3 버킷에 대한 액세스 권한이 있는 경우 `us-east-1` 리전에 있는 조직의 관리 계정에서 보고서를 생성할 수 있습니다. 버킷에는 보고서 저장을 위한 Amazon S3 버킷 정책에 표시된 것과 같은 연결된 버킷 정책이 있어야 합니다. 보고서를 생성하려면 다음 명령을 실행합니다.

```
$ aws resourcegroupstaggingapi get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

한 번에 하나의 보고서를 생성할 수 있습니다.

이 보고서를 완료하려면 약간 시간이 걸릴 수 있습니다. 다음 명령을 실행하여 상태를 확인할 수 있습니다.

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

위의 명령에서 SUCCEEDED가 반환되면 Amazon S3 버킷에서 보고서를 열 수 있습니다.

적용을 지원하는 서비스 및 리소스 유형

태그 정책 적용을 지원하는 서비스 및 리소스 유형은 다음과 같습니다.

서비스 이름	리소스 유형	JSON 구문:
Amazon API Gateway	• API 키 • 도메인 이름 • REST API 작업 • Stages	• "apigateway:apikeys" • "apigateway:domainnames" • "apigateway:restapis" • "apigateway:restapis/stages"
AWS Amplify	• 구성 요소 • 주제	• "amplifyuibuilder:app/environment/components" • "amplifyuibuilder:app/environment/themes"
AWS AppConfig	• 애플리케이션 • 구성 프로파일 • 배포 • 배포 전략 • 환경	• "appconfig:application" • "appconfig:application/configurationprofile" • "appconfig:application/environment/deployment" • "appconfig:deploymentstrategy" • "appconfig:application/environment"
AWS App Mesh	• 모두 • 게이트웨이 라우팅 • 메시 • 경로	• "appmesh:*" • "appmesh:mesh/virtualGateway/gatewayRoute" • "appmesh:mesh"

서비스 이름	리소스 유형	JSON 구문:
	• 가상 게이트웨이 • 가상 노드 • 가상 라우터 • 가상 서비스	• `"appmesh:mesh/virtualRouter/route"` • `"appmesh:mesh/virtualGateway"` • `"appmesh:mesh/virtualNode"` • `"appmesh:mesh/virtualRouter"` • `"appmesh:mesh/virtualService"`
Amazon Athena	• 모두 • 작업 그룹	• `"athena:*"` • `"athena:workgroup"`
AWS Audit Manager	• 평가 • 평가 프레임워크 • 컨트롤	• `"auditmanager:assessment "` • `"auditmanager:assessmentFramework "` • `"auditmanager:control "`
AWS Backup	• 백업 계획 • 볼트 • 게이트웨이 • 하이퍼바이저 • VM	• `"backup:backup-plan"` • `"backup:backup-vault"` • `"backup-gateway:gateway"` • `"backup-gateway:hypervisor"` • `"backup-gateway:vm"`
AWS Batch	• 작업 • 작업 정의 • 작업 대기열	• `"batch:job"` • `"batch:job-definition"` • `"batch:job-queue"`
AWS BugBust	• Event	• `"bugbust:event"`
AWS Certificate Manager	• 모두 • 인증서 • Private Certificate Authority	• `"acm:*"` • `"acm:certificate"` • `"acm-pca:certificate-authority"`

서비스 이름	리소스 유형	JSON 구문:
Amazon Chime	• 애플리케이션 인스턴스 • Channel • 미디어 파이프라인 • 회의 • SIP 미디어 애플리케이션 • 사용자 애플리케이션 인스턴스 • 음성 커넥터	• `"chime:app-instance"` • `"chime:app-instance/channel"` • `"chime:media-pipeline"` • `"chime:meeting"` • `"chime:sma"` • `"chime:app-instance/user"` • `"chime:vc"`
AWS Clean Rooms	• 공동 작업 • 구성된 테이블 • 멤버십 • 구성된 테이블 연결	• `"cleanrooms:collaboration"` • `"cleanrooms:configuredtable"` • `"cleanrooms:membership"` • `"cleanrooms:membership/configuredtableassociation"`
AWS Cloud9	• 환경	• `"cloud9:environment"`
아마존 CloudFront	• 모두 • 배포 • 스트리밍 배포	• `"cloudfront:*"` • `"cloudfront:distribution"` • `"cloudfront:streaming-distribution"`
AWS CloudTrail	• 모두 • 추적	• `"cloudtrail:*"` • `"cloudtrail:trail"`
아마존 CloudWatch	• 모두 • 경보 • Contributor Insights 규칙 • 지표 스트림	• `"cloudwatch:*"` • `"cloudwatch:alarm"` • `"cloudwatch:insight-rule"` • `"cloudwatch:metric-stream"`

서비스 이름	리소스 유형	JSON 구문:
아마존 CloudWatch 인터넷 모니터	• 모니터링	• "internetmonitor:monitor"
아마존 CloudWatch 로그	• 대상 • 로그 그룹	• "logs:destination" • "logs:log-group"
Amazon CloudWatch 옵저버빌리티 액세스 관리자	• 링크 • Sink	• "oam:link" • "oam:sink"
AWS CodeBuild	• 모두 • 프로젝트	• "codebuild:*" • "codebuild:project"
아마존 CodeCatalyst	• 연결	• "codecatalyst:connections"
AWS CodeCommit	• 모두 • 리포지토리	• "codecommit:*" • "codecommit:repository"
AWS CodePipeline	• 모두 • 작업 유형 • 파이프라인 • Webhook	• "codepipeline:*" • "codepipeline:actiontype" • "codepipeline:pipeline" • "codepipeline:webhook"
Amazon Cognito 자격 증명	• 모두 • 자격 증명 풀	• "cognito-identity:*" • "cognito-identity:identitypool"
Amazon Cognito 사용자 풀	• 모두 • 사용자 풀	• "cognito-idp:*" • "cognito-idp:userpool"
Amazon Comprehend	• 모두 • 문서 분류자 • 엔터티 인식기	• "comprehend:*" • "comprehend:document-classifier" • "comprehend:entity-recognizer"

서비스 이름	리소스 유형	JSON 구문:
AWS Config	• 모두 • 집계 권한 부여 • 구성 집계자 • Config 규칙	• "config:*" • "config:aggregation-authorization" • "config:config-aggregator" • "config:config-rule"
아마존 CodeGuru 리뷰어	• 연결	• "codeguru-reviewer:association"
아마존 CodeGuru 시큐리티	• 스캔	• "codeguru-security:scans"
CodeConnections	• 연결 • Host	• "codestar-connections:connection" • "codestar-connections:host"
Amazon Connect	• 고객 응대 흐름 • 통합 어소시에이트 • 대기열 • 빠른 연결 • 라우팅 프로필 • User	• "connect:instance/contact-flow" • "connect:instance/integration-association" • "connect:instance/queue" • "connect:instance/transfer-destination" • "connect:instance/routing-profile" • "connect:instance/agent"
Amazon Q Connect	• 도우미 • 연결 • 내용 • 지식 베이스 • 세션	• "wisdom:assistant" • "wisdom:association" • "wisdom:content" • "wisdom:knowledge-base" • "wisdom:session"

서비스 이름	리소스 유형	JSON 구문:
AWS Database Migration Service	• 모두 • 엔드포인트 • ES • Rep • Subgrp • 작업	• "dms:*" • "dms:endpoint" • "dms:es" • "dms:rep" • "dms:subgrp" • "dms:task"
Amazon Data Lifecycle Manager	• 정책	• "dlm:policy"
AWS 다이오드	• Mapping	• "diode-messaging:mapping"
AWS Direct Connect	• 모두 • Dxcon • Dxlag • Dxvif	• "directconnect:*" • "directconnect:dxcon" • "directconnect:dxlag" • "directconnect:dxvif"
Amazon DynamoDB	• 모두 • 표	• "dynamodb:*" • "dynamodb:table"
Amazon EC2	• 용량 예약 • 용량 예약 플릿 • 통신 사업자 게이트웨이	• "ec2:capacity-reservation" • "ec2:capacity-reservation-fleet" • "ec2:carrier-gateway"
	• Client VPN 엔드포인트 • CoIP 풀 • 고객 게이트웨이	• "ec2:client-vpn-endpoint" • "ec2:coip-pool" • "ec2:customer-gateway"

서비스 이름	리소스 유형	JSON 구문:
	• 전용 호스트 • DHCP 옵션 • 외부 전용 인터넷 게이트웨이	• `"ec2:dedicated-host"` • `"ec2:dhcp-options"` • `"ec2:egress-only-internet-gateway"`
	• 엘라스틱 IP(Elastic IP) • 이벤트 창 • 플릿	• `"ec2:elastic-ip"` • `"ec2:instance-event-window"` • `"ec2:fleet"`
	• FPGA 이미지 • 호스트 예약 • 이미지	• `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"`
	• Instance • 인터넷 게이트웨이 • IP 주소 관리자	• `"ec2:instance"` • `"ec2:internet-gateway"` • `"ec2:ipam"`
	• IP 주소 관리자 풀 • IP 주소 관리자 범위 • IPv4 풀	• `"ec2:ipam-pool"` • `"ec2:ipam-scope"` • `"ec2:ipv4pool-ec2"`
	• 키 페어 • 시작 템플릿 • 로컬 게이트웨이 라우팅 테이블	• `"ec2:key-pair"` • `"ec2:launch-template"` • `"ec2:local-gateway-route-table"`

서비스 이름	리소스 유형	JSON 구문:
	• 로컬 게이트웨이 라우팅 테이블 (가상 인터페이스 그룹 연결) • 로컬 게이트웨이 라우팅 테이블 VPC 연결 • NAT 게이트웨이	• "ec2:local-gateway-route-table-virtual-interface-group-association" • "ec2:local-gateway-route-table-vpc-association" • "ec2:natgateway"
	• 네트워크 ACL • 네트워크 인터페이스 • 네트워크 인사이트 액세스 범위	• "ec2:network-acl" • "ec2:network-interface" • "ec2:network-insights-access-scope"
	• 네트워크 인사이트 액세스 범위 분석 • 네트워크 인사이트 분석 • 네트워크 인사이트 경로	• "ec2:network-insights-access-scope-analysis" • "ec2:network-insights-analysis" • "ec2:network-insights-path"
	• 플레이스먼트 그룹 • 접두사 목록 • 루트 볼륨 교체 작업	• "ec2:placement-group" • "ec2:prefix-list" • "ec2:replace-root-volume-task"
	• 예약 인스턴스 • 라우팅 테이블 • 보안 그룹	• "ec2:reserved-instances" • "ec2:route-table" • "ec2:security-group"
	• 스냅샷 • 스팟 인스턴스 요청 • 서브넷	• "ec2:snapshot" • "ec2:spot-instances-request" • "ec2:subnet"

서비스 이름	리소스 유형	JSON 구문:
	• 서브넷 CIDR 예약 • 트래픽 미러 필터 • 트래픽 미러 세션	• "ec2:subnet-cidr-reservation" • "ec2:traffic-mirror-filter" • "ec2:traffic-mirror-session"
	• 트래픽 미러 대상 • 전송 게이트웨이 • Transit Gateway 어태치먼트	• "ec2:traffic-mirror-target" • "ec2:transit-gateway" • "ec2:transit-gateway-attachment"
	• 트랜짓 게이트웨이 커넥트 피어 • Transit Gateway 멀티캐스트 도메인 • Transit Gateway 정책 표	• "ec2:transit-gateway-connect-peer" • "ec2:transit-gateway-multicast-domain" • "ec2:transit-gateway-policy-table"
	• 전송 게이트웨이 라우팅 테이블 • 검증된 액세스 엔드포인트 • 검증된 액세스 그룹	• "ec2:transit-gateway-route-table" • "ec2:verified-access-endpoint" • "ec2:verified-access-group"
	• 검증된 액세스 인스턴스 • 검증된 액세스 신뢰 제공자 • Volume	• "ec2:verified-access-instance" • "ec2:verified-access-trust-provider" • "ec2:volume"
	• VPC 플로우 로그 • VPC • VPC 엔드포인트	• "ec2:vpc-flow-log" • "ec2:vpc" • "ec2:vpc-endpoint"

서비스 이름	리소스 유형	JSON 구문:
	• VPC 엔드포인트 서비스 • VPC 피어링 연결 • VPN 연결 • VPN 게이트웨이	• "ec2:vpc-endpoint-service" • "ec2:vpc-peering-connection" • "ec2:vpn-connection" • "ec2:vpn-gateway"
Amazon EC2 휴지통	• 규칙	• "rbin:rule"
AWS Elastic Beanstalk	• 애플리케이션 • 애플리케이션 버전 • 구성 템플릿 • 플랫폼	• "elasticbeanstalk:application" • "elasticbeanstalk:applicationversion" • "elasticbeanstalk:configurationtemplate" • "elasticbeanstalk:platform"
Amazon Elastic 컨테이너 레지스트리	• 리포지토리	• "ecr:repository"
Amazon Elastic Container Service	• 용량 제공자 • 클러스터 • Service • 작업 정의 • 작업 세트	• "ecs:capacity-provider" • "ecs:cluster" • "ecs:service" • "ecs:task-definition" • "ecs:task-set"
Amazon Elastic File System	• 모두 • 파일 시스템	• "elasticfilesystem:*" • "elasticfilesystem:file-system"
Amazon Elastic Inference	• 액셀러레이터	• "elastic-inference:elastic-inference-accelerator"
Amazon Elastic Kubernetes 서비스	• 클러스터	• "eks:cluster"

서비스 이름	리소스 유형	JSON 구문:
Amazon Elastic 검색	• 도메인	• `"es:domain"`
Amazon EMR	• 클러스터 • Editor	• `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`
Amazon EMR Serverless	• 애플리케이션	• `"emr-serverless:applications"`
AWS 엔티티 해상도	• 매칭 워크플로 • 스키마 매핑	• `"entityresolution:matchingworkflow"` • `"entityresolution:schemamapping"`
아마존 ElastiCache	• 클러스터	• `"elasticache:cluster"`
아마존 EventBridge	• 모두 • 이벤트 버스 • 규칙	• `"events:*"` • `"events:event-bus"` • `"events:rule"`
아마존 EventBridge 파이프	• 파이프	• `"pipes:pipe"`
아마존 EventBridge 스케줄러	• 스케줄 그룹	• `"scheduler:schedule-group"`
Amazon Fraud Detector	• 감지기 • Detector 버전 • 모델 • 규칙 • 변수	• `"frauddetector:detector"` • `"frauddetector:detector-version"` • `"frauddetector:model"` • `"frauddetector:rule"` • `"frauddetector:variable"`
Amazon Global Accelerator	• 액셀러레이터	• `"globalaccelerator:accelerator"`

서비스 이름	리소스 유형	JSON 구문:
Elastic Load Balancing	• 모두 • 리스너 • 리스너 규칙 • 로드 밸런서 • 대상 그룹	• "elasticloadbalancing:*" • "elasticloadbalancing:listener" • "elasticloadbalancing:listener-rule" • "elasticloadbalancing:loadbalancer" • "elasticloadbalancing:targetgroup"
Amazon FSx	• 모두 • 백업 • 파일 시스템	• "fsx:*" • "fsx:backup" • "fsx:file-system"
아마존 GuardDuty	• 감지기 • 필터 • IP 집합 • 위협 인텔 세트	• "guardduty:detector" • "guardduty:detector/filter" • "guardduty:detector/ipset" • "guardduty:detector/threatintelset"
AWS HealthLake	• 데이터 스토어	• "healthlake:datastore "

서비스 이름	리소스 유형	JSON 구문:
AWS HealthOmics	• 주석 스토어 • Annotation Store 버전 • 참조 스토어 • 레퍼런스 • Run • 그룹 실행 • 시퀀스 스토어 • 읽기 세트 • 변형 스토어 • 워크플로	• `"omics:annotationStore"` • `"omics:annotationStore/version"` • `"omics:referenceStore"` • `"omics:referenceStore/reference"` • `"omics:run"` • `"omics:runGroup"` • `"omics:sequenceStore"` • `"omics:sequenceStore/readSet"` • `"omics:variantStore"` • `"omics:workflow"`
Amazon Inspector	• 필터	• `"inspector2:filter "`
AWS Identity and Access Management	• 인스턴스 프로파일 • MFA • OIDC 공급자 • 정책 • SAML 공급자 • 서버 인증서	• `"iam:instance-profile"` • `"iam:mfa"` • `"iam:oidc-provider"` • `"iam:policy"` • `"iam:saml-provider"` • `"iam:server-certificate"`
AWS IoT Analytics	• 모두 • Channel • 데이터세트 • 데이터 스토어 • 파이프라인	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`
AWS IoT Events	• 모두 • 감지기 모델 • Input	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`

서비스 이름	리소스 유형	JSON 구문:
AWS IoT Fleet Hub	• 애플리케이션	• "iotfleethub:application"
AWS IoT SiteWise	• 자산 • 자산 모델	• "iotsitewise:asset" • "iotsitewise:asset-model "
AWS IoT Greengrass	• 대량 배포 • 커넥터 정의 • 코어 정의 • 디바이스 정의 • 함수 정의 • 로거 정의 • 리소스 정의 • 구독 정의	• "greengrass:bulk" • "greengrass:connectorsDefinition" • "greengrass:coresDefinition" • "greengrass:devicesDefinition" • "greengrass:functionsDefinition" • "greengrass:loggersDefinition" • "greengrass:resourcesDefinition" • "greengrass:subscriptionsDefinition"
AWS Key Management Service	• 모두 • 키	• "kms:*" • "kms:key"
Amazon Kinesis	• 모두 • 애플리케이션	• "kinesisanalytics:*" • "kinesisanalytics:application"
Amazon Data Firehose	• 모두 • 전송 스트림	• "firehose:*" • "firehose:deliverystream"
AWS Lambda	• 모두 • 함수	• "lambda:*" • "lambda:function"
Amazon Macie	• 사용자 지정 데이터 식별자	• "macie2:custom-data-identifier"
아마존 MediaStore	• 컨테이너	• "mediastore:container"

서비스 이름	리소스 유형	JSON 구문:
Amazon MQ	• 브로커 • 구성	• "mq:broker" • "mq:configuration"
Amazon Network Firewall	• 방화벽 • 방화벽 정책 • 상태 유지 규칙 그룹 • 무상태 규칙 그룹	• "network-firewall:firewall" • "network-firewall:firewall-policy" • "network-firewall:stateful-rulegroup" • "network-firewall:stateless-rulegroup"
아마존 OpenSearch 서버리스	• 수집	• "aoss:collection"
AWS Organizations	• 계정 • 조직 단위 • 정책 • 루트	• "organizations:account" • "organizations:ou" • "organizations:policy" • "organizations:root"
Amazon Pinpoint SMS Voice V2	• 구성 세트 • 옵트아웃 목록 • 전화번호 • 풀 • 발신자 ID	• "sms-voice:configuration-set" • "sms-voice:opt-out-list" • "sms-voice:phone-number" • "sms-voice:pool" • "sms-voice:sender-id"

서비스 이름	리소스 유형	JSON 구문:
Amazon RDS	• 클러스터 파라미터 그룹 • 클러스터 엔드포인트 • 이벤트 구독 • DB 옵션 그룹 • DB 파라미터 그룹 • DB 프록시 • RDS Proxy 엔드포인트 • 예약 DB 인스턴스 • DB 보안 그룹 • DB 서브넷 그룹 • 대상 그룹	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`
Amazon Redshift	• 모두 • 클러스터 • DB 그룹 • DB 이름 • DB 사용자 • 이벤트 구독 • HSM 클라이언트 인증서 • HSM 구성 • Parameter Group • 스냅샷 • Snapshot • 스냅샷 일정 • 서브넷 그룹	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:dbgroup"` • `"redshift:dbname"` • `"redshift:dbuser"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`

서비스 이름	리소스 유형	JSON 구문:
Amazon Redshift Serverless	• 네임스페이스 • 작업 그룹	• "redshift-serverless:namespace" • "redshift-serverless:workgroup"
AWS Resource Access Manager	• 모두 • 리소스 공유	• "ram:*" • "ram:resource-share"
AWS Resource Groups	• 모두 • 그룹	• "resource-groups:*" • "resource-groups:group"
Amazon Route 53	• 호스팅 영역	• "route53:hostedzone"
Amazon Route 53 Resolver	• 모두 • 해석기 엔드포인트 • 해석기 규칙	• "route53resolver:*" • "route53resolver:resolver-endpoint" • "route53resolver:resolver-rule"
Amazon S3	• 버킷 • Storage Lens • 스토리지 렌즈 그룹	• "s3:bucket" • "s3:storage-lens" • "s3:storage-lens-group"

서비스 이름	리소스 유형	JSON 구문:
아마존 SageMaker	• 앱 이미지 Config • 아티팩트 • 컨텍스트 • 훈련 작업 • 처리 작업 • 모델 패키지 그룹 • 사용자 작업 UI • 모델 패키지 • 작업 • 파이프라인 • 실험 • 흐름 정의 • 프로젝트	• `"sagemaker:app-image-config"` • `"sagemaker:artifact"` • `"sagemaker:context"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:model-package"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:flow-definition"` • `"sagemaker:project"`
AWS Secrets Manager	• 모두 • Secret	• `"secretsmanager:*"` • `"secretsmanager:secret"`
AWS 시큐리티 레이크	• 데이터 레이크 • 구독자	• `"securitylake:data-lake"` • `"securitylake:subscriber"`
AWS Service Catalog	• 애플리케이션 • 속성 그룹 • 포트폴리오 • 제품	• `"servicecatalog:applications"` • `"servicecatalog:attribute-groups "` • `"catalog:portfolio "` • `"catalog:product "`
Amazon Simple Notification Service(SNS)	• 주제	• `"sns:topic"`

서비스 이름	리소스 유형	JSON 구문:
Amazon Simple Queue Service(SQS)	• 대기열	• `"sqs:queue"`
Amazon States Language	• 모두 • 활동 • 상태 시스템	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• 활동	• `"states:activity"`
AWS Storage Gateway	• 모두 • 게이트웨이 • 공유 • 테이프 • Volume	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`
AWS Systems Manager	• 연결 • 자동화 실행 • 문서 • 유지 관리 기간 • 관리형 인스턴스 • Ops 항목 • 패치 기준 • 세션 • 연락처	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm:session"` • `"ssm-contacts:contact"`
Amazon Textract	• 어댑터 • 버전	• `"textract:adapters"` • `"textract:adapters/versions"`
AWS Transfer Family	• Server • User • 워크플로	• `"transfer:server"` • `"transfer:user"` • `"transfer:workflow"`

서비스 이름	리소스 유형	JSON 구문:
Amazon Well-Architected	• 워크로드	• `"wellarchitected:workload"`
AWS Wickr	• 네트워크	• `"wickr:network"`
아마존 WorkSpaces	• 모두 • 연결 별칭 • 디렉터리 • WorkSpace • WorkSpaces 번들 • WorkSpaces 이미지 • WorkSpaces IP 그룹	• `"workspaces:*"` • `"workspaces:connectionalias"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`
아마존 WorkLink	• 플릿	• `"worklink:fleet"`

태그 정책 구문 및 예제

이 페이지에서는 태그 정책 구문에 대해 설명하고 예제를 제공합니다.

태그 정책 구문

태그 정책은 JSON 규칙에 따라 구성된 일반 텍스트 파일입니다. 태그 정책 구문은 관리 정책 유형에 대한 구문을 따릅니다. 해당 구문에 대한 자세한 내용은 관리 정책 상속에 대한 이해 단원을 참조하세요. 이 항목에서는 태그 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 방법을 중점적으로 설명합니다.

다음 태그 정책은 기본 태그 정책 구문을 보여줍니다.

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
```

```
                    "100",
                    "200"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

태그 정책 구문에는 다음 요소가 포함됩니다.

- tags 필드 키 이름입니다. 태그 정책은 항상 이 고정 키 이름으로 시작합니다. 위의 예제 정책에서 맨 위 줄입니다.
- 정책 설명을 고유하게 식별하는 정책 키입니다. 이 값은 대소문자 처리를 제외하고 태그 키의 값과 일치해야 합니다. 태그 키(다음에 설명)와 달리 정책 값은 대/소문자를 구분하지 않습니다.

  이 예제에서 costcenter는 정책 키입니다.
- 리소스에서 준수하게 하려는 대소문자 처리 방식을 사용하여 허용된 태그 키를 지정하는 최소 하나의 태그 키입니다. 대소문자 처리가 정의되지 않은 경우 태그 키의 기본 대소문자 처리 방법은 소문자입니다. 태그 키의 값은 정책 키의 값과 일치해야 합니다. 그러나 정책 키 값은 대소문자를 구분하지 않으므로 대소문자 처리가 다를 수 있습니다.

  이 예제에서 CostCenter는 태그 키입니다. 이는 태그 정책을 준수하는 데 필요한 대소문자 처리입니다. 이 태그 키에 대한 대체 대소문자 처리를 사용하는 리소스는 태그 정책을 준수하지 않습니다.

  한 태그 정책에 여러 태그 키를 정의할 수 있습니다.
- (선택 사항) 태그 키에 대해 허용 가능한 하나 이상의 태그 값 목록입니다. 태그 정책에 따라 태그 키의 태그 값이 지정되지 않으면 모든 값(값이 전혀 없는 경우 포함)이 정책을 준수하는 것으로 간주됩니다.

  이 예제에서 CostCenter 태그 키에 허용 가능한 값은 100 및 200입니다.
- (선택 사항) 지정된 서비스와 리소스에서 정책 미준수 태그 지정 작업을 금지할지 여부를 나타내는 enforced_for 옵션입니다. 콘솔에서 이 옵션은 태그 정책 생성에 대한 시각적 편집기의 이 태그에 대한 정책 미준수 작업 금지 옵션입니다. 이 옵션의 기본 설정은 null입니다.

  태그 정책 예제는 모든 AWS Secrets Manager 리소스에 이 태그가 있어야 하도록 지정합니다.

> **Warning**
>
> 태그 정책을 사용한 경험이 있는 경우에만 이 옵션을 기본값에서 변경해야 합니다. 그렇지 않으면 조직 계정의 사용자가 필요한 리소스를 생성하지 못하도록 할 수 있습니다.

- 태그 정책이 조직 트리 내의 다른 태그 정책과 병합되어 계정의 유효 태그 정책을 생성하는 방법을 지정하는 연산자입니다. 이 예제에서 `@@assign`은 `tag_key`, `tag_value` 및 `enforced_for`에 문자열을 할당하는 데 사용됩니다. 연산자에 대한 자세한 내용은 상속 연산자 단원을 참조하세요.
- – 태그 값과 `enforced_for` 필드에서 * 와일드카드를 사용할 수 있습니다.
  - 태그 값당 하나의 와일드카드만 사용할 수 있습니다. 예를 들어, `*@example.com`은 허용되지만 `*@*.com`은 허용되지 않습니다.
  - `enforced_for`의 경우 일부 서비스에서 `<service>:*`를 사용하여 해당 서비스의 모든 리소스에 적용하는 기능을 활성화할 수 있습니다. `enforced_for`를 지원하는 서비스 및 리소스의 목록은 적용을 지원하는 서비스 및 리소스 유형을 참조하세요.

    와일드카드를 사용하여 모든 서비스를 지정하거나 모든 서비스에 대한 리소스를 지정할 수는 없습니다.

태그 정책 예제

다음 태그 정책 예제는 정보 제공 용도로만 제공됩니다.

> **Note**
>
> 조직에서 이러한 태그 정책 예제를 사용하려면 먼저 다음 사항에 주의하세요.
>
> - 태그 정책을 시작하려면 권장 워크플로우를 따라야 합니다.
> - 각자 고유의 요구 사항에 맞게 이러한 태그 정책을 신중하게 검토하고 사용자 지정해야 합니다.
> - 태그 정책의 모든 문자는 최대 크기가 정해져 있습니다. 이 설명서의 예제는 가독성을 높이기 위한 추가 공백으로 서식이 지정된 SCP를 보여 줍니다. 하지만 정책 크기가 최대 크기에 도달하는 경우 공간을 절약하기 위해 공백을 모두 삭제할 수 있습니다. 공백의 예에는 따옴표 밖에 있는 공백 문자와 줄 바꿈이 있습니다.
> - 태그가 지정되지 않은 리소스는 결과에 정책 미준수로 나타나지 않습니다.

예제 1: 조직 전체의 태그 키 사례 정의

다음 예제에서는 두 개의 태그 키만 정의하는 태그 정책과 조직의 계정에서 표준화할 대소문자 처리만 정의하는 태그 정책을 보여 줍니다.

정책 A - 조직 루트 태그 정책

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

이 태그 정책은 CostCenter와 Project라는 두 가지 태그 키를 정의합니다 . 이 태그 정책을 조직 루트에 연결하면 다음과 같은 효과가 발생합니다.

- 조직의 모든 계정이 이 태그 정책을 상속합니다.
- 정책을 준수하기 위해 조직의 모든 계정이 정의된 대소문자 처리를 사용해야 합니다. CostCenter 및 Project 태그가 있는 리소스는 정책을 준수합니다. 태그 키에 대한 대체 대소문자 처리를 사용하는 리소스(예: costcenter, Costcenter 또는 COSTCENTER)는 정책을 준수하지 않습니다.
- @@operators_allowed_for_child_policies": ["@@none"] 행은 태그 키를 잠급니다. 조직 트리의 아래쪽에 연결된 태그 정책(하위 정책)은 값 설정(value-setting) 연산자를 사용하여 태그 키를 변경할 수 없습니다(대소문자 처리 포함).
- 모든 태그 정책이 그렇듯이, 태그 없는 리소스 또는 태그 정책에서 정의되지 않은 태그는 태그 정책 준수 여부가 평가되지 않습니다.

AWS에서는 사용할 태그 키에 대해 비슷한 태그 정책을 생성할 때 이 예제를 가이드로 사용하는 것이 좋습니다. 이 태그 정책을 조직 루트에 연결합니다. 그런 다음 정의된 태그 키에 대해 허용 가능한 값만 정의하는 다음 예제와 비슷한 태그 정책을 생성합니다.

다음 단계: 값 정의

이전의 태그 정책을 조직 루트에 연결했다고 가정합니다. 그런 다음, 다음과 같은 태그 정책을 생성하여 계정에 연결할 수 있습니다. 이 정책은 CostCenter 및 Project 태그 키에 대해 허용 가능한 값을 정의합니다.

정책 B - 계정 태그 정책

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

정책 A를 조직 루트에 연결하고 정책 B를 계정에 연결하면 정책이 결합되어 계정에 대해 다음과 같은 유효 태그 정책을 생성합니다.

정책 A + 정책 B = 계정에 대한 유효 태그 정책

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
```

```
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

상속 연산자의 작동 방식 예제 및 유효 태그 정책 예제를 포함하여 정책 상속에 대한 자세한 내용은 관리 정책 상속에 대한 이해 단원을 참조하세요.

예제 2: 태그 키 사용 방지

태그 키의 사용을 방지하기 위해 다음과 같은 태그 정책을 조직 엔터티에 연결할 수 있습니다.

이 예제 정책은 `Color` 태그 키에 어떤 값도 사용할 수 없도록 지정합니다. 또한 하위 태그 정책에서 연산자가 허용되지 않도록 지정합니다. 따라서 영향을 받는 계정의 리소스에 대한 모든 `Color` 태그는 미준수로 간주됩니다. 그러나 `enforced_for` 옵션은 영향을 받는 계정이 Amazon DynamoDB 테이블에만 `Color` 태그를 지정하는 것을 방지합니다.

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
```

```
            }
        }
    }
}
```

지원되는 리전

태그 정책 기능은 다음 리전에서 사용할 수 있습니다.

지역명	리전 파라미터
미국 동부(버지니아 북부) 리전[1]	**us-east-1**
US East (Ohio) Region	us-east-2
US West (N. California) Region	us-west-1
US West (Oregon) Region	us-west-2
아프리카(케이프타운) 리전[2]	af-south-1
아시아 태평양(홍콩) 리전[2]	ap-east-1
Asia Pacific (Mumbai) Region	ap-south-1
아시아 태평양 (하이데라바드) [2]	ap-south-2
아시아 태평양(도쿄) 리전	ap-northeast-1
Asia Pacific (Seoul) Region	ap-northeast-2
Asia Pacific (Osaka) Region	ap-northeast-3
아시아 태평양(싱가포르) 리전	ap-southeast-1
아시아 태평양(시드니) 리전	ap-southeast-2
아시아 태평양 (자카르타) 지역[2]	ap-southeast-3
아시아 태평양 (멜버른) [2]	ap-southeast-4
캐나다 서부 (캘거리) [2]	ca-west-1

지역명	리전 파라미터
캐나다(중부) 리전	`ca-central-1`
Europe (Frankfurt) Region	`eu-central-1`
유럽 (취리히) 지역[2]	`eu-central-2`
유럽(밀라노) 리전[2]	`eu-south-1`
유럽 (스페인) [2]	`eu-south-2`
Europe (Ireland) Region	`eu-west-1`
Europe (London) Region	`eu-west-2`
유럽(파리) 리전	`eu-west-3`
유럽(스톡홀름) 리전	`eu-north-1`
중동 (UAE) 지역[2]	`me-central-1`
중동(바레인) 리전[2]	`me-south-1`
South America (São Paulo) Region	`sa-east-1`
이스라엘 (텔아비브) [2]	`il-central-1`

[1]다음 Organizations 작업을 호출할 때 **`us-east-1`** 리전을 지정해야 합니다.

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- 조직 루트에 대한 기타 모든 작업 (예 ListRoots:

태그 정책 기능의 일부인 다음 Resource Groups Tagging API 작업을 호출할 때도 **`us-east-1`** 리전을 지정해야 합니다.

- DescribeReportCreation

- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> 조직 전체의 태그 정책 준수 여부를 평가하려면 보고서 저장을 위해 미국 동부(버지니아 북부) 리전의 Amazon S3 버킷에 대한 액세스 권한도 있어야 합니다. 자세한 내용은 태깅 AWS 리소스 사용 설명서의 보고서 스토리지에 대한 Amazon S3 버킷 정책을 참조하십시오.

[2]이러한 리전은 수동으로 활성화해야 합니다. 활성화 및 AWS 리전비활성화에 대해 자세히 알아보려면 AWS 리전 계정 관리 참조 안내서에서 사용할 수 있는AWS 계정 지정을 참조하십시오. Resource Groups 콘솔을 이러한 리전에서 사용할 수 없습니다.

서비스 제어 정책(SCP)

서비스 제어 정책(SCP)은 조직의 권한을 관리하는 데 사용할 수 있는 조직 정책 유형입니다. SCP는 조직의 IAM 사용자 및 IAM 역할에 대해 사용 가능한 최대 권한을 중앙에서 제어합니다. SCP를 사용하면 조직의 액세스 제어 지침에 따라 계정을 유지할 수 있습니다. SCP는 활성화된 모든 기능을 가진 조직에서만 사용할 수 있습니다. 조직이 통합 결제 기능만 지원한다면 SCP를 이용할 수 없습니다. SCP 활성화에 대한 지침은 정책 유형 활성화 및 비활성화 단원을 참조하세요.

SCP는 조직의 IAM 사용자 및 IAM 역할에 권한을 부여하지 않습니다. SCP는 어떠한 권한도 부여하지 않습니다. SCP는 조직의 IAM 사용자 및 IAM 역할이 수행할 수 있는 작업에 대해 권한 가드레일을 정의하거나 제한을 설정합니다. 권한을 부여하려면 관리자가 IAM 사용자 및 IAM 역할에 연결된 ID 기반 정책, 계정의 리소스에 연결된 리소스 기반 정책 등 액세스를 제어하는 정책을 연결해야 합니다. 유효 권한은 SCP에서 허용하는 권한과 ID 및 리소스 기반 정책에서 허용하는 항목 간의 논리적 교차점입니다.

> **Important**
>
> SCP는 관리 계정의 사용자 또는 역할에 영향을 미치지 않습니다. 조직의 멤버 계정에만 영향을 줍니다.

이 페이지의 주제

SCP의 효과 테스트

AWS 정책이 계정에 미치는 영향을 철저하게 테스트하지 않고는 조직의 루트에 SCP를 연결하지 않는 것이 좋습니다. 대신 한 번에 하나씩, 또는 소량 단위로 계정을 옮길 수 있는 OU를 만들어 사용자가 주요 서비스를 이용하지 못하는 일이 없게 하세요. 서비스가 계정에 사용되는지 확인하는 한 가지 방법은 IAM에서 마지막으로 데이터를 액세스한 서비스를 살펴보는 것입니다. 또 다른 방법은 API 수준에서 서비스 사용을 AWS CloudTrail 기록하는 데 사용하는 것입니다.

> **Note**
>
> 전체 AWSAccess 정책을 수정하거나 허용된 작업이 포함된 별도의 정책으로 바꾸지 않는 한 전체 정책을 제거해서는 안 됩니다. 그렇지 않으면 구성원 계정의 모든 AWS 작업이 실패합니다.

SCP의 최대 크기

SCP 내 모든 문자는 최대 크기를 기준으로 계수됩니다. 이 설명서의 예제는 가독성을 높이기 위한 추가 공백으로 포맷된 SCP를 보여 줍니다. 하지만 정책 크기가 최대 크기에 근접한 경우 공백을 저장하려면 인용 부호 바깥에 있는 공백 문자(예: 공백 및 줄 바꿈)를 모두 삭제할 수 있습니다.

> **Tip**
>
> 시각적 편집기를 사용하여 SCP를 작성합니다. 편집기가 자동으로 불필요한 공백을 제거합니다.

조직 내 여러 수준에 SCP 연결하기

SCP가 작동하는 방식에 대한 자세한 설명은 SCP 평가을(를) 참조하세요.

권한에 대한 SCP 효과

SCP는 AWS Identity and Access Management (IAM) 권한 정책과 비슷하며 거의 동일한 구문을 사용합니다. 그러나 SCP는 권한을 부여하지는 않습니다. 대신 SCP는 조직의 IAM 사용자 및 IAM 역할에 대한 최대 권한을 지정하는 JSON 정책입니다. 자세한 내용은 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

- SCP는 조직에 속한 계정이 관리하는 IAM 사용자 및 역할에만 영향을 줍니다. SCP는 리소스 기반 정책에 직접 영향을 주지 않습니다. 조직 외부 계정의 사용자 또는 역할에도 영향을 주지 않습니다. 예를 들어 조직의 A 계정이 소유하는 Amazon S3 버킷을 가정해 보겠습니다. 버킷 정책(리소스 기반 정책)은 조직 외부의 B 계정에 속한 사용자에게 액세스 권한을 부여합니다. A 계정에는 SCP가 연결되어 있습니다. 해당 SCP는 B 계정의 외부 사용자에게 적용되지 않습니다. 이 SCP는 조직의 A 계정이 관리하는 사용자에게만 적용됩니다.
- SCP는 멤버 계정의 IAM 사용자 및 역할(멤버 계정의 루트 사용자 포함)에 대해 권한을 제한합니다. 각 계정은 모든 상위 계정이 허용하는 권한만 갖게 됩니다. 권한이 계정 이상의 수준에서 묵시적으로(`Allow` 정책문에 포함되지 않음) 명시적으로(`Deny` 정책문에 포함됨) 막혀 있다면, 영향받는 계정에 있는 사용자나 역할은 계정 관리자가 `*/*` 권한이 있는 `AdministratorAccess` IAM 정책을 사용자에 연결하더라도 해당 권한을 사용할 수 없습니다.
- SCP는 조직의 멤버 계정에만 영향을 미칩니다. 관리 계정의 사용자 또는 역할에는 영향을 미치지 않습니다.
- 사용자와 역할이 적절한 IAM 권한 정책으로 권한을 부여받아야 한다는 사실은 변하지 않습니다. IAM 권한 정책이 없는 사용자는 관련 SCP가 모든 서비스와 작업을 허용해도 액세스 권한이 없습니다.
- 사용자나 역할에게 관련 SCP가 허용하는 작업에 대한 액세스를 부여하는 IAM 권한 정책이 있으면 사용자나 역할이 해당 작업을 수행할 수 있습니다.
- 사용자나 역할에 관련 SCP가 허용하지 않거나 명시적으로 거부한 작업의 액세스 권한을 부여하는 IAM 권한 정책이 있으면 사용자나 역할이 해당 작업을 수행할 수 없습니다.

- SCP는 루트 사용자를 포함하여 추가된 계정의 모든 사용자와 역할에 영향을 줍니다. 유일한 예외는 작업 및 엔터티는 SCP로 제한할 수 없습니다.에 설명되어 있습니다.
- SCP는 어떠한 서비스 연결 역할에도 영향을 미치지 않습니다. 서비스 연결 역할을 사용하면 다른 AWS 서비스를 SCP와 통합할 수 AWS Organizations 있으며 SCP가 이를 제한할 수 없습니다.
- 루트에서 SCP 정책 유형을 사용하지 않도록 설정하면 해당 루트의 모든 개체에서 모든 SCP가 자동으로 분리됩니다. AWS Organizations AWS Organizations 엔티티에는 조직 단위, 조직 및 계정이 포함됩니다. 루트에서 SCP를 다시 활성화하면, 해당 루트는 루트의 모든 개체에 자동적으로 연결된 기본 `FullAWSAccess` 정책으로 돌아갑니다. SCP를 비활성화하기 전에 이루어진 SCP와 AWS Organizations 개체 연결은 모두 사라지며, 수동으로 다시 연결할 수는 있지만 자동으로 복원되지는 않습니다.
- 권한 경계(고급 IAM 기능)와 SCP가 둘 다 있는 경우 권한 경계, SCP 및 자격 증명 기반 정책 모두에서 해당 작업을 허용해야 합니다.

액세스 데이터를 사용하여 SCP 개선

관리 계정 자격 증명으로 로그인하면 IAM 콘솔 AWS Organizations섹션에서 AWS Organizations 엔티티 또는 정책에 대한 서비스에 마지막으로 액세스한 데이터를 볼 수 있습니다. IAM의 AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 서비스에서 마지막으로 액세스한 데이터를 검색할 수도 있습니다. 이 데이터에는 AWS Organizations 계정의 IAM 사용자 및 역할이 마지막으로 액세스를 시도한 허용된 서비스와 언제 액세스했는지에 대한 정보가 포함됩니다. 이 정보를 사용하여 사용되지 않는 권한을 확인할 수 있으므로 SCP를 구체화함으로써 최소 권한의 원칙을 보다 잘 준수할 수 있습니다.

예를 들어 세 서비스에 대한 액세스를 금지하는 거부 목록 SCP가 있을 수 있습니다. AWS SCP의 `Deny` 문에 없는 모든 서비스는 허용됩니다. 서비스에서 마지막으로 액세스한 IAM의 데이터는 SCP에서 허용했지만 사용하지 않는 AWS 서비스를 알려줍니다. 이 정보로 SCP를 업데이트하여 필요 없는 서비스에 대한 액세스를 거부할 수 있습니다.

자세한 내용은 IAM 사용 설명서에서 다음 주제를 참조하세요.

- Organizations에서 서비스가 마지막으로 액세스한 데이터 보기
- 데이터를 사용하여 조직 단위의 권한 구체화

작업 및 엔터티는 SCP로 제한할 수 없습니다.

다음 작업은 SCP를 사용해 제한할 수 없습니다.

- 관리 계정이 수행하는 모든 작업
- 서비스 연결 역할에 연결된 권한을 사용한 모든 작업.
- 루트 사용자로 Enterprise Support 플랜 등록하기
- 루트 사용자로서 AWS 지원 수준을 변경하십시오.
- CloudFront 비공개 콘텐츠를 위한 신뢰할 수 있는 서명자 기능 제공
- 루트 사용자로 Amazon Lightsail 이메일 서버 및 Amazon EC2 인스턴스에 대한 역방향 DNS 구성
- 일부 AWS관련 서비스의 작업:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - Amazon 제품 마케팅 API

서비스 제어 정책의 생성, 업데이트, 삭제

조직의 관리 계정에 로그인하면 서비스 제어 정책(SCP)을 생성하거나 업데이트할 수 있습니다. 지정하는 서비스 및 작업에 대한 액세스를 거부하거나 허용하는 문을 작성하여 SCP를 생성합니다.

SCP 작업을 위한 기본 구성은 "차단 목록" 전략을 사용하는 것입니다. 이 전략에서는 액세스를 거부하는 문을 만들어 차단할 작업 외에는 모든 작업이 암시적으로 허용됩니다. 거부 문에서는 리소스 및 조건을 지정하고 NotAction 요소를 사용할 수 있습니다. 허용 문에서는 서비스 및 작업만 지정할 수 있습니다. 액세스를 거부하는 문과 액세스를 허용하는 문에 대한 자세한 내용은 SCP 평가 단원을 참조하세요.

> **Tip**
>
> IAM에서 서비스가 마지막으로 액세스한 데이터를, SCP 업데이트를 위한 데이터 포인트로 사용하여 필요한 AWS 서비스로만 액세스를 제한할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 Organizations에서 서비스가 마지막으로 액세스한 데이터 보기를 참조하세요.

이 주제에서 수행할 작업

- 조직에 대해 서비스 제어 정책을 사용하도록 설정한 후에 정책을 생성할 수 있습니다.
- SCP 요구 사항이 변경되면 기존 정책을 업데이트할 수 있습니다.

- 정책이 더 이상 필요하지 않은 경우 모든 조직 단위(OU) 및 계정에서 정책을 분리한 후 삭제할 수 있습니다.

SCP 생성

> **최소 권한**
>
> SCP를 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.
>
> - `organizations:CreatePolicy`

AWS Management Console

서비스 제어 정책을 생성하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 제어 정책(Service control policies) 페이지에서 정책 생성(Create policy)을 선택합니다.
3. 새 서비스 제어 정책 생성(Create new service control policy) 페이지에서 정책 이름과 정책 설명(선택 사항)을 입력합니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 하나 이상의 태그를 추가합니다. 값을 공백으로 남겨두면 `null`이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 정보는 AWS Organizations 리소스에 태그 지정을 참조하세요.

   > **Note**
   >
   > 이어지는 대부분의 단계에서는 JSON 편집기의 오른쪽에 있는 컨트롤을 사용하여 요소별로 정책을 구성하는 방법에 대해 설명합니다. 또는 언제든 창 왼쪽의 JSON 편집기에 간단히 텍스트를 입력할 수 있습니다. 직접 입력하거나 복사 및 붙여넣기를 사용할 수 있습니다.

5. 정책 작성은 추가하는 문이 액세스를 거부하는지, 아니면 허용하지에 따라 그 다음 단계가 달라집니다. 자세한 내용은 SCP 평가 섹션을 참조하세요. `Deny` 문을 사용할 경우 특정 리소스에 대한 액세스를 제한하고, SCP가 효력을 발휘하는 조건을 정의하고, NotAction 요소를 사용하

는 추가 컨트롤을 사용할 수 있습니다. 구문에 대한 자세한 내용은 SCP 구문 단원을 참조하세요.

액세스를 거부하는 문을 추가하려면:

a. 편집기의 오른쪽 문 편집 창에 있는 작업 추가에서 AWS 서비스를 선택합니다.

   오른쪽 창에서 옵션을 선택하면 JSON 편집기가 업데이트되어 왼쪽에 해당하는 JSON 정책이 표시됩니다.

b. 서비스를 선택하면 해당 서비스에 대해 사용 가능한 작업이 포함된 목록이 열립니다. 모든 작업(All actions)을 선택하거나, 거부하려는 개별 작업을 하나 이상 선택할 수 있습니다.

   왼쪽의 JSON이 업데이트되면서 선택한 작업이 포함됩니다.

   > **Note**
   >
   > 개별 작업을 선택한 다음 돌아가서 모든 작업을 선택하는 경우 *servicename*/*에 대한 예상 항목이 JSON에 추가되지만 이전에 선택한 개별 작업은 JSON에 남아 제거되지 않습니다.

c. 추가 서비스에서 작업을 추가하려면 문(Statement) 상자 상단에서 모든 서비스(All services)를 선택한 다음 필요에 따라 앞의 두 단계를 반복할 수 있습니다.

d. 문에 포함할 리소스를 지정합니다.

   - 리소스 추가 옆에 있는 추가를 선택합니다.
   - 리소스 추가 대화 상자의 목록에서 리소스를 제어하려는 서비스를 선택합니다. 이전 단계에서 선택한 서비스 중에서만 선택할 수 있습니다.
   - 리소스 유형(Resource type)에서 제어할 리소스 유형을 선택합니다.
   - 마지막으로 액세스를 제어하려는 특정 리소스를 식별하기 위해 리소스 ARN(Resource ARN)에 Amazon 리소스 이름(ARN)을 작성합니다. 중괄호 {}로 둘러싸인 모든 자리 표시자를 교체해야 합니다. 해당 리소스 유형의 ARN 구문이 허용하는 경우 와일드카드(*)를 지정할 수 있습니다. 와일드카드를 사용할 수 있는 상황에 대한 내용은 특정 리소스 유형에 대한 설명서를 참조하세요.
   - 리소스 추가(Add resource)를 선택해 정책에 대한 추가 항목을 저장합니다. JSON의 `Resource` 요소는 추가 또는 변경 사항을 반영합니다. 리소스 요소는 필수입니다.

> **Tip**
>
> 선택한 서비스에 대한 모든 리소스를 지정하려면 목록에서 모든 리소스(All resources) 옵션을 선택하거나 `"Resource":"*"`를 읽는 JSON에서 `Resource` 문을 직접 편집합니다.

e. (선택 사항) 정책 문이 적용되는 상황을 제한하는 조건을 지정하려면 조건 추가 옆에 있는 추가를 선택합니다.

- 조건 키(Condition key) - 목록에서 모든 AWS 서비스에 사용할 수 있는 조건 키(예: `aws:SourceIp`) 또는 해당 문에 대해 선택한 서비스 중 하나에 대한 서비스별 키를 선택할 수 있습니다.
- 한정어(Qualifier) – (선택 사항) 조건에 여러 값을 입력할 경우(특정 조건 키에 따라 다름) 값에 대해 요청을 테스트할 한정어를 지정할 수 있습니다.
  - 기본값(Default) - 정책의 조건 키 값에 대해 요청의 한 값을 테스트합니다. 요청의 값이 정책의 값과 일치하면 조건이 true를 반환합니다. 정책에 둘 이상의 값이 지정되어 있으면 “or” 테스트로 처리되고, 요청 값이 임의의 정책 값과 일치하는 경우 조건이 true를 반환합니다.
  - 요청의 임의의 값에 대해(For any value in a request) - 요청이 여러 값을 가질 수 있는 경우 이 옵션은 요청 값 중 하나 이상이 정책의 조건 키 값 중 하나 이상과 일치하는지 확인합니다. 요청의 키 값 중 하나가 정책의 조건 값 중 하나와 일치하면 조건이 true를 반환합니다. 일치하는 키가 없거나 null 데이터 세트의 경우 조건에서 false를 반환합니다.
  - 요청의 모든 값에 대해(For all values in a request) - 요청이 여러 값을 가질 수 있는 경우 이 옵션은 모든 요청 값이 정책의 조건 키 값과 일치하는지 확인합니다. 요청의 모든 키 값이 정책에 있는 하나 이상의 값과 일치하면 조건이 true를 반환합니다. 요청에 키가 없거나 키 값이 빈 문자열과 같은 null 데이터 세트로 확인되는 경우에도 true를 반환합니다.
- 연산자(Operator) - 연산자는 수행할 비교의 유형을 지정합니다. 표시되는 옵션은 조건 키의 데이터 유형에 따라 다릅니다. 예를 들어 `aws:CurrentTime` 전역 조건 키를 사용하면 날짜 비교 연산자 중 하나를 선택할 수 있습니다. 또는 `Null`을 사용하면 값이 요청에 있는지 여부를 테스트할 수 있습니다.

  `Null` 테스트를 제외한 모든 조건 연산자에 대해 IfExists 옵션을 선택할 수 있습니다.
- 값(Value) - (선택 사항) 요청에서 테스트할 값을 하나 이상 지정합니다.

[Add condition]을 선택합니다.

조건 키에 대한 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

f. (선택 사항) `NotAction` 요소를 사용하여 지정된 작업을 제외한 모든 작업에 대해 액세스를 거부하려면 왼쪽 창의 `Action`을 `NotAction`으로 바꿉니다(`"Effect": "Deny"`, 요소 바로 뒤에서). 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: NotAction을 참조하세요.

6. 액세스를 허용하는 문을 추가하려면:

a. 왼쪽의 JSON 편집기에서 `"Effect": "Deny"` 라인을 `"Effect": "Allow"`로 변경합니다.

오른쪽 창에서 옵션을 선택하면 JSON 편집기가 업데이트되어 왼쪽에 해당하는 JSON 정책이 표시됩니다.

b. 서비스를 선택하면 해당 서비스에 대해 사용 가능한 작업이 포함된 목록이 열립니다. 모든 작업(All actions)을 선택하거나, 허용하려는 개별 작업을 하나 이상 선택할 수 있습니다.

왼쪽의 JSON이 업데이트되면서 선택한 작업이 포함됩니다.

> **Note**
>
> 개별 작업을 선택한 다음 돌아가서 모든 작업을 선택하는 경우 *servicename*`/*`에 대한 예상 항목이 JSON에 추가되지만 이전에 선택한 개별 작업은 JSON에 남아 제거되지 않습니다.

c. 추가 서비스에서 작업을 추가하려면 문(Statement) 상자 상단에서 모든 서비스(All services)를 선택한 다음 필요에 따라 앞의 두 단계를 반복할 수 있습니다.

7. (선택 사항) 정책에 다른 문을 추가하려면 문 추가(Add statement)를 선택하고 시각적 편집기를 사용하여 다음 문을 작성합니다.

8. 문을 모두 추가했으면 정책 생성을 선택하여 완료된 SCP를 저장합니다.

새 SCP가 조직의 정책 목록에 표시됩니다. 이제 루트, OU 또는 계정에 SCP를 연결할 수 있습니다.

AWS CLI & AWS SDKs

서비스 제어 정책을 생성하려면

다음 명령 중 하나를 사용하여 SCP를 생성할 수 있습니다.

- AWS CLI: create-policy

  다음 예제에서는 JSON 정책 텍스트가 포함된 Deny-IAM.json이라는 파일을 가정합니다. 이 파일은 새 서비스 제어 정책을 생성하는 데 사용됩니다.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDK: CreatePolicy

> **Note**
>
> SCP는 관리 계정과 몇 가지 다른 상황에서는 적용되지 않습니다. 자세한 정보는 작업 및 엔터티는 SCP로 제한할 수 없습니다.을 참조하세요.

SCP 업데이트

조직의 관리 계정에 로그인하면, 정책의 이름을 변경하거나 내용을 변경할 수 있습니다. SCP 내용 변경은 연결된 모든 계정의 사용자, 그룹과 역할에 즉시 영향을 줍니다.

최소 권한

SCP를 업데이트하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 organizations:UpdatePolicy
- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 organizations:DescribePolicy

AWS Management Console

정책을 업데이트하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 제어 정책 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책의 세부 정보 페이지에서 정책 편집(Edit policy)을 선택합니다.
4. 다음 중 원하는 변경을 수행합니다.
   - 정책 이름(Policy name)에 새 이름을 입력하여 정책 이름을 변경할 수 있습니다.
   - 정책 설명(Policy description)에 새 텍스트를 입력하여 설명을 변경할 수 있습니다.
   - 왼쪽 창에서 JSON 형식의 정책을 편집하여 정책 텍스트를 편집할 수 있습니다. 또는 오른쪽 편집기에서 문을 선택하고 컨트롤을 사용하여 해당 요소를 변경할 수도 있습니다. 각 컨트롤에 대한 자세한 내용은 이 주제 앞부분의 SCP 프로시저 생성을 참조하세요.
5. 작업을 마쳤으면 변경 내용 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

정책을 업데이트하려면 다음 명령 중 한 가지를 사용합니다.

- AWS CLI: update-policy

  다음 예제에서는 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

다음 예제에서는 서비스 제어 정책에 대한 설명을 추가하거나 변경합니다.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

다음 예제에서는 새 JSON 정책 텍스트를 포함한 파일을 지정하여 SCP의 정책 문서를 변경합니다.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDK: UpdatePolicy

자세한 정보

SCP 생성에 대한 자세한 내용은 다음 주제를 참조하세요.

- 서비스 제어 정책 예
- SCP 구문

SCP에 연결된 태그 편집

조직의 관리 계정으로 로그인하여 SCP에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요AWS Organizations 리소스에 태그 지정

> **최소 권한**
>
> AWS 조직의 SCP에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.
>
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

- `organizations:DescribePolicy` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

SCP에 연결된 태그를 편집하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 제어 정책(Service control policies) 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 정책 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 다음 중 원하는 변경을 수행합니다.
   - 이전 값 대신 새 값을 입력하여 태그 값을 변경합니다. 태그 키는 직접 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제한 다음 새 키를 가진 태그를 추가해야 합니다.
   - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
   - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 `null`이 아닌 빈 문자열이 됩니다.
5. 작업을 마쳤으면 변경 내용 저장을 선택합니다.

AWS CLI & AWS SDKs

SCP에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 SCP에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: tag-resource 및 untag-resource
- AWS SDK: TagResource 및 UntagResource

SCP 삭제

조직의 관리 계정에 로그인하면 조직에서 더 이상 필요 없는 정책을 삭제할 수 있습니다.

> **주의**
>
> - 정책을 삭제하기 전에 먼저 연결된 모든 개체에서 정책을 분리해야 합니다.
> - `FullAWSAccess`라는 SCP와 같은 AWS 관리형 SCP는 삭제할 수 없습니다.

> **최소 권한**
>
> SCP를 삭제하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.
>
> - `organizations:DeletePolicy`

AWS Management Console

SCP를 삭제하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 제어 정책(Service control policies) 페이지에서 삭제할 SCP의 이름을 선택합니다.
3. 먼저 모든 루트, OU와 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제(Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제(Delete)를 선택합니다.

AWS CLI & AWS SDKs

SCP를 삭제하려면

정책을 삭제하려면 다음 명령 중 한 가지를 사용합니다.

- AWS CLI: delete-policy

다음 예제에서는 지정한 SCP를 삭제합니다.

```
$ aws organizations delete-policy \
    --policy-id p-i9j8k7l6m5
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: DeletePolicy

서비스 제어 정책 연결 및 분리

조직의 관리 계정에 로그인하면 이전에 생성한 SCP(서비스 제어 정책)를 연결할 수 있습니다. SCP를 조직 루트 또는 조직 단위(OU)에 연결하거나 계정에 직접 연결할 수 있습니다. SCP를 연결하려면 다음 단계를 완료하세요.

> 최소 권한
>
> SCP를 루트, OU 또는 계정에 연결하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.
>
> - 동일한 정책 명령문에서 지정된 정책의 Amazon 리소스 이름(ARN)(또는 "*"), 루트의 ARN, 또는 정책을 연결할 루트, OU, 계정의 ARN을 포함하는 `Resource` 요소를 가진 `organizations:AttachPolicy`

AWS Management Console

정책으로 이동하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 SCP를 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 SCP를 연결하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 SCP를 연결할 루트, OU, 계정을 찾아서 그 옆에 있는 확인란을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).

3. 정책(Policies) 탭의 서비스 제어 정책(Service control policies)에 대한 항목에서 연결(Attach)을 선택합니다.
4. 원하는 정책을 찾아서 정책 연결(Attach policy)을 선택합니다.

   정책(Policies) 탭의 연결된 SCP 목록이 업데이트되어 새 추가 항목이 목록에 포함됩니다. 정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 IAM 사용자와 역할이 가지는 권한에 영향을 줍니다.

정책으로 이동하여 SCP를 연결하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 제어 정책(Service control policies) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
5. 정책 연결을 선택합니다.

   대상(Policies) 탭의 연결된 SCP 목록이 업데이트되어 새 추가 항목이 목록에 포함됩니다. 정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 IAM 사용자와 역할이 가지는 권한에 영향을 줍니다.

AWS CLI & AWS SDKs

루트, OU 또는 계정으로 이동하여 SCP를 연결하려면

다음 명령 중 하나를 사용하여 SCP를 연결할 수 있습니다.

- AWS CLI: attach-policy

  다음 예제에서는 정책을 OU에 연결합니다.

```
$ aws organizations attach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: AttachPolicy

정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 IAM 사용자와 역할이 가지는 권한에 영향을 줍니다.

조직 루트, OU 또는 계정에서 SCP 분리

조직의 관리 계정에 로그인하면 연결된 루트, OU 또는 계정에서 SCP를 분리할 수 있습니다. 개체에서 SCP를 분리하면 해당 SCP는 현재 분리된 개체의 영향을 받는 IAM 사용자 및 IAM 역할에 더 이상 적용되지 않습니다. SCP를 분리하려면 다음 단계를 완료하세요.

> **Note**
>
> 마지막 SCP는 루트, OU 또는 계정에서 분리할 수 없습니다. 모든 루트, OU, 계정에는 언제나 하나 이상의 SCP가 연결돼 있어야 합니다.

> **최소 권한**
>
> 루트, OU 또는 계정에서 SCP를 분리하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.
>
> - `organizations:DetachPolicy`

AWS Management Console

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 SCP를 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 SCP을 분리하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다

(▶
선택). 루트, OU 또는 계정의 이름을 선택합니다.

3. 정책(Policies) 탭에서, 분리할 SCP 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

   연결된 SCP의 목록이 업데이트됩니다. SCP 분리로 인해 발생하는 정책 변경은 즉시 적용됩니다. 예를 들어, SCP 분리는 이전에 연결된 계정이나 이전에 연결된 루트 또는 OU에 있는 계정의 IAM 사용자와 역할이 가지고 있는 권한에 즉시 영향을 미칩니다.

정책으로 이동하여 SCP를 분리하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 제어 정책(Service control policies) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
   (▶
   선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

   연결된 SCP의 목록이 업데이트됩니다. SCP 분리로 인해 발생하는 정책 변경은 즉시 적용됩니다. 예를 들어, SCP 분리는 이전에 연결된 계정이나 이전에 연결된 루트 또는 OU에 있는 계정의 IAM 사용자와 역할이 가지고 있는 권한에 즉시 영향을 미칩니다.

AWS CLI & AWS SDKs

루트, OU 또는 계정에서 SCP를 분리하려면

다음 명령 중 하나를 사용하여 SCP를 분리할 수 있습니다.

- AWS CLI: detach-policy

  다음 예제에서는 지정된 OU에서 지정된 SCP를 분리합니다.

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWS SDK: DetachPolicy

정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 IAM 사용자와 역할이 가지는 권한에 영향을 줍니다.

SCP 평가

> **Note**
>
> 이 단원의 정보는 AI 서비스 옵트아웃 정책, 백업 정책 또는 태그 정책을 비롯한 관리 정책 유형에 적용되지 않습니다. 자세한 내용은 관리 정책 상속에 대한 이해 섹션을 참조하세요.

AWS Organizations에서 여러 수준의 다양한 서비스 제어 정책 (SCP) 을 연결할 수 있으므로 SCP가 평가되는 방식을 이해하면 올바른 결과를 산출하는 SCP를 작성하는 데 도움이 될 수 있습니다.

주제

- SCP가 Allow와 협력하는 방식
- SCP가 거부를 처리하는 방식
- SCP 사용 전략

SCP가 Allow와 협력하는 방식

특정 계정에 대한 권한을 허용하려면 계정(대상 계정 자체 포함)의 직접 경로에 대한 루트부터 각 OU까지 모든 수준에서 명시적인 **`Allow`** 설명이 있어야 합니다. 그렇기에 SCP를 활성화하면 AWS Organizations은(는) 모든 서비스와 작업을 허용하는 FullAWSAccess라는 AWS 관리형 SCP 정책이 연결됩니다. 조직의 어느 수준에서도 이 정책을 제거하고 교체하지 않으면 해당 수준 이하의 모든 OU와 계정은 어떤 조치도 취하지 못하게 됩니다.

예를 들어 그림 1과 2에 표시된 시나리오를 살펴보겠습니다. 계정 B에서 권한 또는 서비스를 허용하려면 권한 또는 서비스를 허용하는 SCP를 루트, 프로덕션 OU 및 계정 B 자체에 연결해야 합니다.

SCP 평가는 기본 거부 모델을 따릅니다. 즉, SCP에서 명시적으로 허용되지 않은 권한은 거부됩니다. 루트, 프로덕션 OU 또는 계정 B와 같은 수준의 SCP에 허용되는 설명이 없으면 액세스가 거부됩니다.

> **주의**
>
> - SCP의 `Allow` 문에서 `Resource` 요소에는 `"*"` 항목만 사용할 수 있습니다.
> - SCP의 `Allow` 문은 어떠한 `Condition` 요소도 가질 수 없습니다.

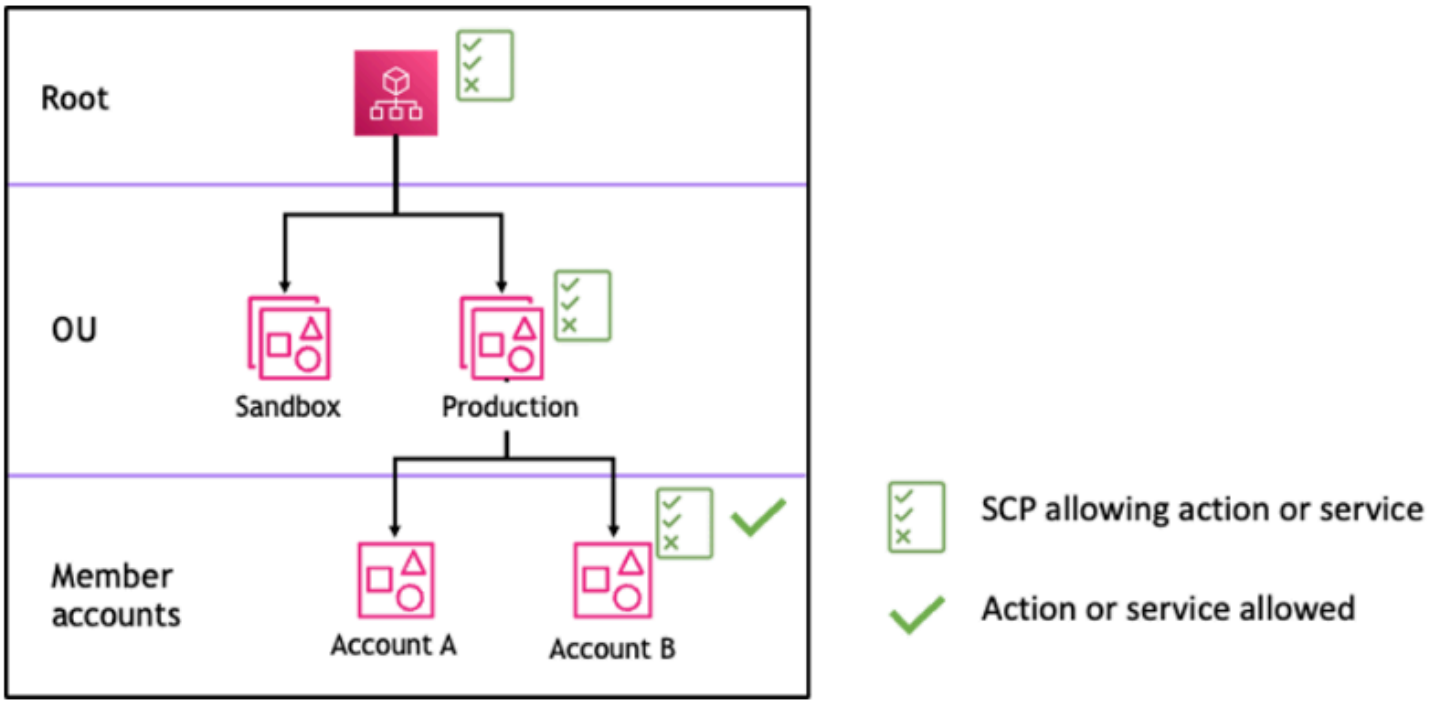


그림 1: 루트, 프로덕션 OU 및 계정 B에 `Allow` 설명이 첨부된 조직 구조의 예

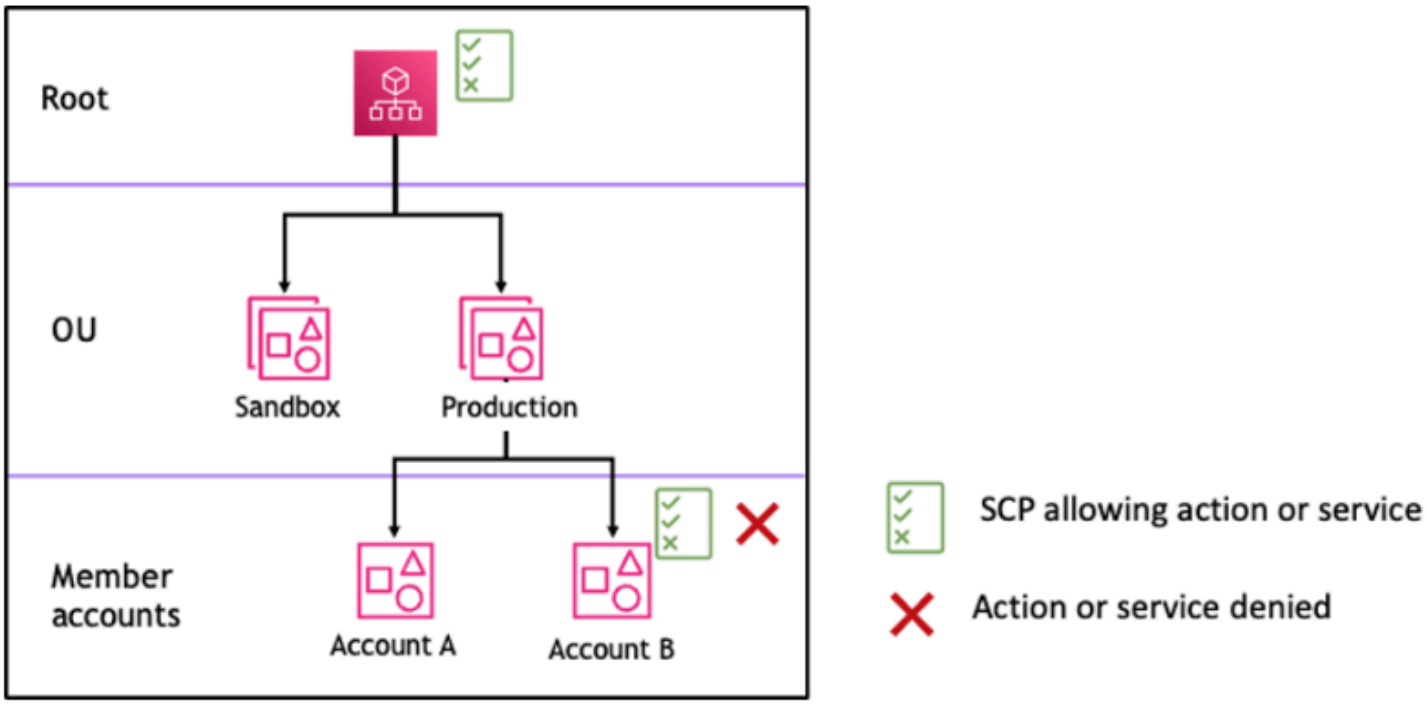


그림 2: 프로덕션 OU에서 누락된 Allow 설명이 있는 조직 구조의 예와 이것이 계정 B에 미치는 영향

SCP가 거부를 처리하는 방식

특정 계정에 대한 권한이 거부되는 경우, 루트에서 각 OU를 거쳐 계정의 직접 경로(대상 계정 자체 포함)에 있는 모든 SCP가 해당 권한을 거부할 수 있습니다.

예를 들어 프로덕션 OU에 특정 서비스에 대한 명시적 Deny 설명이 있는 SCP가 연결되어 있다고 가정해 보겠습니다. 그림 3과 같이 루트와 계정 B에 연결된 또 다른 SCP가 있는데, 이는 동일한 서비스에 대한 액세스를 명시적으로 허용합니다. 따라서 조직의 모든 수준에 연결된 거부 정책을 모든 OU 및 해당 계정 아래에 있는 멤버 계정에서 평가하므로 계정 A와 계정 B 모두 서비스에 대한 액세스가 거부됩니다.

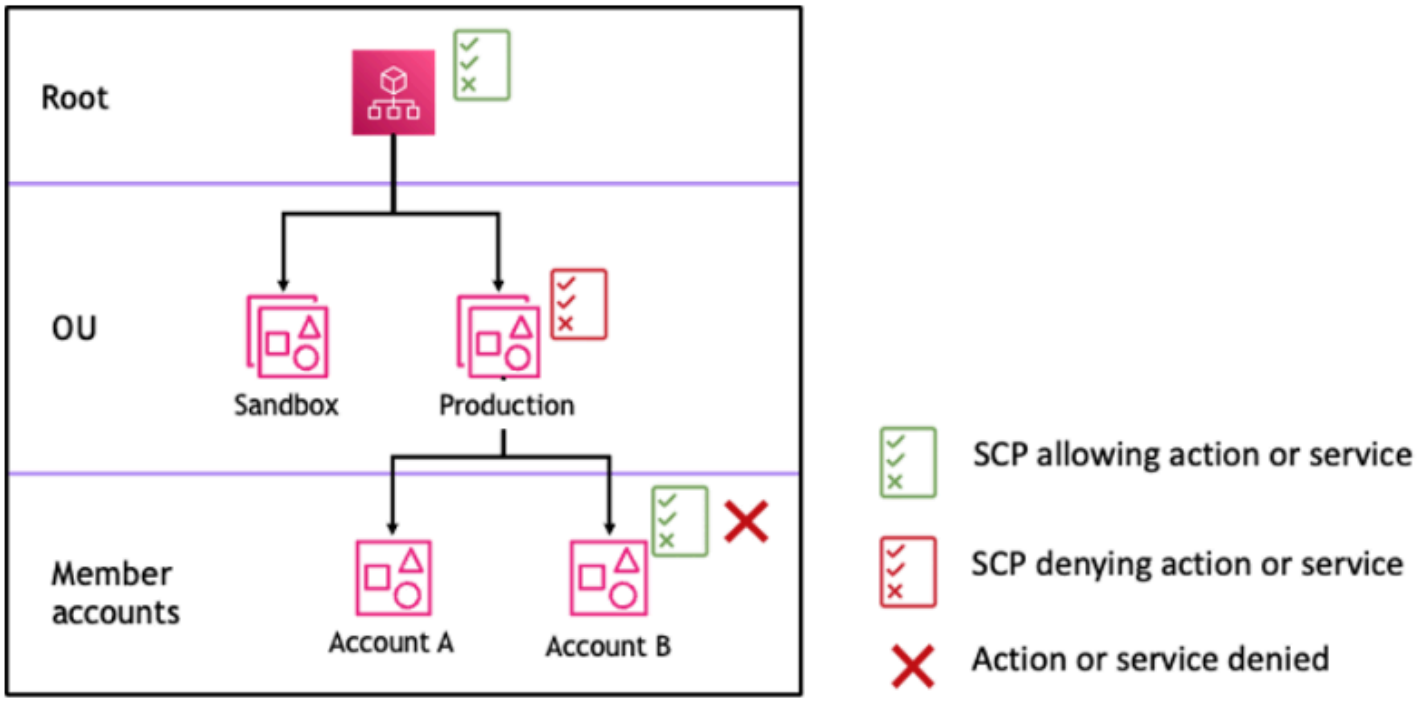


그림 3: 프로덕션 OU에 Deny 설명이 연결된 조직 구조의 예와 이것이 계정 B에 미치는 영향

SCP 사용 전략

SCP를 작성할 때 Allow 및 Deny 명령문을 조합하여 조직에서 의도한 조치와 서비스를 허용할 수 있습니다. Deny 명령문은 루트 수준이나 OU 수준에서 적용되면 그 아래 있는 모든 계정에 적용되기 때문에 조직 또는 OU의 더 넓은 부분에 적용되어야 하는 제한을 구현할 수 있는 강력한 방법입니다.

예를 들어 루트 수준에서 멤버 계정이 조직을 나가지 못하도록 방지을(를) 사용한 정책을 구현할 수 있는데, 이 정책은 조직의 모든 계정에 유효합니다. 거부 명령문은 예외를 생성하는 데 유용할 수 있는 조건 요소도 지원합니다.

> **Tip**
>
> IAM에서 서비스가 마지막으로 액세스한 데이터를 사용하여 필요한 AWS 서비스로만 액세스를 제한할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 Organizations에서 서비스가 마지막으로 액세스한 데이터 보기를 참조하세요.

AWS Organizations은(는) FullAWSAccess라는 AWS 관리형 SCP를 생성할 때 이를 모든 루트와 OU에 연결합니다. 이 정책은 모든 서비스와 작업을 허용합니다. FullAWSAccess를 서비스 집합만 허용하는 정책으로 대체하여 SCP를 업데이트하여 명시적으로 허용하지 않는 한 새 AWS 서비스가 허용되지

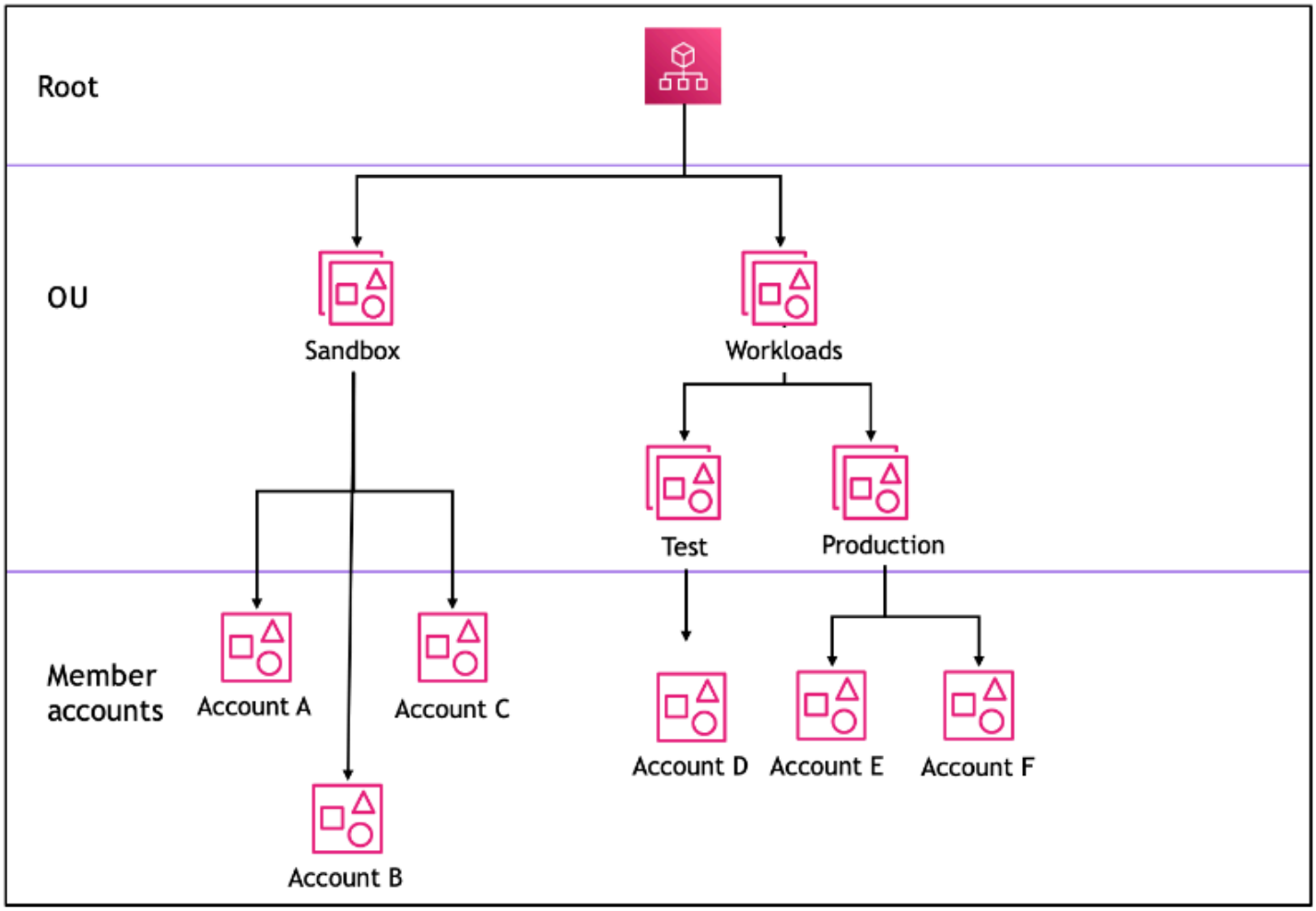
않도록 할 수 있습니다. 예를 들어 조직에서 사용자 환경의 하위 집합 서비스만 사용하도록 허용하려는 경우 Allow 명령문을 사용하여 특정 서비스만 허용할 수 있습니다.

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

두 명령문을 조합한 정책은 멤버 계정이 조직을 떠나는 것을 방지하고 원하는 AWS 서비스의 사용을 허용하는 다음 예와 유사할 수 있습니다. 조직 관리자는 FullAWSAccess 정책을 분리하고 대신에 이 정책을 연결하면 됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

이제 다음 샘플 조직 구조를 살펴보고 조직의 여러 수준에 다양한 SCP를 적용하는 방법을 이해해 보세요.



다음 표에는 샌드박스 OU의 효과적인 정책이 나와 있습니다.

시나리오	루트의 SCP	샌드박스 OU의 SCP	계정 A의 SC	계정 A의 결과 정책	계정 B 및 계정 C의 결과 정책
1	모든 AWS 액세스	모든 AWS 액세스 + S3 액세스 거부	모든 AWS 액세스 + EC2 액세스 거부	S3도 없고 EC2도 액세스할 수 없음	S3 액세스 권한 없음
2	모든 AWS 액세스	Amazon Elastic Compute	EC2 액세스 허용	EC2 액세스만 허용	EC2 액세스만 허용

시나리오	루트의 SCP	샌드박스 OU의 SCP	계정 A의 SC	계정 A의 결과 정책	계정 B 및 계정 C의 결과 정책
		Cloud(Amazon EC2) 액세스 허용			
3	S3 액세스 거부	S3 액세스 허용	모든 AWS 액세스	서비스 액세스 권한 없음	서비스 액세스 권한 없음

다음 표에는 워크로드 OU의 효과적인 정책이 나와 있습니다.

시나리오	루트의 SCP	워크로드 OU의 SCP	테스트 OU의 SCP	계정 D의 결과 정책	프로덕션 OU, 계정 E 및 계정 F의 결과 정책
1	모든 AWS 액세스	모든 AWS 액세스	모든 AWS 액세스 + EC2 액세스 거부	EC2 액세스 권한 없음	모든 AWS 액세스
2	모든 AWS 액세스	모든 AWS 액세스	EC2 액세스 허용	EC2 액세스 허용	모든 AWS 액세스
3	S3 액세스 거부	모든 AWS 액세스	S3 액세스 허용	서비스 액세스 권한 없음	서비스 액세스 권한 없음

SCP 구문

서비스 제어 정책 (SCP) 은 (IAM) 권한 정책 및 리소스 기반 정책 AWS Identity and Access Management (예: Amazon S3 버킷 정책) 에서 사용하는 것과 유사한 구문을 사용합니다. IAM 정책과 그 구문에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 개요를 참조하세요.

SCP는 JSON 규칙에 따라 구성된 일반 텍스트 파일입니다. SCP는 이번 주제에서 설명하는 요소를 사용합니다.

> **Note**
>
> SCP 내 모든 문자는 최대 크기를 기준으로 계수됩니다. 이 설명서의 예제는 가독성을 높이기 위한 추가 공백으로 포맷된 SCP를 보여 줍니다. 하지만 정책 크기가 최대 크기에 근접한 경우 공백을 저장하려면 인용 부호 바깥에 있는 공백 문자(예: 공백 및 줄 바꿈)를 모두 삭제할 수 있습니다.

SCP에 대한 일반적인 내용은 서비스 제어 정책(SCP) 단원을 참조하세요.

요소 요약

다음 표에는 SCP에서 사용할 수 있는 정책 요소가 요약되어 있습니다. 일부 정책 요소는 작업을 거부하는 SCP에서만 사용할 수 있습니다. 지원되는 효과(Supported effects) 열에는 SCP에서 각 정책 요소와 함께 사용할 수 있는 효과 유형이 나열되어 있습니다.

Element	용도	지원되는 효과
버전	정책을 처리하는 데 사용할 언어 구문 규칙을 지정합니다.	`Allow, Deny`
Statement	정책 요소 컨테이너의 역할을 합니다. SCP에 여러 문을 포함할 수 있습니다.	`Allow, Deny`
Statement ID(Sid)	(선택 사항) 문의 표시 이름	`Allow, Deny`

Element	용도	지원되는 효과
	을 제공합니다.	
효과	SCP 문이 계정의 IAM 사용자 및 역할에 대해 액세스를 허용하는지, 아니면 거부하는지를 정의합니다.	`Allow`, `Deny`
작업	SCP가 AWS 허용하거나 거부하는 서비스 및 작업을 지정합니다.	`Allow`, `Deny`
NotAction	SCP에서 제외되는 AWS 서비스 및 작업을 지정합니다. `Action` 요소 대신 사용합니다.	`Deny`

Element	용도	지원되는 효과
리소스	SCP가 적용되는 AWS 리소스를 지정합니다.	Deny
Condition	문이 효력을 발휘하는 조건을 지정합니다.	Deny

다음 섹션에서는 SCP에서 정책 요소가 사용되는 방식에 대한 자세한 설명 및 예제를 제공합니다.

`Version` 요소

모든 SCP에는 값이 `"2012-10-17"`인 `Version` 요소가 있어야 합니다. 이 버전 값은 IAM 권한 정책의 최신 버전과 같습니다.

```
    "Version": "2012-10-17",
```

자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 버전을 참조하세요.

`Statement` 요소

SCP는 하나 이상의 `Statement` 요소로 구성됩니다. 정책은 `Statement` 키워드 하나만 가질 수 있지만, 값은 ([ ] 문자로 구분한) JSON 문 어레이가 될 수 있습니다.

다음 예제는 하나의 `Effect`, `Action` 및 `Resource` 요소로 구성된 한 문을 보여줍니다.

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

다음 예제는 하나의 Statement 요소 안에 어레이 목록으로 존재하는 문 2개를 보여줍니다. 첫 번째 문은 모든 작업을 허용하지만 두 번째 문은 모든 EC2 작업을 거부합니다. 그 결과 계정 관리자는 Amazon Elastic Compute Cloud(Amazon EC2)를 제외한 모든 출처의 권한을 위임할 수 있습니다.

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 문을 참조하세요.

Statement ID(**Sid**) 요소

Sid는 정책 문에 입력되는 식별자(옵션)입니다. Sid 값은 문 배열에서 각 문에 할당할 수 있습니다. 다음 예제 SCP는 샘플 Sid 문을 보여줍니다.

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: ID를 참조하세요.

Effect 요소

각 문에는 Effect 요소 하나가 있어야 합니다. 이때 값은 Allow 또는 Deny가 될 수 있습니다. 이것은 같은 문에서 나열하는 모든 작업에 영향을 줍니다.

자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 효과를 참조하세요.

"Effect": "Allow"

다음 예제는 계정 사용자가 Amazon S3 서비스를 위한 작업을 수행하도록 허용하는 Allow 값을 갖는 Effect 요소를 포함한 문이 있는 SCP를 보여줍니다. 이 예제는 허용 목록 전략을 사용하는 조직에서 유용하게 활용할 수 있습니다(기본 FullAWSAccess 정책이 모두 분리되어 있어 기본적으로 권한이 묵시적으로 거부되는 전략). 결과적으로 이 문은 연결된 모든 계정에 대해 Amazon S3 권한을 허용합니다.

```
{
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

이 문은 IAM 권한 정책과 동일한 Allow 값 키워드를 사용하지만, SCP에서는 실제로 사용자에게 특정 작업을 수행할 수 있는 권한을 부여하지 않습니다. 대신 SCP는 조직의 IAM 사용자 및 IAM 역할에 대한 최대 권한을 지정하는 필터 역할을 합니다. 이전 예제에서, 계정의 사용자에게 AdministratorAccess 관리형 정책이 연결돼 있다 하더라도 이 SCP는 영향받는 계정의 모든 사용자가 Amazon S3 작업만 할 수 있게 합니다.

"Effect": "Deny"

Effect 요소의 값이 Deny인 문에서는 특정 리소스에 대한 액세스를 제한하거나 SCP가 효력을 발휘하는 조건을 정의할 수도 있습니다.

다음 예제는 거부 문에서 조건 키를 사용하는 방법을 보여줍니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
```

```
}
```

SCP에서 이 문은 Amazon EC2 인스턴스가 `t2.micro`로 설정되지 않은 경우 영향받는 계정(SCP가 계정 자체에 연결된 계정 또는 계정을 포함한 조직 루트 또는 OU에 연결된 계정)이 Amazon EC2 인스턴스를 시작하는 것을 금지하는 가드레일을 설정합니다. 이 작업을 허용하는 IAM 정책이 계정에 연결되어 있더라도 SCP에 의해 생성된 가드레일이 이를 금지합니다.

`Action` 및 `NotAction` 요소

각 문은 다음 중 하나를 포함해야 합니다.

- 허용 및 거부 문에서, `Action` 요소.
- 거부 문에서만(`Effect` 요소의 값이 `Deny`인 경우), `Action` 또는 `NotAction` 요소.

`Action`or `NotAction` 요소의 값은 명령문에 의해 허용되거나 거부되는 AWS 서비스 및 작업을 식별하는 문자열 목록 (JSON 배열) 입니다.

각 문자열은 서비스의 소문자 약자("s3", "ec2", "iam" 또는 "organizations" 등) 뒤에 콜론이 오고 그 뒤에 해당 서비스의 작업이 붙는 형태로 구성됩니다. Action 및 NotAction은 대/소문자를 구분하며, 각 서비스의 문서에 표시된 그대로 입력해야 합니다. 일반적으로 각 단어는 첫 글자만 대문자로, 나머지는 소문자로 입력합니다. 예를 들면 `"s3:ListAllMyBuckets"`입니다.

SCP에서 별표(*) 또는 물음표(?) 와 같은 와일드카드 문자도 사용할 수도 있습니다.

- 이름의 일부를 공유하는 여러 작업을 일치시키려면 별표(*)를 와일드카드로 사용하십시오. `"s3:*"` 값은 Amazon S3 서비스의 모든 작업을 의미합니다. `"ec2:Describe*"` 값은 "Describe"로 시작하는 EC2 작업에만 대응합니다.
- 단일 문자를 일치시키려면 물음표(?) 와일드카드를 사용하십시오.

> **Note**
>
> SCP에서 `Action` 또는 `NotAction` 요소의 와일드카드 문자 (*) 및 (?)는 단독으로 또는 문자열 끝에만 사용할 수 있습니다. 문자열 처음이나 중간에는 표시할 수 없습니다. 따라서 `"servicename:action*"`은 유효하지만 `"servicename:*action"`과 `"servicename:some*action"`은 SCP에서 유효하지 않습니다.

AWS Organizations SCP와 IAM 권한 정책에서 지원하는 모든 서비스 및 작업의 목록은 IAM 사용 설명서의 AWS 서비스에 대한 작업, 리소스 및 조건 키를 참조하십시오.

자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 작업 및 IAM JSON 정책 요소:를 참조하십시오. NotAction

`Action` 요소 예제

다음은 계정 관리자가 계정의 EC2 인스턴스에 대한 권한 설명, 시작, 중단, 중지를 위임하게 하는 문이 포함된 SCP를 보여주는 예제입니다. 이 예제는 허용 목록의 예입니다. 허용 목록은 기본 `Allow *` 정책이 연결되지 않아 기본적으로 권한이 묵시적으로 거부되는 때에 유용합니다. 기본 `Allow *` 정책이 다음과 같은 정책이 연결된 루트, OU 또는 계정에 여전히 연결돼 있다면, 해당 정책은 영향을 주지 못하게 됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

다음 예제는 연결된 계정에서 사용하지 않으려는 서비스에 대해 액세스를 거부하는 방법을 보여 줍니다. 기본 `"Allow *"` SCP가 모든 OU와 루트에 여전히 연결돼 있다고 가정합니다. 이 예제 정책은 연결 계정에 있는 계정 관리자가 IAM, Amazon EC2, Amazon RDS 서비스에 대해 어떤 권한도 위임하지 못하게 합니다. 이러한 권한을 거부하는 다른 연결된 정책이 없는 한, 다른 서비스의 모든 작업을 위임할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
```

```
}
```

NotAction 요소 예제

다음 예는 NotAction 요소를 사용하여 정책의 영향에서 AWS 서비스를 제외하는 방법을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
       }
     }
   ]
}
```

이 설명문을 사용하면 IAM 작업을 사용하는 경우를 제외하고 영향을 받는 계정은 지정된 AWS 리전작업을 수행하는 것으로 제한됩니다.

Resource 요소

Effect 요소의 값이 Allow인 문에서는 SCP의 Resource 요소에 "*"만 지정할 수 있습니다. 개별 Amazon 리소스 이름(ARN) 리소스를 지정할 수 없습니다.

리소스 요소에서 별표(*) 또는 물음표(?)와 같은 와일드카드 문자를 사용할 수도 있습니다.

- 이름의 일부를 공유하는 여러 작업을 일치시키려면 별표(*)를 와일드카드로 사용하십시오.
- 단일 문자를 일치시키려면 물음표(?) 와일드카드를 사용하십시오.

Effect 요소의 값이 Deny인 문에서는 다음 예제와 같이 개별 ARN을 지정하는 것이 가능합니다.

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

```
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

이 SCP는 영향받는 계정의 IAM 사용자 및 역할이 조직 내 모든 계정에 생성된 공통 관리 IAM 역할을 변경하지 못하게 제한합니다.

자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 리소스를 참조하세요.

`Condition` 요소

SCP에서 거부 문에 `Condition` 요소를 지정할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

이 SCP는 나열된 서비스의 작업을 제외하고 `eu-central-1` 및 `eu-west-1` 리전 외부의 작업에 대한 액세스를 거부합니다.

자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

지원되지 않는 요소

다음 요소는 SCP에서 지원되지 않습니다.

- `Principal`
- `NotPrincipal`
- `NotResource`

서비스 제어 정책 예

이 주제에 나온 예제 서비스 제어 정책(SCP)은 정보 제공용입니다.

> **이 예제를 사용하기 전에**
>
> 조직에서 예제 SCP를 사용하기 전에 다음 단계를 수행해야 합니다.
>
> - 신중하게 예제 SCP를 검토하고 자신의 요구 사항에 맞게 사용자 지정합니다.
> - 자신의 환경과 사용 중인 AWS 서비스에서 SCP를 철저히 테스트합니다.
>
> 이 단원의 정책 예제는 SCP의 구현과 사용을 보여줍니다. 그러나 제시된 그대로 실행할 수 있는 공식적인 AWS 권장 사항 또는 모범 사례로 해석해서는 안 됩니다. 고객은 자신의 환경이 가진 비즈니스 요구 사항을 해결하기 위해 거부 기반 정책의 적합성을 테스트할 책임이 있습니다. 거부 기반 서비스 제어 정책은 정책에 필요한 예외 항목을 추가하지 않는 한 AWS

서비스 사용을 의도하지 않게 제한하거나 차단할 수 있습니다. 이러한 예외의 예는 원하지 않는 AWS 리전에 대한 액세스를 차단하는 규칙에서 전역 서비스를 제외하는 첫 번째 예에 제시되어 있습니다.

- SCP는 모든 사용자 및 역할(연결된 모든 계정의 루트 사용자 포함)에 영향을 준다는 점을 기억해야 합니다.

Tip

IAM에서 서비스가 마지막으로 액세스한 데이터를 사용하여 필요한 AWS 서비스로만 액세스를 제한할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 Organizations에서 서비스가 마지막으로 액세스한 데이터 보기를 참조하세요.

다음 각 정책은 거부 목록 정책 전략의 예제입니다. 거부 목록 정책은 해당 계정에서 승인된 작업을 허용하는 다른 정책과 연결되어야 합니다. 예를 들어 기본 `FullAWSAccess` 정책은 계정의 모든 서비스 사용을 허용합니다. 이 정책은 기본적으로 루트, 모든 조직 단위(OU) 및 모든 계정에 연결됩니다. 실제로 권한을 부여하지 않습니다. 어떠한 SCP도 부여하지 않습니다. 그 대신, 이 정책은 해당 계정의 관리자가 표준 AWS Identity and Access Management(IAM) 권한 정책을 계정의 사용자, 역할 또는 그룹에 연결하여 이러한 작업에 대한 액세스를 위임할 수 있도록 허용합니다. 그런 다음 이러한 각 거부 목록 정책은 특정 서비스 또는 작업에 대한 액세스를 차단하여 모든 정책을 재정의합니다.

예

- 일반 예제
  - 요청된 AWS 리전에 따라 AWS에 대한 액세스를 거부
  - IAM 사용자 및 역할이 특정 변경을 수행하지 못하도록 방지
  - IAM 사용자 및 역할이 지정된 변경을 수행하지 못하도록 방지(지정된 관리자 역할은 제외)
  - API 작업을 수행하기 위해 MFA 필요
  - 루트 사용자의 서비스 액세스 차단
  - 멤버 계정이 조직을 나가지 못하도록 방지
- Amazon CloudWatch에 대한 SCP 예제
  - 사용자의 CloudWatch 비활성화 또는 구성 변경 방지
- AWS Config에 대한 SCP 예제
  - 사용자의 AWS Config 비활성화 또는 규칙 변경 방지

일반 예제

요청된 AWS 리전에 따라 AWS에 대한 액세스를 거부

이 SCP는 지정된 리전 외부의 모든 작업에 대한 액세스를 거부합니다. `eu-central-1`과 `eu-west-1`을, 사용할 AWS 리전으로 대체합니다. 승인된 글로벌 서비스의 운영에 대한 공제를 제공합니다. 이 예제에서는 지정된 두 관리자 역할 중 하나에 의해 수행되는 요청을 제외하는 방법도 보여 줍니다.

> **Note**
>
> 리전 거부 SCP를 AWS Control Tower와 함께 사용하려면 요청된 AWS 리전에 따라 AWS에 대한 액세스를 거부 단원을 참조하세요.

이 정책은 Deny 효과를 사용하여 승인된 두 리전(eu-central-1 및 eu-west-1) 중 하나를 대상으로 하지 않는 작업에 대한 모든 요청에 대한 액세스를 거부합니다. NotAction 요소를 사용하면 이 제한에서 제외되는 작업(또는 개별 작업)의 서비스를 나열할 수 있습니다. 글로벌 서비스에는 us-east-1 리전에 의해 물리적으로 호스팅되는 엔드포인트가 있으므로 이러한 방식으로 제외해야 합니다. 이러한 방식으로 구성된 SCP에서는 요청된 서비스가 NotAction 요소에 포함된 경우 us-east-1 리전의 글로벌 서비스를 요청합니다. us-east-1 리전 내 서비스에 대한 다른 요청은 이 예제 정책에 의해 거부됩니다.

> **Note**
>
> 이 예제는 최근 전역 AWS 서비스 또는 작업을 모두 포함하지 않을 수 있습니다. 서비스 및 작업 목록을 조직 내 계정에 의해 사용되는 전역 서비스로 대체합니다.
>
> > **도움말**
> >
> > IAM 콘솔에서 서비스가 마지막으로 액세스한 데이터를 보고, 조직에서 사용하는 글로벌 서비스를 확인할 수 있습니다. IAM 사용자, 그룹 또는 역할에 대한 세부 정보 페이지의 액세스 관리자(Access Advisor) 탭에는 해당 엔터티에서 사용했던 AWS 서비스가 가장 최근 액세스를 기준으로 정렬되어 표시됩니다.

> **고려 사항**
>
> - AWS KMS 및 AWS Certificate Manager는 리전 엔드포인트를 지원합니다 그러나 Amazon CloudFront와 같은 글로벌 서비스와 함께 사용하려면 다음 SCP 예제의 글로벌 서비스 제외 목록에 이를 포함시켜야 합니다. Amazon CloudFront와 같은 글로벌 서비스는 일반적으로 동일한 리전에서 AWS KMS 및 ACM에 액세스해야 합니다. 글로벌 서비스의 경우 미국 동부(버지니아 북부) 리전(us-east-1)입니다.
> - 기본적으로 AWS STS는 글로벌 서비스이며, 글로벌 서비스 제외 목록에 포함되어야 합니다. 그러나 AWS STS가 하나의 글로벌 엔드포인트 대신에 리전 엔드포인트를 사용하도록

설정할 수 있습니다. 이렇게 하면 다음 예제 SCP의 글로벌 서비스 제외 목록에서 STS를 제거할 수 있습니다. 자세한 내용은 AWS 리전에서 AWS STS 관리를 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
```

```
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

IAM 사용자 및 역할이 특정 변경을 수행하지 못하도록 방지

이 SCP는 IAM 사용자 및 역할이 조직 내 모든 계정에 생성된 특정 IAM 역할을 변경하지 못하게 제한합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
```

```
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

IAM 사용자 및 역할이 지정된 변경을 수행하지 못하도록 방지(지정된 관리자 역할은 제외)

이 SCP는 이전 예제를 기반으로 관리자에 대한 예외를 추가하여 작성된 것입니다. 이 정책은 영향받는 계정의 IAM 사용자 및 역할이 조직 내 모든 계정에 생성된 공통 관리 IAM 역할을 변경하지 못하게 제한하되 지정된 역할을 사용하는 관리자는 제외합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
```

```
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

API 작업을 수행하기 위해 MFA 필요

다음과 같은 SCP를 사용하면 IAM 사용자 또는 역할이 작업을 수행하기 위해 먼저 멀티 팩터 인증(MFA)을 활성화하도록 요구할 수 있습니다. 이 예제에서 작업은 Amazon EC2 인스턴스를 중지하는 것입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

루트 사용자의 서비스 액세스 차단

다음 정책은 멤버 계정의 루트 사용자에 대해 지정된 작업에 대한 모든 액세스를 제한합니다. 계정이 특정 방식으로 루트 자격 증명을 사용하는 것을 방지하려면 이 정책에 자체 작업을 추가하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
```

```
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

멤버 계정이 조직을 나가지 못하도록 방지

다음 정책은 `LeaveOrganization` API 작업 사용을 차단해 멤버 계정의 관리자가 조직에서 자신의 계정을 제거하지 못하도록 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon CloudWatch에 대한 SCP 예제

이 범주의 예

- 사용자의 CloudWatch 비활성화 또는 구성 변경 방지

사용자의 CloudWatch 비활성화 또는 구성 변경 방지

하급 CloudWatch 운영자는 대시보드와 경보를 모니터링해야 합니다. 그러나 이러한 운영자는 상급 운영자가 설정한 어떠한 대시보드 또는 경보도 삭제하거나 변경할 수 없어야 합니다. 이 SCP는 영향받는 모든 계정의 사용자 또는 역할이 대시보드 또는 알람을 삭제하거나 변경할 수 있는 어떠한 CloudWatch 명령도 수행하지 못하도록 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Config에 대한 SCP 예제

이 범주의 예

- 사용자의 AWS Config 비활성화 또는 규칙 변경 방지

사용자의 AWS Config 비활성화 또는 규칙 변경 방지

SCP는 어떠한 영향을 받은 계정의 사용자 또는 역할이든지 AWS Config를 비활성화거나 그 규칙을 변경 또는 트리거할 수 있는 AWS Config 작업을 수행하지 못하도록 합니다.

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

```
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon Elastic Compute Cloud(Amazon EC2)에 대한 SCP 예제

이 범주의 예

- Amazon EC2 인스턴스가 특정 유형을 사용하도록 요구
- IMDSv2가 없는 EC2 인스턴스 시작을 방지
- 기본 Amazon EBS 암호화 비활성화 방지

Amazon EC2 인스턴스가 특정 유형을 사용하도록 요구

이 SCP는 `t2.micro` 인스턴스 유형을 사용하지 않는 인스턴스 시작을 모두 거부합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

IMDSv2가 없는 EC2 인스턴스 시작을 방지

다음 정책은 모든 사용자가 IMDSv2 없이 EC2 인스턴스를 시작하지 못하도록 제한합니다.

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

다음 정책은 모든 사용자가 IMDSv2 없이 EC2 인스턴스를 시작하지 못하도록 제한하지만 특정 IAM 자격 증명이 인스턴스 메타데이터 옵션을 수정할 수 있도록 허용합니다.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
```

```
      }
    }
  }
]
```

기본 Amazon EBS 암호화 비활성화 방지

다음 정책은 모든 사용자가 기본 Amazon EBS 암호화를 비활성화하지 못하도록 제한합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

Amazon GuardDuty에 대한 SCP 예제

이 범주의 예

- 사용자의 GuardDuty 비활성화 또는 구성 변경 방지

사용자의 GuardDuty 비활성화 또는 구성 변경 방지

이 SCP는 영향받는 모든 계정의 사용자 또는 역할이 직접적인 명령이나 콘솔을 통해서 GuardDuty를 비활성화하거나 그 구성을 변경하지 못하도록 합니다. 이를 통해 GuardDuty 정보 및 리소스의 읽기 전용 액세스를 효과적으로 활성화할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
```

```
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Resource Access Manager에 대한 SCP 예제

이 범주의 예

- 외부 공유 방지
- 특정 계정에 대해 지정된 자원 유형만 공유하도록 허용
- 조직 또는 조직 단위(OU)와의 공유 금지
- 지정된 IAM 사용자 및 역할과의 공유만 허용

외부 공유 방지

다음 SCP 예제는 사용자가 조직에 속하지 않은 IAM 사용자 및 역할과의 공유를 허용하는 리소스 공유를 만들지 못하도록 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

특정 계정에 대해 지정된 자원 유형만 공유하도록 허용

다음 SCP는 111111111111 및 222222222222 계정이 접두사 목록을 공유하는 리소스 공유를 만들고 접두사 목록을 기존 리소스 공유와 연결할 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
```

```
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

조직 또는 조직 단위(OU)와의 공유 금지

다음 SCP는 사용자가 리소스를 AWS 조직 또는 OU와 공유하는 리소스 공유를 생성하지 못하도록 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

지정된 IAM 사용자 및 역할과의 공유만 허용

다음 SCP 예제는 사용자에게 조직 `o-12345abcdef`, 조직 단위 `ou-98765fedcba`, 계정 111111111111과의 리소스 공유만을 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
    ]
}
```

Amazon Route 53 애플리케이션 복구 컨트롤러용 예시 SCP

이 범주의 예

- 사용자가 Route 53 ARC 라우팅 제어 상태를 업데이트하지 못하도록 방지

사용자가 Route 53 ARC 라우팅 제어 상태를 업데이트하지 못하도록 방지

하위 수준의 Route 53 ARC 운영자는 대시보드를 모니터링하고 Route 53 ARC 정보를 볼 수 있어야 합니다. 상급 운영자는 가능하지만, 운영자는 라우팅 제어를 업데이트하여 한 AWS 리전 애플리케이션에서 다른 애플리케이션으로 장애 조치를 수행할 수 없어야 합니다. 이 SCP는 영향을 받는 계정의 사용자 또는 역할이 Route 53 ARC 라우팅 제어를 업데이트하는 Route 53 ARC 작업을 실행하지 못하도록 합니다.

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

```
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

SCP for Amazon S3 예제

이 범주의 예

- Amazon S3의 암호화되지 않은 객체 업로드 방지

Amazon S3의 암호화되지 않은 객체 업로드 방지

다음 정책은 모든 사용자가 암호화되지 않은 객체를 S3 버킷에 업로드하지 못하도록 제한합니다.

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

다음 정책은 모든 사용자가 암호화되지 않은 객체를 S3 버킷에 업로드하지 못하도록 제한하고 버킷의 객체 업로드에 대해 지정된 암호화 유형(AES256 또는 aws:kms)을 적용합니다.

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

리소스 태그 지정에 대한 SCP 예제

이 범주의 예

- 생성되는 특정 리소스에 대한 태그 요구
- 권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지

생성되는 특정 리소스에 대한 태그 요구

다음 SCP는 요청에 지정된 태그가 포함되지 않은 경우 영향받는 계정의 IAM 사용자 및 역할이 특정 리소스 유형을 생성하지 못하도록 합니다.

> **Important**
>
> 자신의 환경에서 사용하는 서비스에서 거부 기반 정책을 테스트해야 합니다. 다음 예제는 태그가 지정되지 않은 보안 암호를 생성하거나 태그가 지정되지 않은 Amazon EC2 인스턴스를 실행하는 것을 차단하며, 예외가 없습니다.

다음 정책 예제는 작성된 바와 같이 AWS CloudFormation과 호환되지 않습니다. 해당 서비스는 보안 암호를 생성한 다음 분리된 두 단계로 태그를 지정하기 때문입니다. 이 정책 예제는 AWS CloudFormation이 스택의 일부로 보안 암호를 생성하는 것을 효과적으로 차단합니다. 이러한 작업은 요구에 따라 태그가 지정되지 않은 보안 암호를 짧은 시간 내에 생성하기 때문입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
```

```
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

AWS Organizations SCP와 IAM 권한 정책에서 모두 지원하는 서비스와 작업의 전체 목록을 확인하려면, IAM 사용 설명서의 AWS 서비스에 사용되는 작업 및 조건 키를 참조하세요.

권한 있는 보안 주체 외에는 태그를 수정할 수 없도록 방지

다음 SCP는 권한 있는 보안 주체만 리소스에 연결된 태그를 수정하도록 정책을 구성하는 방법을 보여줍니다. 이는 AWS 클라우드 보안 전략의 일환으로 속성 기반 액세스 제어(ABAC)를 사용할 때 중요한 부분입니다. 이 정책은 권한 부여 태그(이 예제에서는 `access-project`)가 요청을 수행하는 사용자 또는 역할에 연결된 동일한 권한 부여 태그와 정확히 일치하는 리소스의 태그만을 호출자가 수정할 수 있도록 허용합니다. 또한 이 정책은 권한 있는 사용자가 권한 부여에 사용되는 태그의 값을 변경하지 못하도록 합니다. 변경을 수행하려면 호출하는 보안 주체에게 권한 부여 태그가 있어야 합니다.

이 정책은 권한 없는 사용자만 태그를 변경하지 못하도록 차단합니다. 이 정책에 의해 차단되지 않은 권한 있는 사용자에게는 관련 태그 지정 API에서 `Allow` 권한을 명시적으로 부여하는 별도의 IAM 정책이 여전히 필요합니다. 예를 들어 사용자에게 `Allow */*`(모든 서비스와 모든 작업 허용)를 사용한 관리자 정책이 있는 경우 결합을 통해 관리 사용자는 사용자의 보안 주체에 연결된 권한 부여 태그와 일치하는 권한 부여 태그 값을 가진 태그만 변경할 수 있습니다. 이 정책의 명시적 `Deny`가 관리자 정책의 명시적 `Allow`를 무시하기 때문입니다.

Important

이는 완전한 정책 솔루션이 아니므로 여기에 제시된 대로 사용해서는 안 됩니다. 이 예제는 ABAC 전략의 일부를 설명하기 위한 것이므로 프로덕션 환경에 맞게 사용자 지정하고 테스트해야 합니다.
작동 방식에 대한 상세 분석을 포함한 전체 정책은 AWS Organizations에서 서비스 제어 정책을 사용하여 권한 부여에 사용되는 리소스 태그 보호를 참조하세요.
자신의 환경에서 사용하는 서비스에서 거부 기반 정책을 테스트해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Amazon Virtual Private Cloud(Amazon VPC)에 대한 SCP 예제

이 범주의 예

- 사용자의 Amazon VPC 흐름 로그 삭제 방지
- 인터넷 액세스가 없는 VPC가 액세스 권한을 얻지 못하도록 방지

사용자의 Amazon VPC 흐름 로그 삭제 방지

이 SCP는 영향 받는 모든 계정의 사용자 또는 역할이 Amazon Elastic Compute Cloud(Amazon EC2) 흐름 로그나 CloudWatch 로그 그룹 또는 로그 스트림을 삭제하지 못하도록 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

인터넷 액세스가 없는 VPC가 액세스 권한을 얻지 못하도록 방지

이 SCP는 영향 받는 모든 계정의 사용자 또는 역할이 Amazon EC2 virtual private clouds(VPC)의 구성을 변경하여 인터넷에 대한 직접 액세스 권한을 부여하는 것을 방지합니다. 이는 기존 직접 액세스 또는 온프레미스 네트워크 환경을 통한 라우팅을 하는 어떠한 액세스도 막지 않습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
```

```
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

조직 단위 관리

조직 단위(OU)를 사용하면 계정을 그룹으로 만들어 단일 유닛으로 관리할 수 있습니다. 이 기능을 이용하면 계정 관리가 대단히 간편해집니다. 예를 들어 정책 기반 제어를 OU에 연결하면, OU 안의 모든 계정이 정책을 자동으로 상속합니다. 단일 조직에서 여러 OU를 생성하고, 다른 OU 안에 OU를 만들 수도 있습니다. OU 하나에 여러 개의 계정을 적용할 수 있고, 계정을 다른 OU로 옮길 수도 있습니다. 하지만 상위 OU나 루트에는 고유한 OU 이름만 존재해야 합니다.

> **Note**
>
> 조직에는 루트가 하나 있으며, 이 루트는 조직을 처음 설정할 때 자동으로 AWS Organizations 생성됩니다.

주제

- 루트 및 OU 계층 관리
- OU 만들기
- OU 이름 변경
- OU에 연결된 태그 편집
- 계정을 OU로 이동하거나 루트와 OU 간에 이동
- OU 삭제

조직 전체의 모든 OU를 검토할 수도 있습니다. 자세한 내용은 OU의 세부 정보 보기를 참조하세요.

루트 및 OU 계층 관리

계정을 이동하거나 정책을 연결할 때 다른 OU 또는 루트로 이동하기 위해 기본 “트리” 보기를 사용할 수 있습니다.

AWS Management Console

조직을 '트리'로 탐색하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. AWS 계정 페이지의 조직(Organization) 섹션 상단에서 계층 구조(Hierarchy) 토글(목록(List) 대신)을 선택합니다.
3. 처음에 트리에는 하위 OU 및 계정의 첫 번째 레벨만 표시된 루트가 나타납니다. 하위 레벨을 더 표시하도록 트리를 확장하려면 상위 엔터티 옆에 있는 확장 아이콘 ( ) 을 선택합니다. 트리 가지를 축소하여 간단하게 표시하려면 확장된 상위 개체 옆에 있는 축소 아이콘 ( ) 을 선택합니다.
4. 세부 정보를 보고 특정 작업을 수행하려면 OU 또는 루트의 이름을 선택합니다. 또는 이름 옆의 라디오 버튼을 선택하고 작업(Actions) 메뉴에서 해당 엔터티에 대한 작업을 선택합니다.

또한 OU를 찾기 위해 먼저 탐색할 필요 없이 조직의 계정 목록만 표 형식으로 볼 수도 있습니다. 이 보기에서는 OU를 보거나 그에 연결된 정책을 조작할 수 없습니다.

AWS Management Console

계층 구조가 없는 단순 계정 목록으로 조직을 표시하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정페이지의 조직 섹션 상단에서 보기 AWS 계정 전용 스위치 아이콘을 선택하여 활성화합니다.
3. 계정 목록이 계층 구조 없이 표시됩니다.

OU 만들기

조직의 관리 계정에 로그인하면 조직의 루트에서 OU를 생성할 수 있습니다. OU는 최대 5개까지 중첩할 수 있습니다. OU를 만들려면 다음 단계를 완료하세요.

> **Important**
>
> 이 조직을 로 AWS Control Tower관리하는 경우 AWS Control Tower 콘솔 또는 API를 사용하여 OU를 생성하십시오. Ouganizations에서 OU를 생성하는 경우 해당 OU는 등록되지 않

습니다 AWS Control Tower. 자세한 내용은 AWS Control Tower사용 설명서의 AWS Control Tower 외부 리소스 참조를 참조하세요.

최소 권한

조직의 루트 내에 OU를 만들려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:CreateOrganizationalUnit`

AWS Management Console

OU를 만들려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지로 이동합니다.

   콘솔에 루트 OU와 그 내용이 표시됩니다. 루트를 처음으로 방문하면 콘솔의 최상위 보기에 모든 AWS 계정 이 표시됩니다. 이전에 OU를 생성해 계정을 OU로 이동했다면, 콘솔은 최상위 OU와 아직 OU로 이동하지 않은 계정만 표시합니다.
3. (선택 사항) 기존 OU 내에 OU를 생성하려면, 하위 OU의 이름(확인란 아님)을 선택하거나 원하는 항목이 보일 때까지 트리 보기에서 OU 옆의 ▶ 을 선택하여 하위 OU로 이동한 다음 이름을 선택합니다.
4. 계층 구조에서 올바른 상위 OU를 선택했으면 작업(Actions) 메뉴의 조직 단위(Organizational Unit)에서 새로 만들기(Create new)를 선택합니다.
5. 조직 단위 생성(Create organizational unit) 대화 상자에서 생성하려는 OU의 이름을 입력합니다.
6. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 하나 이상의 태그를 추가합니다. 값을 공백으로 남겨두면 `null`이 아닌 빈 문자열로 설정됩니다. OU에는 최대 50개의 태그를 연결할 수 있습니다.
7. 마지막으로 조직 단위 생성(Create organizational unit)을 선택합니다.

새 OU가 상위 OU 내에 표시될 것입니다. 이제 계정을 이 OU로 이동하거나 OU에 정책을 연결할 수 있습니다.

AWS CLI & AWS SDKs

OU를 만들려면

다음 명령 중 하나를 사용하여 OU를 생성할 수 있습니다.

- AWS CLI: create-organizational-unit

  OU를 생성하려면 먼저 새 OU의 상위가 될 루트 또는 OU의 자격 증명을 찾아야 합니다.

  루트의 자격 증명을 찾으려면 list-roots 명령을 사용합니다. OU의 자격 증명을 찾으려면 list-children을 사용해 원하는 OU로 이동합니다.

  다음 예제에서는 루트의 자격 증명을 찾은 다음 루트 아래에서 OU의 자격 증명을 찾는 방법을 보여 줍니다. 마지막 명령은 찾은 OU에서 새 OU를 만드는 방법을 보여 줍니다.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children \
    --parent-id r-a1b2 \
    --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
```

```
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- AWS SDK: CreateOrganizationalUnit

OU 이름 변경

조직의 관리 계정에 로그인하면 OU 이름을 바꿀 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

> 최소 권한
>
> AWS 조직의 루트 내에서 OU의 이름을 바꾸려면 다음 권한이 있어야 합니다.
>
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
> - `organizations:UpdateOrganizationalUnit`

AWS Management Console

OU의 이름을 바꾸려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 이름을 바꿀 OU로 이동한 다음, 아래의 단계 중 하나를 수행합니다.
   - 이름을 변경할 OU 옆에 있는 라디오 버튼  을 선택합니다. 그런 다음 작업(Actions) 메뉴의 조직 단위(Organizational unit)에서 이름 바꾸기(Rename)를 선택합니다.
   - OU의 이름을 선택하여 OU의 세부 정보 페이지에 액세스합니다. 페이지 상단에서 이름 바꾸기(Rename)를 선택합니다.

3. 조직 단위 이름 바꾸기(Rename organizational unit) 대화 상자에서 새 이름을 입력하고 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

OU의 이름을 바꾸려면

다음 명령 중 하나를 사용하여 OU 이름 바꿀 수 있습니다.

- AWS CLI: update-organizational-unit

  다음 예제에서는 OU의 이름을 바꾸는 방법을 보여 줍니다.

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- AWS SDK: UpdateOrganizationalUnit

OU에 연결된 태그 편집

조직의 관리 계정으로 로그인하면 OU에 연결된 태그를 추가하거나 제거할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

> 최소 권한
>
> AWS 조직의 루트 내에 있는 OU에 첨부된 태그를 편집하려면 다음 권한이 있어야 합니다.
>
> - `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
> - `organizations:DescribeOrganizationalUnit` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

OU에 연결된 태그를 편집하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 태그를 편집하려는 OU로 이동하여 이름을 선택합니다.
3. OU의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 탭에서 다음과 같은 작업을 수행할 수 있습니다.
   - 이전 값 대신 새 값을 입력하여 태그의 값을 편집합니다. 태그 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
   - 제거하려는 태그 옆의 제거(Remove)를 선택하여 기존 태그를 제거합니다.
   - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 `null`이 아닌 빈 문자열이 됩니다.
5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

OU에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 OU에 연결된 태그를 변경할 수 있습니다.

- AWS CLI: tag-resource 및 untag-resource

  다음 예제에서는 `"Department"="12345"` 태그를 OU에 연결합니다. `Key`와 `Value`는 대소문자를 구분합니다.

```
$ aws organizations tag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tags Key=Department,Value=12345
```

이 명령은 성공 시 출력을 생성하지 않습니다.

다음 예제에서는 OU에서 Department를 제거합니다.

```
$ aws organizations untag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tag-keys Department
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: TagResource 및 UntagResource

계정을 OU로 이동하거나 루트와 OU 간에 이동

조직의 관리 계정에 로그인하면, 조직의 계정을 루트에서 OU로 이동하거나, 한 OU에서 다른 OU로 이동하거나, OU에서 다시 루트로 이동할 수 있습니다. OU 내에 계정을 배치하면 계정은 상위 OU 및 루트까지의 상위 체인에 속한 모든 OU에 연결된 정책을 적용받게 됩니다. 계정이 OU 안에 있지 않다면, 계정은 루트에 바로 연결된 정책과 계정에 바로 연결된 정책을 적용받게 됩니다. 계정을 이동하려면 다음 단계를 수행합니다.

> 최소 권한
>
> OU 계층 구조 내 새 위치로 계정을 이동하려면 다음과 같은 권한이 있어야 합니다.
>
> - organizations:DescribeOrganization – Organizations 콘솔을 사용하는 경우에만 필요합니다.
> - organizations:MoveAccount

AWS Management Console

계정을 OU로 이동하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 이동할 계정을 찾습니다. OU 계층 구조를 탐색하거나, AWS 계정 만 보기(View AWS 계정 only)를 활성화하여 OU 구조 없이 단순 계정 목록을 확인할 수 있습니다.

계정이 많은 경우 이동할 모든 항목을 찾기 위해 목록 하단에 있는 'ou-name'에서 추가 계정 로드(Load more accounts in 'ou-name')를 선택해야 할 수도 있습니다.

3. 이동할 각 계정의 이름 옆에 있는 확인란 ☑ 을 선택합니다.
4. 작업(Actions) 메뉴의 AWS 계정에서 이동(Move)을 선택합니다.
5. AWS 계정이동(Move AWS 계정) 대화 상자에서 계정을 옮길 OU나 루트를 선택한 다음 AWS 계정이동(Move AWS 계정)을 선택합니다.

AWS CLI & AWS SDKs

계정을 OU로 이동하려면

다음 명령 중 하나를 사용하여 계정을 이동할 수 있습니다.

- AWS CLI: move-account

  다음 예제는 AWS 계정 루트에서 OU로 를 이동합니다. 원본 컨테이너의 ID와 대상 컨테이너의 ID를 모두 지정해야 합니다.

```
$ aws organizations move-account \
    --account-id 111122223333 \
    --source-parent-id r-a1b2 \
    --destination-parent-id ou-a1b2-f6g7h111
```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDK: MoveAccount

OU 삭제

조직의 관리 계정에 로그인하면 더 이상 필요 없는 모든 OU를 삭제할 수 있습니다.

먼저 모든 계정을 해당 OU 및 모든 하위 OU 밖으로 옮긴 다음 하위 OU를 삭제해야 합니다.

> **최소 권한**
>
> OU를 삭제하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:DeleteOrganizationalUnit`

AWS Management Console

OU를 삭제하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. AWS 계정 페이지에서 삭제할 OU를 찾고 각 OU 이름 옆에 있는 확인란 ☑ 을 선택합니다.
3. 작업(Actions)을 선택한 다음 조직 단위(Organizational unit)에서 삭제(Delete)를 선택합니다.
4. OU 삭제를 확인하려면 OU의 이름(하나만 삭제하기로 선택한 경우) 또는 'delete'라는 단어(둘 이상을 선택한 경우)를 입력한 다음 삭제(Delete)를 선택합니다.

   AWS Organizations OU를 삭제하고 목록에서 제거합니다.

AWS CLI & AWS SDKs

OU를 삭제하는 방법

다음 명령 중 하나를 사용하여 OU를 삭제할 수 있습니다.

- AWS CLI: delete-organizational-unit

  다음 예제에서는 OU를 삭제하는 방법을 보여줍니다.

  ```
  $ aws organizations delete-organizational-unit \
      --organizational-unit-id ou-a1b2-f6g7h222
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS SDK: DeleteOrganizationalUnit

AWS Organizations 리소스에 태그 지정

태그는 리소스를 좀 더 쉽게 식별하고 구성하고 검색하기 위해 AWS 리소스에 추가하는 사용자 지정 속성 레이블입니다. 각 태그에는 다음 두 가지 부분이 있습니다.

- 태그 키(예: `CostCenter`, `Environment` 또는 `Project`) 태그 키는 최대 128자이며 대/소문자를 구분합니다.
- 태그 값(예: `111122223333` 또는 `Production`). 값은 최대 256자이며 태그 키와 같이 대/소문자를 구분합니다. 태그의 값을 빈 문자열로 설정할 수 있지만 태그의 값을 Null로 설정할 수는 없습니다. 태그 값을 생략하는 것은 빈 문자열을 사용하는 것과 같습니다.

태그 키 또는 값에 허용되는 문자에 대한 자세한 내용은 Resource Groups 태그 지정 API 참조에서 태그 API의 태그 파라미터를 참조하세요.

태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 자세한 내용은 AWS 리소스 태그 지정 모범 사례를 참조하십시오.

> **Tip**
>
> 태그 정책을 사용하면 조직의 계정에 있는 리소스 전반에서 태그를 표준화할 수 있습니다.

관리 계정으로 로그인할 때 현재 AWS Organizations에서 지원하는 태그 지정 작업은 다음과 같습니다.

- 태그를 추가할 수 있는 조직 리소스는 다음과 같습니다.
  - AWS 계정
  - 조직 단위
  - 조직의 루트
  - 정책

태그를 추가할 수 있는 시점은 다음과 같습니다.

- 리소스를 생성할 때 — Organizations 콘솔에서 태그를 지정하거나 `Create` API 작업 중 하나에 `Tags` 파라미터를 사용합니다. 이는 조직의 루트에 적용되지 않습니다.
- 리소스를 생성한 후 — Organizations 콘솔을 사용하거나 `TagResource` 작업을 호출합니다.

콘솔을 사용하거나 ListTagsForResource 작업을 호출하여 AWS Organizations에서 태그 지정이 가능한 모든 리소스에 대한 태그를 볼 수 있습니다.

콘솔을 사용하거나 UntagResource 작업을 호출하여 제거할 키를 지정하면 리소스에서 태그를 제거할 수 있습니다.

태그 사용

태그를 사용하면 유용한 범주별로 항목을 그룹화할 수 있어서 조직의 리소스를 구성하는 데 도움이 됩니다. 예를 들어 담당 부서를 추적하는 “부서(Department)” 태그를 할당할 수 있습니다. “환경(Environment)” 태그를 할당하면 주어진 리소스가 알파, 베타, 감마 또는 프로덕션 환경에 속하는지 추적할 수 있습니다.

태그를 사용하여 다음을 수행할 수도 있습니다.

- 리소스에 태깅 표준을 적용하세요.
- 리소스에 액세스할 수 있는 제어.

태그 추가, 업데이트 및 제거

조직의 관리 계정에 로그인하면 조직의 리소스에 태그를 추가할 수 있습니다.

리소스를 생성할 때 리소스에 태그 추가

> 최소 권한
>
> 리소스를 생성할 때 태그를 추가하려면 다음 권한이 필요합니다.
>
> - 지정된 유형의 리소스를 생성할 수 있는 권한
> - `organizations:TagResource`
> - `organizations:ListTagsForResource` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

다음 리소스를 생성할 때 리스소에 연결되는 태그 키와 값을 포함할 수 있습니다.

- AWS 계정
  - 생성된 계정

  - 초대된 계정
- 조직 단위(OU)
- 정책
  - AI 서비스 옵트아웃 정책
  - 백업 정책
  - 서비스 제어 정책
  - 태그 정책

조직 루트는 조직을 처음 만들 때 생성되므로 기존 리소스로만 태그를 추가할 수 있습니다.

기존 리소스에 대한 태그 추가 또는 업데이트

새 태그를 추가하거나 기존 리소스에 연결된 태그의 값을 업데이트할 수도 있습니다.

> 최소 권한
>
> 조직의 리소스에 태그를 추가하거나 업데이트하려면 다음 권한이 필요합니다.
>
> - `organizations:TagResource`
> - `organizations:ListTagsForResource` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
>
> 조직의 리소스에서 태그를 제거하려면 다음 권한이 필요합니다.
>
> - `organizations:UntagResource`

AWS Management Console

기존 리소스에 대한 태그를 추가, 업데이트 또는 제거하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 계정, 루트, OU 또는 정책을 탐색하여 선택하고 이름을 클릭해 세부 정보 페이지를 엽니다.
3. 태그 탭에서 태그 관리를 선택합니다.
4. 새 태그를 추가하거나, 기존 태그의 값을 수정하거나, 태그를 제거할 수 있습니다.

태그를 추가하려면 태그 추가(Add tag)를 선택한 다음 해당 태그에 대한 키와 값을 입력합니다. 값은 선택 사항입니다.

태그를 제거하려면 제거(Remove)를 선택합니다.

태그 키와 값은 대소문자를 구분합니다. 표준화하려는 대문자를 사용합니다. 또한 적용되는 태그 정책의 요구 사항을 준수해야 합니다.

5. 필요한 만큼 이전 단계를 반복합니다.
6. 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

태그를 업데이트하거나 기존 리소스에 추가하려면

다음 명령 중 하나를 사용하여 조직의 태그 지정 가능 리소스에 태그를 추가할 수 있습니다.

- AWS CLI: tag-resource
- AWSSDK: TagResource

조직의 리소스에서 태그를 삭제하려면

다음 명령 중 하나를 사용하여 태그를 삭제할 수 있습니다.

- AWS CLI: untag-resource
- AWSSDK: UntagResource

다른 AWS 서비스와 함께 AWS Organizations 사용

신뢰할 수 있는 액세스를 사용하여 사용자가 지정한 지원되는 AWS 서비스를 활성화할 수 있습니다. 이러한 서비스를 신뢰할 수 있는 서비스라 하며, 사용자를 대신해 조직과 그 계정의 작업을 수행합니다. 이 과정에는 신뢰할 수 있는 서비스에 대한 권한 부여가 포함되지만 사용자 또는 역할에 대한 권한에는 달리 영향을 미치지 않습니다. 액세스를 활성화하면 신뢰할 수 있는 서비스는 필요할 때 언제든 조직의 모든 계정에서 서비스 연결 역할(service-linked role)이라는 IAM 역할을 생성할 수 있습니다. 이 역할에는 신뢰할 수 있는 서비스가 해당 서비스의 설명서에 명시된 작업을 수행할 수 있도록 활성화하는 권한 정책이 있습니다. 따라서 신뢰할 수 있는 서비스가 사용자를 대신하여 사용자의 조직 계정으로 관리할 설정 및 구성 세부 정보를 지정할 수 있습니다. 신뢰할 수 있는 서비스는 조직의 모든 계정이 아니라 계정에 대한 관리 작업을 수행해야 하는 경우에만 서비스 연결 역할을 생성합니다.

Important

옵션이 제공되는 경우, 신뢰할 수 있는 액세스의 활성화 및 비활성화에는 신뢰할 수 있는 서비스의 콘솔이나, 그 AWS CLI 또는 API 작업만을 사용할 것을 적극 권장합니다. 이렇게 하면 신뢰할 수 있는 액세스를 활성화할 때 신뢰할 수 있는 서비스가 모든 필수 리소스를 생성하는 등의 필요한 모든 초기화를 수행할 수 있으며, 신뢰할 수 있는 서비스를 비활성화할 때 필요한 모든 리소스 정리 작업을 수행할 수 있습니다.

신뢰할 수 있는 서비스를 사용해 조직에 대한 신뢰할 수 있는 서비스 액세스를 활성화하거나 비활성화하는 방법은 AWS 함께 사용할 수 있는 서비스 AWS Organizations의 신뢰할 수 있는 액세스 지원 열 아래에 있는 자세히 알아보기를 참조하세요.

Organizations 콘솔, CLI 명령 또는 API 작업을 사용하여 액세스를 비활성화하면 다음의 동작이 발생합니다.

- 조직 내 계정에서 더 이상 서비스 연결 역할을 만들 수 없습니다. 즉, 서비스가 사용자를 대신하여 조직의 새 계정에 대해 작업을 수행할 수 없습니다. 서비스는 서비스가 AWS Organizations의 정리를 완료할 때까지 이전 계정에서 작업을 계속 수행할 수 있습니다.
- 역할에 연결된 IAM 정책에서 작업을 명시적으로 허용하지 않는 한 서비스가 더 이상 조직의 멤버 계정에서 작업을 수행할 수 없습니다. 이러한 작업으로는 멤버 계정에서부터 관리 계정 또는 위임된 관리자 계정(해당하는 경우)에 이르는 모든 데이터의 집계가 있습니다.
- 일부 서비스는 이를 감지하고 통합과 관련된 나머지 데이터 또는 리소스를 정리하는 반면, 다른 서비스는 조직에 대한 액세스를 중지하되 통합의 재활성화를 지원하기 위해 기록 데이터 및 구성을 그대로 남겨둡니다.

그 대신 다른 서비스의 콘솔이나 명령을 사용하여 통합을 비활성화하면 다른 서비스가 통합에 만 필요한 리소스를 정리할 수 있습니다. 서비스가 조직의 계정에서 리소스를 정리하는 방식은 해당 서비스에 따라 다릅니다. 자세한 내용은 다른 AWS 서비스의 설명서를 참조하세요.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한

신뢰할 수 있는 액세스의 경우 두 서비스인 AWS Organizations 및 신뢰할 수 있는 서비스에 대한 권한이 필요합니다. 신뢰할 수 있는 액세스를 활성화하려면 다음 시나리오 중 하나를 선택합니다.

- AWS Organizations 및 신뢰할 수 있는 서비스 모두에 대한 권한을 가진 자격 증명이 있으면, 신뢰할 수 있는 서비스에서 제공하는 도구(콘솔 또는 AWS CLI)를 사용하여 액세스를 활성화합니다. 이렇게 하면 서비스가 사용자를 대신해 AWS Organizations에서 신뢰할 수 있는 액세스를 활성화하고 해당 서비스가 사용자의 조직에서 작동하는 데 필요한 리소스를 생성할 수 있습니다.

  이러한 자격 증명에 필요한 최소 권한은 다음과 같습니다.

  - `organizations:EnableAWSServiceAccess`. 이 작업에 `organizations:ServicePrincipal` 조건 키를 사용하여 승인된 서비스 보안 주체 이름의 목록에 대해 해당 작업이 수행하는 요청을 제한할 수 있습니다. 자세한 정보는 조건 키을 참조하세요.
  - `organizations:ListAWSServiceAccessForOrganization` – AWS Organizations 콘솔을 사용하는 경우에 필요합니다.
  - 신뢰할 수 있는 서비스에서 필요한 최소 권한은 서비스에 따라 결정됩니다. 자세한 내용은 신뢰할 수 있는 서비스의 설명서를 참조하세요.
- 한 사람에게는 AWS Organizations의 권한이 있는 자격 증명이 있고, 다른 사람에게는 신뢰할 수 있는 서비스의 권한이 있는 자격 증명이 있는 경우에는 다음 단계를 다음 순서대로 수행합니다.

  1. AWS Organizations의 권한 자격 증명이 있는 사람은 AWS Organizations 콘솔, AWS CLI 또는 AWS SDK를 사용하여 신뢰할 수 있는 서비스에 대한 신뢰할 수 있는 액세스를 활성화해야 합니다. 이렇게 하면 다음 단계(2단계)를 수행할 때 다른 서비스가 조직에서 필요한 권한을 수행할 수 있는 권한이 부여됩니다.

     최소 AWS Organizations 권한은 다음과 같습니다.

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – AWS Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Organizations에서 신뢰할 수 있는 액세스를 활성화하는 구체적인 단계는 신뢰할 수 있는 액세스를 활성화 또는 비활성화하는 방법을 참조하세요.

2. 신뢰할 수 있는 서비스의 권한이 있는 자격 증명이 있는 사람이 해당 서비스를 AWS Organizations로 작업할 수 있도록 합니다. 이것은 해당 서비스에게 신뢰할 수 있는 서비스가 조직에서 작업하는 데 필요한 리소스 생성 같은 필요한 초기화를 수행하도록 지시하는 것입니다. 자세한 내용은 AWS 함께 사용할 수 있는 서비스 AWS Organizations에서 서비스별 지침을 참조하세요.

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한

신뢰할 수 있는 서비스가 사용자의 조직이나 그 계정으로 작업하는 것을 중단하려면 다음 시나리오 중 하나를 선택하세요.

> **Important**
>
> 신뢰할 수 있는 서비스 액세스를 비활성화한다고 해서 해당 권한이 있는 사용자와 역할이 해당 서비스를 사용하지 못하게 되는 것은 아닙니다. 사용자 및 역할이 AWS 서비스에 액세스하지 못하도록 완전히 차단하려면 해당 액세스 권한을 부여하는 IAM 권한을 제거하거나 AWS Organizations에서 서비스 제어 정책(SCP)을 사용할 수 있습니다.
> SCP는 멤버 계정에만 적용할 수 있습니다. 관리 계정에는 SCP가 적용되지 않습니다. 관리 계정에서 서비스를 실행하지 않는 것이 좋습니다. 그 대신 SCP를 사용하여 보안을 제어할 수 있는 멤버 계정에서 서비스를 실행합니다.

- AWS Organizations 및 신뢰할 수 있는 서비스 모두에 대한 권한을 가진 자격 증명이 있으면, 신뢰할 수 있는 서비스에 사용할 수 있는 도구(콘솔 또는 AWS CLI)를 사용하여 액세스를 비활성화합니다. 그러면 해당 서비스가 더 이상 필요하지 않는 리소스를 제거하고 사용자 대신 AWS Organizations에서 서비스에 대한 신뢰할 수 있는 액세스를 비활성화하여 정리됩니다.

  이러한 자격 증명에 필요한 최소 권한은 다음과 같습니다.

  - `organizations:DisableAWSServiceAccess`. 이 작업에 `organizations:ServicePrincipal` 조건 키를 사용하여 승인된 서비스 보안 주체 이름의 목록에 대해 해당 작업이 수행하는 요청을 제한할 수 있습니다. 자세한 정보는 조건 키을 참조하세요.
  - `organizations:ListAWSServiceAccessForOrganization` – AWS Organizations 콘솔을 사용하는 경우에 필요합니다.

  - 신뢰할 수 있는 서비스에서 필요한 최소 권한은 서비스에 따라 결정됩니다. 자세한 내용은 신뢰할 수 있는 서비스의 설명서를 참조하세요.
- AWS Organizations의 권한이 있는 자격 증명이 신뢰할 수 있는 서비스의 권한이 있는 자격 증명이 아닌 경우에는 다음 단계를 다음 순서대로 수행합니다.
  1. 먼저 신뢰할 수 있는 서비스에 대한 권한이 있는 사람이 해당 서비스를 사용하여 액세스를 비활성화합니다. 이것은 신뢰할 수 있는 서비스에게 신뢰할 수 있는 액세스에 필요한 리소스를 삭제하여 정리하라고 지시하는 것입니다. 자세한 내용은 AWS 함께 사용할 수 있는 서비스 AWS Organizations에서 서비스별 지침을 참조하세요.
  2. 그런 다음 AWS Organizations의 권한이 있는 사람이 AWS Organizations 콘솔, AWS CLI 또는 AWS SDK를 사용하여 신뢰할 수 있는 서비스에 대한 액세스를 비활성화할 수 있습니다. 이제 신뢰할 수 있는 서비스에 대한 권한이 조직과 그 계정에서 삭제됩니다.

     최소 AWS Organizations 권한은 다음과 같습니다.

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – AWS Organizations 콘솔을 사용하는 경우에만 필요합니다.

     AWS Organizations의 신뢰할 수 있는 액세스를 비활성화하는 구체적인 단계는 신뢰할 수 있는 액세스를 활성화 또는 비활성화하는 방법을 참조하세요.

신뢰할 수 있는 액세스를 활성화 또는 비활성화하는 방법

AWS Organizations에 대한 권한만 있고, 다른 AWS 서비스의 관리자를 대신하여 사용자의 조직에 대한 신뢰할 수 있는 액세스를 활성화 또는 비활성화하려면 다음 절차를 사용하세요.

> **Important**
>
> 옵션이 제공되는 경우, 신뢰할 수 있는 액세스의 활성화 및 비활성화에는 신뢰할 수 있는 서비스의 콘솔이나, 그 AWS CLI 또는 API 작업만을 사용할 것을 적극 권장합니다. 이렇게 하면 신뢰할 수 있는 액세스를 활성화할 때 신뢰할 수 있는 서비스가 모든 필수 리소스를 생성하는 등의 필요한 모든 초기화를 수행할 수 있으며, 신뢰할 수 있는 서비스를 비활성화할 때 필요한 모든 리소스 정리 작업을 수행할 수 있습니다.
> 신뢰할 수 있는 서비스를 사용해 조직에 대한 신뢰할 수 있는 서비스 액세스를 활성화하거나 비활성화하는 방법은 AWS 함께 사용할 수 있는 서비스 AWS Organizations의 신뢰할 수 있는 액세스 지원 열 아래에 있는 자세히 알아보기를 참조하세요.

Organizations 콘솔, CLI 명령 또는 API 작업을 사용하여 액세스를 비활성화하면 다음의 동작이 발생합니다.

- 조직 내 계정에서 더 이상 서비스 연결 역할을 만들 수 없습니다. 즉, 서비스가 사용자를 대신하여 조직의 새 계정에 대해 작업을 수행할 수 없습니다. 서비스는 서비스가 AWS Organizations의 정리를 완료할 때까지 이전 계정에서 작업을 계속 수행할 수 있습니다.
- 역할에 연결된 IAM 정책에서 작업을 명시적으로 허용하지 않는 한 서비스가 더 이상 조직의 멤버 계정에서 작업을 수행할 수 없습니다. 이러한 작업으로는 멤버 계정에서부터 관리 계정 또는 위임된 관리자 계정(해당하는 경우)에 이르는 모든 데이터의 집계가 있습니다.
- 일부 서비스는 이를 감지하고 통합과 관련된 나머지 데이터 또는 리소스를 정리하는 반면, 다른 서비스는 조직에 대한 액세스를 중지하되 통합의 재활성화를 지원하기 위해 기록 데이터 및 구성을 그대로 남겨둡니다.

그 대신 다른 서비스의 콘솔이나 명령을 사용하여 통합을 비활성화하면 다른 서비스가 통합에만 필요한 리소스를 정리할 수 있습니다. 서비스가 조직의 계정에서 리소스를 정리하는 방식은 해당 서비스에 따라 다릅니다. 자세한 내용은 다른 AWS 서비스의 설명서를 참조하세요.

AWS Management Console

신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 활성화하려는 서비스의 행을 찾고 그 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 활성화를 선택합니다.
4. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화는 옵션 표시(Show the option to enable trusted access)를 선택하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
5. 액세스를 활성화하는 경우에는 다른 AWS 서비스 관리자에게 이제 다른 서비스를 AWS Organizations로 작업할 수 있다고 알려줍니다.

신뢰할 수 있는 서비스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. 서비스(Services) 페이지에서 비활성화하려는 서비스의 행을 찾고 그 이름을 선택합니다.
3. 다른 서비스의 관리자가, 서비스가 비활성화되어 해당 리소스가 정리되었다고 알려줄 때까지 기다립니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.

AWS CLI, AWS API

신뢰할 수 있는 서비스 액세스를 활성화 또는 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하거나 비활성화할 수 있습니다.

- AWS CLI: AWS organizations enable-aws-service-access
- AWS CLI: AWS organizations disable-aws-service-access
- AWS API: EnableAWSServiceAccess
- AWS API: DisableAWSServiceAccess

AWS Organizations 및 서비스 연결 역할

AWS Organizations는 IAM 서비스 연결 역할을 사용하여 신뢰할 수 있는 서비스가 조직의 멤버 계정에서 사용자를 대신하여 작업을 수행할 수 있도록 합니다. 신뢰할 수 있는 서비스를 구성하고 이를 조직에 통합하도록 승인하면 이 서비스에서 AWS Organizations가 해당 멤버 계정으로 서비스 연결 역할을 생성하도록 요청할 수 있습니다. 신뢰할 수 있는 서비스가 동시에 조직 내 모든 계정에 필수적으로 진행하지 않고 필요할 때 이를 비동기적으로 진행합니다. 서비스 연결 역할에는 신뢰할 수 있는 서비스가 해당 계정 내에서 특정 작업만을 수행하도록 허용하는 사전 정의된 IAM 권한이 있습니다. 일반적으로 AWS에서 모든 서비스 연결 역할을 관리합니다. 따라서 사용자는 일반적으로 역할 또는 연결된 정책을 변경할 수 없습니다.

이 모든 것이 가능하도록 하려면 조직 내에 계정을 생성하거나 조직에 대한 기존 계정의 초대를 허용할 때 AWS Organizations가 멤버 계정에 `AWSServiceRoleForOrganizations`라는 서비스 연결 역할을 프로비저닝합니다. AWS Organizations 서비스 자체만이 이 역할을 맡을 수 있습니다. 이 역할은 AWS Organizations가 다른 AWS 서비스에 대한 서비스 연결 역할을 생성할 수 있도록 허용하는 권한을 보유합니다. 이 서비스 연결 역할은 모든 조직에 존재합니다.

권장하는 방법은 아니지만 조직에서 통합 결제 기능만 활성화된 경우, `AWSServiceRoleForOrganizations`라는 이름의 서비스 연결 역할이 절대 사용되지 않으며, 이를

삭제할 수 있습니다. 이후에 조직 내 모든 기능을 활성화려면 이 역할이 필요하므로, 복원해야 합니다. 다음 상태 확인은 모든 기능을 활성화하는 절차를 시작할 때 발생합니다.

- 조직에 가입하도록 초대된 각 멤버 계정 – 계정 관리자가 모든 기능 활성화에 동의하는 요청을 수신합니다. 요청에 동의하려면 관리자가 `organizations:AcceptHandshake` 권한과 `iam:CreateServiceLinkedRole` 권한(서비스 연결 역할(`AWSServiceRoleForOrganizations`)이 아직 없는 경우)이 모두 있어야 합니다. `AWSServiceRoleForOrganizations` 역할이 이미 존재하는 경우 관리자는 요청 허용에 `organizations:AcceptHandshake` 권한만이 필요합니다. 관리자가 요청에 동의하면 AWS Organizations는 서비스 연결 역할을 생성합니다(아직 없는 경우).
- 조직에 생성된 각 멤버 계정 – 계정 관리자가 서비스 연결 역할을 다시 생성하는 요청을 수신합니다. (멤버 계정의 관리자는 모든 기능을 활성화하는 요청을 수신하지 않습니다. 관리 계정(이전의 "마스터 계정")의 관리자가 생성된 멤버 계정의 소유자로 간주되기 때문입니다.) 멤버 계정 관리자가 요청을 허용할 때 AWS Organizations는 서비스 연결 역할을 생성합니다. 성공적으로 핸드셰이크를 수락하려면 관리자는 `organizations:AcceptHandshake` 및 `iam:CreateServiceLinkedRole` 권한을 보유해야 합니다.

조직에서 모든 기능을 활성화한 이후에는 더 이상 모든 계정에서 `AWSServiceRoleForOrganizations` 서비스 연결 역할을 삭제할 수 없습니다.

> **Important**
>
> AWS Organizations SCP는 서비스 연결 역할에 절대 영향을 주지 않습니다. 이러한 역할은 모든 SCP 제한에서 제외됩니다.

AWS 함께 사용할 수 있는 서비스 AWS Organizations

AWS Organizations 를 사용하면 여러 조직을 단일 AWS 계정 조직으로 통합하여 대규모로 계정 관리 활동을 수행할 수 있습니다. 계정을 통합하면 다른 서비스를 사용하는 방법이 단순해집니다. AWS 일부 AWS 서비스에서 제공되는 다중 계정 관리 서비스를 활용하여 AWS Organizations 조직 구성원의 모든 계정에 대한 작업을 수행할 수 있습니다.

다음 표에는 함께 AWS Organizations사용할 수 있는 AWS 서비스와 조직 차원에서 각 서비스를 사용할 때 얻을 수 있는 이점이 나열되어 있습니다.

신뢰할 수 있는 액세스 — 호환되는 AWS 서비스를 사용하여 조직 AWS 계정 내 모든 영역에서 작업을 수행할 수 있습니다. 자세한 정보는 다른 AWS 서비스와 함께 AWS Organizations 사용을 참조하세요.

AWS 서비스에 대한 위임 관리자 — 호환되는 AWS 서비스는 조직의 AWS 구성원 계정을 해당 서비스의 조직 계정에 대한 관리자로 등록할 수 있습니다. 자세한 정보는 Organizations과 연동되는 AWS 서비스의 위임된 관리자을 참조하세요.

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Account Management 조직의 모든 세부 정보 및 메타데이터를 관리하세요. AWS 계정	조직의 모든 계정에 대한 대체 연락처 정보를 생성, 업데이트 및 삭제할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	
AWS Application Migration Service AWS Application Migration Service 기업은 호환성 문제, 성능 저하 또는 긴 컷오버 기간 없이 많은 수의 물리적, 가상 또는 클라우드 서버를 사용할 수 있습니다. lift-and-shift AWS	여러 계정에 대해 대규모 마이그레이션을 관리할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Artifact ISO 및 PCI 보고서와 같은 AWS 보안 규정 준수 보고서를 다운로드하십시오.	조직 내 모든 계정을 대신하여 계약을 수락할 수 있습니다.	 예 자세히 알아보기	 아니요	
AWS Audit Manager 지속적인 증거 수집을 자동화하여 클라우드 서비스 사용을 감사할 수 있습니다.	조직의 여러 계정에 대한 AWS 사용 현황을 지속적으로 감사하여 위험 및 규정 준수를 평가하는 방법을 간소화하세요.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Backup 조직의 모든 계정에서 백업을 관리하고 모니터링합니다.	전체 조직 또는 OU(조직 단위)의 계정 그룹에 대한 백업 계획을 구성하고 관리할 수 있습니다. 모든 계정의 백업을 중앙에서 모니터링할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Billing and Cost Management AWS 클라우드 재무 관리 데이터에 대한 개요를 제공하고 정보에 입각한 결정을 더 빠르고 정확하게 내리는 데 도움이 됩니다.	해당하는 경우 분할 비용 할당 데이터를 통해 AWS Organizations 정보를 검색하고, 선택한 분할 비용 할당 데이터 서비스에 대한 원격 측정 데이터를 수집할 수 있습니다. 자세한 내용은 무엇입니까를 참조하십시오. AWS Billing and Cost ManagementBilling and Cost Management	 예 자세히 알아보기	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
	t 사용 설명서에서 확인할 수 있습니다.			
AWS CloudFormation StackSets 단일 작업으로 여러 계정 및 리전에 대해 스택을 생성, 업데이트 또는 삭제합니다.	관리 계정 또는 위임된 관리자 계정의 사용자는 서비스 관리형 권한을 사용하여 조직의 계정에 스택 인스턴스를 배포하는 스택 세트를 생성할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS CloudTrail 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화합니다.	관리 계정 또는 위임된 관리자 계정의 사용자는 조직의 모든 계정에 대한 모든 이벤트를 로깅하는 조직 추적 또는 이벤트 데이터 스토어를 생성할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Compute Optimizer AWS 컴퓨팅 최적화 권장 사항을 확인하세요.	조직의 계정에 있는 모든 리소스를 분석하여 최적화 권장 사항을 얻을 수 있습니다. 자세한 내용은 AWS Compute Optimizer 사용 설명서의 Compute Optimizer에서 지원하는 계정을 참조하세요.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Config AWS 리소스의 구성을 액세스, 감사 및 평가합니다.	규정 준수 상태를 조직 전체 수준에서 확인할 수 있습니다. 또한 AWS Config API 작업을 사용하여 조직 내 모든 AWS Config AWS 계정 규칙과 규정 준수 팩을 관리할 수 있습니다. 위임된 관리자 계정을 사용하여 AWS Organizations에서 조직 내 모든 멤버 계정의 리소스 구성 및	 예 자세히 알아보기	 예 자세히 알아보기: Config 규칙 적합성 팩 다중 계정 다중 리전 데이터 집계	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
	규정 준수 데이터를 집계할 수 있습니다. 자세한 내용은 AWS Config 개발자 안내서의 위임된 관리자 등록을 참조하세요.			

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Control Tower 안전하고 규정을 준수하는 다중 계정 AWS 환경을 설정하고 관리합니다.	모든 AWS 리소스를 위한 다중 계정 환경인 landing Zone을 설정할 수 있습니다. 이 환경에는 조직과 조직 엔터티가 포함됩니다. 이 환경을 사용하여 모든 계정에 규정 준수 규정을 적용할 수 있습니다. AWS 계정 자세한 내용은 AWS Control Tower 사용 설명서의 AWS Control Tower의	 예 자세히 알아보기	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
	작동 방식 및 AWS Organizations를 통한 계정 관리를 참조하세요.			

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Cost Optimization Hub AWS 최적화 제품 전반에 대한 비용 권장 사항을 수집하세요.	AWS Organizations 회원 계정 및 AWS 지역 전반에서 AWS 비용 최적화 권장 사항을 쉽게 식별, 필터링 및 집계할 수 있습니다. 자세한 내용은 비용 최적화 허브 사용 안내서의 비용 최적화 허브를 참조하십시오.	 예 자세히 알아보기	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
Amazon Detective 로그 데이터에서 보안 결과 또는 의심스러운 활동의 근본 원인을 분석하고, 조사하고, 빠르게 식별하기 위한 시각화를 생성합니다.	Amazon Detective와 AWS Organizations 통합하여 Detective 행동 그래프가 모든 조직 계정의 활동에 대한 가시성을 제공하도록 할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
아마존 DevOps 전문가 운영 데이터와 애플리케이션 지표 및 이벤트를 분석하여 정상적인 운영 패턴에서 벗어나는 동작을 식별합니다. DevOpsGuru가 운영 문제 또는 위험을 감지하면 사용자에게 알림이 전송됩니다.	와 AWS Organizations 통합하여 조직 전체의 모든 계정에서 얻은 통찰력을 관리할 수 있습니다. 관리자가 모든 계정의 인사이트를 보고, 정렬하고, 필터링하여 조직 전체 수준에서 모니터링되는 모든 애플리케이션의 상태를 확인할 수 있도록 권한을 위임합니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Directory Service AWS 클라우드에서 디렉터리를 설정 및 실행하거나 AWS 리소스를 기존 온-프레미스 Microsoft Active Directory에 연결합니다.	AWS Directory Service와 AWS Organizations 통합하여 여러 계정 및 지역 내 모든 VPC 간에 원활한 디렉터리 공유를 수행할 수 있습니다.	 예 자세히 알아보기	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
아마존 EventBridge 실행 중인 AWS 리소스와 애플리케이션을 AWS 실시간으로 모니터링하십시오.	조직의 모든 계정에서 모든 Amazon EventBridge 이벤트(이전의 Amazon CloudWatch Events)를 공유하도록 활성화할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 이벤트 전송 AWS 계정 및 수신을 참조하십시오.	 아니요	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Firewall Manager 사용자의 계정과 애플리케이션 전체에서 웹 애플리케이션에 대한 방화벽 규칙을 중앙에서 구성하고 관리합니다.	조직 내 계정 전체의 AWS WAF 규칙을 중앙에서 구성하고 관리할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
아마존 GuardDuty GuardDuty 다양한 데이터 소스의 정보를 분석하고 처리하는 지속적인 보안 모니터링 서비스입니다. 위협 인텔리전스 피드와 기계 학습을 바탕으로 Machine Learning을 적용하여 AWS 환경에서 예기치 않게 발생하는 잠재적 무단 활동과 악의적 활동을 찾아냅니다.	조직의 모든 계정을 보고 관리할 GuardDuty 구성원 계정을 지정할 수 있습니다. 구성원 계정을 추가하면 선택한 GuardDuty AWS 리전 계정의 해당 계정이 자동으로 활성화됩니다. 조직에 추가된 새 계정의 GuardDuty 활성화를 자동화할 수도 있습니다. 자세한 내용은 Amazon	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
	GuardDuty 사용 설명서의 Organizations를 참조하십시오GuardDuty .			
AWS Health 리소스 성능 또는 AWS 서비스 가용성 문제에 영향을 미칠 수 있는 이벤트를 파악할 수 있습니다.	조직 내 계정 전체의 AWS Health 이벤트를 집계할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Identity and Access Management AWS 리소스에 대한 액세스를 안전하게 제어하세요.	IAM에서 서비스가 마지막으로 액세스한 데이터를 사용하여 조직 전반의 AWS 활동을 더욱 잘 파악할 수 있습니다. 이 데이터를 사용하여 해당 조직의 계정이 사용하는 AWS 서비스로만 액세스를 제한하는 서비스 제어 정책(SCP)을 생성하고 업데이트할 수 있습니다.	 아니요	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
	예시는 IAM 사용 설명서의 데이터를 사용하여 조직 단위의 권한 구체화를 참조하세요.			
IAM 액세스 분석기 AWS 환경의 리소스 기반 정책을 분석하여 신뢰 영역 외부의 보안 주체에게 액세스 권한을 부여하는 정책을 식별하십시오.	멤버 계정을 IAM 액세스 분석기의 관리자로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 Access Analyzer 활성화를 참조하세요.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
Amazon Inspector AWS 워크로드에 취약성이 있는지 자동으로 스캔하여 Amazon ECR에 있는 Amazon EC2 인스턴스 및 컨테이너 이미지를 발견하여 소프트웨어 취약성 및 의도하지 않은 네트워크 노출을 찾아냅니다.	관리자에게 멤버 계정의 스캔을 활성화하거나 비활성화하고, 전체 조직에서 집계된 결과 데이터를 보고, 억제 규칙을 생성하고 관리할 수 있는 권한을 위임합니다. 자세한 내용은 Amazon Inspector 사용 설명서의 AWS Organizations로 여러 계정 관리를 참조하세요.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS License Manager 소프트웨어 라이선스를 클라우드로 가져오는 프로세스를 간소화합니다.	조직 전체의 컴퓨팅 리소스에 대한 교차 계정 발견을 활성화할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
Amazon Macie 데이터 보안 및 개인 정보 보호 요구 사항을 충족할 수 있도록 기계 학습을 사용하여 비즈니스 크리티컬 콘텐츠를 검색 및 분류합니다. Amazon S3에 저장된 콘텐츠를 지속적으로 평가하고 잠재적인 문제를 알려줍니다.	조직의 모든 계정에 대해 Amazon Macie를 구성하여 지정된 Macie 관리자 계정의 모든 계정에 대한 모든 데이터의 통합 보기를 Amazon S3로 가져올 수 있습니다. 조직이 성장함에 따라 새 계정의 리소스를 자동으로 보호하도록 Macie를 구성할 수 있습니다. 조직 전체의 S3 버	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
	킷에서 잘못된 정책 구성을 수정하면 경고가 표시됩니다.			
AWS Marketplace 솔루션을 구축하고 비즈니스를 운영하는 데 필요한 타사 소프트웨어, 데이터, 서비스를 찾아 구매, 배포 및 관리까지 할 수 있도록 큐레이션 프로세스를 거친 디지털 카탈로그입니다.	AWS Marketplace 구독 및 구매에 대한 라이선스를 조직의 여러 계정에서 공유할 수 있습니다.	 예 자세히 알아보기	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Marketplace 프라이빗 마켓플레이스 에서 AWS Marketplace사용할 수 있는 광범위한 제품 카탈로그와 해당 제품에 대한 세밀한 관리를 제공합니다.	조직 전체, 하나 이상의 OU 또는 조직 내 하나 이상의 계정과 관련된 여러 개의 비공개 마켓플레이스 경험을 만들 수 있으며 각 계정에는 승인된 제품 세트가 있습니다. 또한 AWS 관리자는 회사 또는 팀의 로고, 메시지 및 색 구성표를 사용하여 각 비공개 마켓플레이스 환경에 회사 브랜딩을 적	예 자세히 알아보기	예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
	용할 수 있습니다.			
AWS Network Manager AWS 계정, 지역 및 온프레미스 위치에서 AWS Cloud WAN 코어 네트워크와 AWS Transit Gateway 네트워크를 중앙에서 관리할 수 있습니다.	조직 내 여러 AWS 계정의 트랜짓 게이트웨이 및 연결된 리소스를 사용하여 글로벌 네트워크를 중앙에서 관리하고 모니터링할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
Amazon Q 개발자 Amazon Q Developer는 애플리케이션을 이해, 구축, 확장 및 운영하는 데 도움이 되는 생성적 인공 지능 (AI) 기반 대화형 도우미입니다. AWS	Amazon Q Developer의 유료 구독 버전에는 조직 통합이 필요합니다.	 예 자세히 알아보기	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Resource Access Manager 소유하고 있는 특정 AWS 리소스를 다른 계정과 공유하십시오.	추가 초대를 교환하지 않고도 조직 내에서 리소스를 공유할 수 있습니다. 공유할 수 있는 리소스에는 Route 53 Resolver 규칙, 온디맨드 용량 예약 등이 포함됩니다. 용량 예약 공유에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서 또는 Windows 인스턴	 예 자세히 알아보기	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
	스용 Amazon EC2 사용 설명서를 참조하세요. 공유 가능한 리소스 목록은 AWS RAM 사용 설명서의 공유 가능한 리소스를 참조하세요.			
AWS 리소스 탐색기 인터넷 검색 엔진과 같은 경험을 사용하여 리소스를 탐색하세요.	다중 계정 검색을 활성화하십시오.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Security Hub 에서 보안 상태를 확인하고 보안 업계 표준 AWS 및 모범 사례와 비교하여 환경을 확인하십시오.	추가된 새 계정을 포함하여 조직의 모든 계정에 대해 Security Hub를 자동으로 활성화하도록 설정할 수 있습니다. 이렇게 하면 Security Hub 검사 및 결과의 적용 범위가 늘어나 전반적인 보안 상태를 보다 정확하게 파악할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
Amazon S3 스토리지 렌즈 Amazon S3 Storage 사용량과 활동 지표에 대한 가시성과, 스토리지 최적화를 위한 실효성 있는 권장 사항을 제공합니다.	Amazon S3 스토리지 사용량 및 활동 추세에 대한 가시성과, 조직의 모든 멤버 계정에 대한 권장 사항을 얻을 수 있도록 Amazon S3 Storage Lens를 구성합니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
Amazon Security Lake Amazon Security Lake는 클라우드, 온프레미스 및 사용자 지정 소스의 보안 데이터를 계정에 저장된 데이터 레이크로 중앙 집중화합니다.	계정 전체에서 로그와 이벤트를 수집하는 데이터 레이크를 생성합니다.	 예 자세히 알아보기	 예 자세히 알아보기	
AWS Service Catalog AWS에서 사용하도록 승인된 IT 서비스의 카탈로그를 생성하고 관리합니다.	포트폴리오 ID를 공유하지 않고도 여러 계정에서 더 쉽게 포트폴리오를 공유하고 제품을 복사할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
Service Quotas 중앙 위치에서 서비스 할당량(또는 한도)을 확인하고 관리합니다.	조직의 계정을 만들 때 할당량 요청 템플릿을 만들어 할당량 증가를 자동으로 요청할 수 있습니다.	 예 자세히 알아보기	 아니요	
AWS IAM Identity Center 모든 계정 및 클라우드 애플리케이션에 대한 SSO(Single Sign-On) 액세스를 제공합니다.	사용자는 회사 자격 증명을 사용하여 AWS 액세스 포털에 로그인하고 할당된 관리 계정 또는 회원 계정의 리소스에 액세스할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Systems Manager AWS 리소스를 파악하고 제어할 수 있게 하세요.	Systems Manager 탐색기를 사용하여 조직 AWS 계정 내 모든 조직의 운영 데이터를 동기화할 수 있습니다. Systems Manager Change Manager를 사용하여 위임된 관리자 계정에서 조직의 모든 멤버 계정에 대한 변경 템플릿, 승인, 보고를 관리할 수 있습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
태그 정책 조직의 계정에 있는 리소스 전체에서 태그를 표준화합니다.	태그 정책을 생성하여 특정 리소스 및 리소스 유형에 대한 태그 지정 규칙을 정의하고 이러한 정책을 조직 단위 및 계정에 연결해 해당 규칙을 적용할 수 있습니다.	 예 자세히 알아보기	 아니요	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Trusted Advisor Trusted Advisor AWS 환경을 검사하여 비용을 절감하거나, 시스템 가용성과 성능을 개선하거나, 보안 격차를 해소할 수 있는 기회가 있을 때 권장 사항을 제시합니다.	조직 AWS 계정 내 모든 직원을 대상으로 Trusted Advisor 검사를 실행하십시오.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Well-Architected Tool 워크로드 상태를 문서화하고 최신 AWS 아키텍처 모범 사례와 비교하는 AWS Well-Architected Tool 데 도움이 됩니다.	AWS WA Tool Organizations 고객과 Organizations 고객 모두 조직의 다른 AWS WA Tool 구성원과 리소스를 공유하는 프로세스를 단순화할 수 있습니다.	 예 자세히 알아보기	 아니요	
Amazon VPC IP 주소 관리자 (IPAM) IPAM은 워크로드의 IP 주소를 더 쉽게 계획, 추적 및 모니터링할 수 있게 해주는 VPC 기능입니다. AWS	조직 전체의 IP 주소 사용을 모니터링하고 멤버 계정 간에 IP 주소 풀을 공유합니다.	 예 자세히 알아보기	 자세히 알아보기	예

AWS 서비스	다음과 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
Amazon VPC Reachability Analyzer Reachability Analyzer는 Virtual Private Cloud(VPC)에서 소스 리소스와 대상 리소스 간의 연결을 테스트할 수 있는 구성 분석 도구입니다.	조직 내의 여러 계정에 걸쳐 경로를 추적합니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS Account Management 및 AWS Organizations

AWS Account Management은 조직의 모든 AWS 계정에 대한 계정 정보 및 메타데이터를 관리하는 데 도움이 됩니다. 조직의 각 멤버 계정에 대한 대체 연락처 정보를 설정, 수정 또는 삭제할 수 있습니다. 자세한 내용은 AWS Account Management 사용 설명서의 조직에서 AWS Account Management 사용을 참조하세요.

다음 정보는 AWS Account Management를 AWS Organizations와 통합하는 데 도움을 줍니다.

Account Management로 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

조직의 이 서비스에 대한 위임된 관리자로 구성원 계정을 지정하려면 먼저 Account Management에 AWS Organizations에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Account Management의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Account Management의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Account Management를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: EnableAWSServiceAccess

Account Management로 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 AWS Account Management와 상호 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Account Management의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **`disable`**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 AWS Account Management의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Account Management를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal account.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Account Management에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 지정된 계정의 사용자 및 역할이 조직의 다른 멤버 계정의 AWS 계정 메타데이터를 관리할 수 있습니다. 위임된 관리자 계정을 활성화하지 않으면 조직의 관리 계정에서만 이러한 작업을 수행할 수 있습니다. 이렇게 하면 조직의 관리와 계정 세부 정보의 관리를 분리하는 데 도움이 됩니다.

> 최소 권한
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Account Management에 대한 위임된 관리자로 구성할 수 있습니다

위임 정책을 구성하는 방법에 대한 일반적인 설명은 리소스 기반 위임 정책 생성 또는 업데이트을(를) 참조하세요.

AWS CLI, AWS API

AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체 `account.amazonaws.com`을 파라미터로 식별합니다.

AWS Application Migration Service (애플리케이션 마이그레이션 서비스) 및 AWS Organizations

AWS Application Migration Service 애플리케이션을 마이그레이션하는 작업을 간소화, 가속화하고 비용을 절감합니다. AWS Organizations과 통합하면 글로벌 뷰 기능을 사용하여 여러 계정에 걸친 대규모 마이그레이션을 관리할 수 있습니다. 자세한 내용은 애플리케이션 마이그레이션 서비스 사용 AWS Organizations설명서에서 설정을 참조하십시오.

다음 정보를 AWS Application Migration Service 사용하면 통합에 도움이 AWS Organizations됩니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 애플리케이션 마이그레이션 서비스는 조직의 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다.

응용 프로그램 마이그레이션 서비스와 Organizations 간에 신뢰할 수 있는 액세스를 사용하지 않도록 설정하거나 조직에서 구성원 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForApplicationMigrationService`

응용 프로그램 마이그레이션 서비스에서 사용하는 서비스 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. 응용 프로그램 마이그레이션 서비스에서 사용하는 서비스 연결 역할은 다음 서비스 주체에 대한 액세스 권한을 부여합니다.

- `mgn.amazonaws.com`

애플리케이션 마이그레이션 서비스를 통해 신뢰할 수 있는 액세스 활성화

응용 프로그램 마이그레이션 서비스를 통해 신뢰할 수 있는 액세스를 활성화하면 글로벌 보기 기능을 사용하여 여러 계정에 걸친 대규모 마이그레이션을 관리할 수 있습니다. 글로벌 뷰는 다양한 AWS 계정의 소스 서버, 앱 및 웨이브에 대한 가시성과 특정 작업을 수행할 수 있는 기능을 제공합니다. 자세한 내용은 AWS Application Migration Service 사용 안내서의 AWS Organizations 설정을 참조하십시오.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Application Migration Service 콘솔이나 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다. AWS Organizations

> **Important**
>
> 가능하면 AWS Application Migration Service 콘솔이나 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이를 통해 서비스에 필요한 리소스를 만드는 등 필요한 모든 구성을 AWS Application Migration Service 수행할 수 있습니다. AWS Application Migration Service에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
> AWS Application Migration Service 콘솔이나 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면 이 단계를 완료할 필요가 없습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Application Migration Service의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. only AWS Organizations관리자인 경우 관리자에게 이제 콘솔을 사용하여 해당 서비스를 사용할 수 있도록 설정할 수 있다고 알려주십시오. AWS Application Migration Service AWS Organizations

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Application Migration Service 서비스로 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: 활성화 AWSServiceAccess

애플리케이션 마이그레이션 서비스를 통한 신뢰할 수 있는 액세스 비활성화

Organizations 관리 계정의 관리자만 응용 프로그램 마이그레이션 서비스를 통해 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Application Migration Service 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 가능하면 AWS Application Migration Service 콘솔이나 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등 필요한 정리 AWS Application Migration Service 작업을 수행할 수 있습니다. AWS Application Migration Service에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.
>
> AWS Application Migration Service 콘솔이나 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 이 단계를 완료할 필요가 없습니다.

AWS Organizations 콘솔을 사용하거나 Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. 서비스(Services) 페이지에서 AWS Application Migration Service의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 전용 AWS Organizations관리자인 경우 관리자에게 이제 콘솔이나 도구를 사용하여 해당 서비스를 사용하지 않도록 설정할 수 AWS Application Migration Service 있다고 알려주십시오. AWS Organizations

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Application Migration Service 서비스로 사용하지 않도록 설정할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 비활성화 AWSServiceAccess

애플리케이션 마이그레이션 서비스를 위한 위임된 관리자 계정 활성화

구성원 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할은 조직의 관리 계정에 있는 사용자나 역할만 수행할 수 있는 응용 프로그램 마이그레이션 서비스에 대한 관리 작업을 수행할 수 있습니다. 이렇게 하면 조직 관리를 응용 프로그램 마이그레이션 서비스 관리와 분리할 수 있습니다. 자세한 내용은 애플리케이션 마이그레이션 서비스 사용 설명서의 설정을 AWS Organizations 참조하십시오.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 구성원 계정을 조직의 응용 프로그램 마이그레이션 서비스에 대한 위임 관리자로 구성할 수 있습니다.

AWS CLI, AWS API

AWS CLI 또는 SDK 중 AWS 하나를 사용하여 위임된 관리자 계정을 구성하려는 경우 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal mgn.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 오퍼레이션과 회원 계정의 ID 번호를 호출하고 계정 서비스를 `mgn.amazonaws.com` 매개변수로 식별합니다.

애플리케이션 마이그레이션 서비스에 대한 위임 관리자 비활성화

Organizations 관리 계정의 관리자만 응용 프로그램 마이그레이션 서비스의 위임된 관리자를 제거할 수 있습니다. Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

AWS Artifact 및 AWS Organizations

AWS Artifact ISO 및 PCI 보고서와 같은 AWS 보안 규정 준수 보고서를 다운로드할 수 있는 서비스입니다. 를 사용하면 AWS Artifact새 보고서와 계정이 추가되더라도 조직의 관리 계정에 있는 사용자가 조직의 모든 구성원 계정을 대신하여 계약을 자동으로 수락할 수 있습니다. 멤버 계정 사용자는 계약을 보고 다운로드할 수 있습니다. 자세한 내용은 사용 AWS Artifact 안내서의 AWS Artifact의 여러 계정에 대한 계약 관리를 참조하십시오.

다음 정보를 AWS Artifact 사용하면 AWS Organizations쉽게 통합할 수 있습니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AWS Artifact 조직의 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS Artifact 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

조직에서 멤버 계정을 제거하는 경우 이 역할을 삭제하거나 수정할 수 있지만 권장하지는 않습니다.

역할 수정은 교차 서비스의 혼동된 대리자와 같은 보안 문제를 발생시킬 수 있으므로 권장하지 않습니다. 혼동된 대리자 예방에 대해 자세히 알아보려면 AWS Artifact 사용 설명서의 교차 서비스 대리자 예방을 참조하세요.

- `AWSServiceRoleForArtifact`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. 에서 사용하는 서비스 연결 역할은 다음 서비스 주체에게 액세스 AWS Artifact 권한을 부여합니다.

- `artifact.amazonaws.com`

AWS Artifact와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다. AWS

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. 서비스(Services) 페이지에서 AWS Artifact의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. only AWS Organizations관리자인 경우 관리자에게 이제 콘솔을 사용하여 해당 서비스를 사용할 수 있도록 설정할 수 있다고 알려주십시오. AWS Artifact AWS Organizations

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Artifact 서비스로 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: 활성화 AWSServiceAccess

AWS Artifact와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 신뢰할 수 있는 액세스를 비활성화할 수 AWS Artifact있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Artifact 조직 계약을 사용하려면 신뢰할 AWS Organizations 수 있는 액세스 권한이 필요합니다. 조직 계약을 사용하는 AWS Organizations 동안 신뢰할 수 있는 액세스를 사용하지 않도록 설정하면 조직에 액세스할 수 없으므로 기능이 중지됩니다. AWS Artifact 동의한 모든 조직 AWS Artifact 계약은

그대로 유지되지만 액세스할 수는 없습니다 AWS Artifact. AWS Artifact 생성한 AWS Artifact 역할은 그대로 유지됩니다. 신뢰할 수 있는 액세스를 다시 활성화하면 AWS Artifact 가 이전과 같이 계속 작동하므로 서비스를 다시 구성할 필요가 없습니다.

조직에서 제거된 독립 실행형 계정은 어떠한 조직 계약에도 더 이상 액세스할 수 없습니다.

AWS Organizations 콘솔을 사용하거나 Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Artifact의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 전용 AWS Organizations관리자인 경우 관리자에게 이제 콘솔이나 도구를 사용하여 해당 서비스를 사용하지 않도록 설정할 수 AWS Artifact 있다고 알려주십시오. AWS Organizations

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Artifact 서비스로 사용하지 않도록 설정할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: 비활성화 AWSServiceAccess

AWS Audit Manager 및 AWS Organizations

AWS Audit Manager는 AWS 사용을 지속적으로 감사하여 위험을 평가하고 규정 및 업계 표준을 준수하는 방법을 간소화할 수 있도록 지원합니다. Audit Manager는 증거 수집을 자동화하여 정책, 절차 및 활동이 효과적으로 운영되는지 더욱 쉽게 평가할 수 있도록 합니다. 감사 시기에 Audit Manager는 수동 작업을 줄여주어 통제에 대한 이해 관계자 검토를 관리하고 감사 준비 보고서를 작성하는 데 도움을 줍니다.

Audit Manager와 AWS Organizations를 통합하면 평가 범위 안에 조직의 여러 AWS 계정을 포함시켜 더 광범위한 소스에서 증거를 수집할 수 있습니다.

자세한 내용은 Audit Manager 사용 설명서의 AWS Organizations 활성화를 참조하세요.

다음 정보는 AWS Audit Manager와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Audit Manager는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Audit Manager와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Audit Manager가 이 역할을 사용하는 방식에 대한 자세한 내용은 AWS Audit Manager 사용 설명서의 서비스 연결 역할 사용을 참조하세요.

- `AWSServiceRoleForAuditManager`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Audit Manager가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `auditmanager.amazonaws.com`

Audit Manager와 상호 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

멤버 계정을 조직의 위임된 관리자로 지정하려면 먼저 Audit Manager에게 AWS Organizations에 대한 신뢰할 수 있는 액세스가 필요합니다.

AWS Audit Manager 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Audit Manager 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Audit Manager가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Audit Manager에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오. AWS Audit Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Audit Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 방법은 AWS Audit Manager 사용 설명서의 설정을 참조하세요.

> **Note**
>
> AWS Audit Manager 콘솔을 사용해 위임된 관리자를 구성하는 경우 AWS Audit Manager가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Audit Manager를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal auditmanager.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

Audit Manager와 상호 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 AWS Audit Manager와 상호 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Audit Manager를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Audit Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Audit Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Audit Manager 관리와 조직 관리를 분리하는 데 도움을 줍니다.

> **최소 권한**
>
> 다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Audit Manager에 대한 위임된 관리자로 구성할 수 있습니다.
> `audit-manager:RegisterAccount`

Audit Manager에 대한 위임된 관리자 계정 활성화에 대한 설명은 AWS Audit Manager사용 설명서의 설정을 참조하세요.

AWS Audit Manager 콘솔을 사용해 위임된 관리자를 구성하는 경우 Audit Manager가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

AWS CLI, AWS API

AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK: `RegisterAccount` 작업을 호출하고 `delegatedAdminAccount`를 파라미터로 제공하여 관리자 계정을 위임합니다.

AWS Backup 및 AWS Organizations

AWS Backup은 조직의 AWS Backup 작업을 관리하고 모니터링할 수 있는 서비스입니다. AWS Backup을 사용하면 조직의 관리 계정의 사용자로 로그인하여 조직 전체에서 백업 보호 및 모니터링을 활성화할 수 있습니다. 백업 정책을 사용하여 조직 내 모든 계정의 리소스에 AWS Backup 계획을 중앙에서 적용함으로써 규정 준수를 달성할 수 있습니다. AWS Backup과 AWS Organizations를 함께 사용하면 다음과 같은 이점을 얻을 수 있습니다.

보호

조직에서 백업 정책 유형을 활성화한 다음 조직의 루트, OU 또는 계정에 연결할 백업 정책을 생성할 수 있습니다. 백업 정책은 AWS Backup 계획과 계정에 해당 계획을 자동으로 적용하는 데 필요한 다른 세부 정보를 결합합니다. 계정에 직접 연결된 정책은 조직의 루트 및 모든 상위 OU에서 상속된 정책과 병합되어 계정에 적용되는 유효 정책을 형성합니다. 정책에는 계정의 리소스에 AWS Backup을 실행할 권한이 있는 IAM 역할의 ID가 포함됩니다. AWS Backup은 IAM 역할을 사용하여 유효 정책의 백업 계획에 지정된 대로 사용자를 대신하여 백업을 수행합니다.

모니터링(Monitoring)

조직에서 AWS Backup에 대한 신뢰할 수 있는 액세스를 활성화하면 AWS Backup 콘솔을 사용하여 조직의 모든 계정에서 백업, 복원 및 복사 작업의 세부 정보를 볼 수 있습니다. 자세한 내용은 AWS Backup 개발자 안내서의 백업 작업 모니터링을 참조하세요.

AWS Backup에 대한 자세한 내용은 AWS Backup개발자 안내서 단원을 참조하세요.

다음 정보는 AWS Backup와 AWS Organizations를 통합하는 데 도움을 줍니다.

AWS Backup와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Backup 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Backup 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Backup가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Backup에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
> AWS Backup 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

AWS Backup을 사용해 신뢰할 수 있는 액세스를 활성화하려면 AWS Backup 개발자 안내서의 여러 AWS 계정에서 백업 활성화를 참조하세요.

AWS Backup와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Backup이 조직의 계정에서 백업, 복원 및 복사 작업을 모니터링하려면 AWS Organizations와 상호 신뢰할 수 있는 액세스가 필요합니다. 신뢰할 수 있는 액세스를 비활성화하면 AWS Backup이 현재 계정 외부의 작업을 볼 수 없게 됩니다. AWS Backup이 생성한 AWS Backup 역할은 그대로 남아 있습니다. 신뢰할 수 있는 액세스를 다시 활성화하면 AWS Backup이 이전과 같이 계속 작동하므로 서비스를 다시 구성할 필요가 없습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Backup를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

AWS Backup에 대한 위임된 관리자 계정 활성화

AWS Backup 개발자 안내서의 위임된 관리자를 참조하세요.

AWS Billing and Cost Management 및 AWS Organizations

AWS Billing and Cost Management 청구 설정, 청구서 검색 및 지불, 비용 분석, 구성, 계획 및 최적화에 도움이 되는 일련의 기능을 제공합니다. Billing and Cost AWS Organizations Management를 함께 사용하는 경우 비용 할당 데이터를 분할하여 AWS Organizations 정보를 검색하고 (해당하는 경우) 선택한 분할 비용 할당 데이터 서비스에 대한 원격 분석 데이터를 수집할 수 있습니다.

다음 정보를 활용하면 쉽게 AWS Billing and Cost Management 통합할 수 있습니다. AWS Organizations

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Billing and Cost Management는 조직의 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Billing and Cost Management와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 구성원 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

자세한 내용은 Billing and Cost Management 사용 설명서에서 Billing and Cost Management의 서비스 연결 역할 권한을 참조하십시오.

- `AWSServiceRoleForSplitCostAllocationData`

Billing and Cost Management에서 사용하는 서비스 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Billing and Cost Management에서 사용하는 서비스 연결 역할은 다음 서비스 주체에 대한 액세스 권한을 부여합니다.

Billing and Cost Management는 `billing-cost-management.amazonaws.com` 서비스 주체를 사용합니다.

Billing 및 Cost Management를 통한 신뢰할 수 있는 액세스 지원

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

관리 계정을 통해 신뢰할 수 있는 액세스를 활성화하면 고객은 Billing and Cost Management의 분할 비용 할당 데이터 기능을 활용할 수 있습니다. 고객이 Prometheus용 Amazon Managed Service를 사

용하여 Amazon Elastic Kubernetes Service에 대한 분할 비용 할당 데이터를 활성화하면 신뢰할 수 있는 액세스가 호출되어 조직 내 모든 구성원 계정에 대한 서비스 연결 역할을 생성합니다. 이를 통해 비용 할당 데이터를 분할하여 고객의 Amazon Managed Service for Prometheus 작업 공간에서 텔레메트리 데이터를 수집하고 해당 지표를 기반으로 비용 할당을 수행할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다. AWS

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Billing and Cost Management의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. only AWS Organizations관리자인 경우 관리자에게 이제 콘솔을 사용하여 해당 서비스를 사용할 수 있도록 설정할 수 있다고 알려주십시오. AWS Billing and Cost Management AWS Organizations

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Billing and Cost Management 서비스로 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 활성화 AWSServiceAccess

트러스트된 액세스 사용 중지

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Billing and Cost Management 서비스로 사용하지 않도록 설정할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 비활성화 AWSServiceAccess

AWS CloudFormation StackSets와 AWS Organizations

AWS CloudFormation StackSets를 사용하면 단일 작업으로 여러 AWS 계정 및 AWS 리전에 대해 스택을 생성, 업데이트 또는 삭제할 수 있습니다. StackSets와 AWS Organizations의 통합으로 고객은 각 멤버 계정에서 관련 권한을 보유한 서비스 연결 역할을 사용하여 서비스 관리형 권한이 있는 스택 세트를 생성할 수 있습니다. 이를 통해 조직의 멤버 계정에 스택 인스턴스를 배포할 수 있습니다. StackSets가 사용자를 대신하여 각 멤버 계정에 IAM 역할을 생성하므로 필요한 AWS Identity and Access Management 역할을 생성할 필요가 없습니다.

나중에 조직에 추가되는 계정에 자동 배포를 활성화하기로 선택할 수도 있습니다. 자동 배포가 활성화되면 연결된 스택 세트 인스턴스의 역할 및 배포가 향후 해당 OU에 추가되는 모든 계정에 자동으로 추가됩니다.

StackSets와 Organizations 간의 신뢰할 수 있는 액세스가 활성화되면 관리 계정은 조직의 스택 세트를 생성하고 관리할 수 있는 권한을 보유하게 됩니다. 관리 계정은 최대 5개의 멤버 계정을 위임된 관리자로 등록할 수 있습니다. 신뢰할 수 있는 액세스를 활성화하면 위임된 관리자도 조직의 스택 세트를 생성하고 관리할 수 있는 권한을 갖습니다. 서비스 관리형 권한이 있는 스택 세트는 위임된 관리자가 생성한 스택 세트를 포함하여 관리 계정에 생성됩니다.

> **Important**
>
> 위임된 관리자는 조직의 계정에 배포할 수 있는 모든 권한을 가집니다. 관리 계정은 위임된 관리자 권한을 특정 OU에 배포하는 권한 또는 특정 스택 세트 작업을 수행하는 권한으로 제한할 수 없습니다.

StackSets와 Organizations의 통합에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation StackSets 사용을 참조하세요.

다음 정보는 AWS CloudFormation StackSets와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AWS CloudFormation Stacksets는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS CloudFormation Stacksets와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- 관리 계정: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

서비스 연결 역할 `AWSServiceRoleForCloudFormationStackSetsOrgMember`를 생성하려면 조직 내 멤버 계정의 경우 먼저 관리 계정에 스택 세트를 생성해야 합니다. 이렇게 하면 스택 세트 인스턴스가 생성되고, 멤버 계정에 역할이 생성됩니다.

- 멤버 계정: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

스택 세트 생성에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation StackSets 사용을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. AWS CloudFormation Stacksets가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- 관리 계정: `stacksets.cloudformation.amazonaws.com`

  StackSets와 Organizations 간의 신뢰할 수 있는 액세스가 비활성화된 경우에만 이 역할을 수정하거나 삭제할 수 있습니다.
- 멤버 계정: `member.org.stacksets.cloudformation.amazonaws.com`

  StackSets와 Organizations 간의 신뢰할 수 있는 액세스를 먼저 비활성화하거나, 계정을 대상 조직 또는 조직 단위(OU)에서 먼저 제거한 경우에만 이 역할을 수정하거나 삭제할 수 있습니다.

AWS CloudFormation Stacksets와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

Organizations 관리 계정의 관리자만 다른 AWS 서비스와 상호 신뢰할 수 있는 액세스를 활성화할 권한이 있습니다. AWS CloudFormation 콘솔 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

신뢰할 수 있는 액세스는 AWS CloudFormation StackSets로만 활성화할 수 있습니다.

AWS CloudFormation Stacksets 콘솔을 사용해 신뢰할 수 있는 액세스를 활성화하려면 AWS CloudFormation 사용 설명서에서 AWS Organizations와 상호 신뢰할 수 있는 액세스 활성화를 참조하세요.

AWS CloudFormation Stacksets와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

Organizations 관리 계정의 관리자만 다른 AWS 서비스와 상호 신뢰할 수 있는 액세스를 비활성화할 권한이 있습니다. 신뢰할 수 있는 액세스는 Organizations 콘솔로만 비활성화할 수 있습니다.

StackSets를 사용하는 동안 Organizations와 상호 신뢰할 수 있는 액세스를 비활성화하면 이전에 생성된 모든 스택 인스턴스는 유지됩니다. 그러나 서비스 연결 역할의 권한을 사용하여 배포된 스택 세트는 더 이상 조직에서 관리하는 계정에 대한 배포를 수행할 수 없습니다.

AWS CloudFormation 콘솔 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 신뢰할 수 있는 액세스를 프로그래밍 방식으로 비활성화하면(예: AWS CLI 또는 API 사용) 권한이 제거된다는 점을 유의해야 합니다. AWS CloudFormation 콘솔로 신뢰할 수 있는 액세스를 비활성화하는 것이 더 좋습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 페이지에서 AWS CloudFormation StackSets의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **`disable`**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 AWS CloudFormation StackSets의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS CloudFormation StackSets를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

AWS CloudFormation Stacksets에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 AWS CloudFormation Stacksets에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 AWS CloudFormation Stacksets 관리와 조직 관리를 분리하는 데 도움을 줍니다.

조직에서 멤버 계정을 AWS CloudFormation Stacksets의 위임된 관리자로 지정하는 방법에 관한 설명은 AWS CloudFormation 사용 설명서의 위임된 관리자 등록을 참조하세요.

AWS CloudTrail 및 AWS Organizations

AWS CloudTrail 기업의 거버넌스, 규정 준수, 운영 및 위험 감사를 가능하게 하는 AWS 서비스입니다. AWS 계정를 사용하여 AWS CloudTrail관리 계정의 사용자는 조직 내 모든 사용자에 대한 모든 AWS 계정 이벤트를 기록하는 조직 내역을 만들 수 있습니다. 조직 추적 기록은 조직 내 모든 구성원 계정에 자동으로 적용됩니다. 구성원 계정은 조직 추적 기록을 볼 수 있지만 수정하거나 삭제할 수는 없습니다. 기본적으로 멤버 계정은 Amazon S3 버킷에 있는 조직 추적 기록에 대한 로그 파일에 액세스할 수 있는 권한이 없습니다. 이는 조직 내 계정에 걸쳐 이벤트 로깅 방식을 일관적으로 적용 및 시행하는 데 도움이 됩니다.

자세한 내용은 AWS CloudTrail 사용 설명서에서 조직에 대한 추적 생성을 참조하세요.

다음 정보를 활용하면 AWS CloudTrail 통합에 도움이 AWS Organizations됩니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 CloudTrail 조직의 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다.

CloudTrail 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForCloudTrail`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. 에서 사용하는 서비스 연결 역할은 다음 서비스 주체에게 액세스 CloudTrail 권한을 부여합니다.

- `cloudtrail.amazonaws.com`

CloudTrail와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS CloudTrail 콘솔에서 트레일을 만들어 신뢰할 수 있는 액세스를 활성화하면 신뢰할 수 있는 액세스가 자동으로 구성됩니다 (권장). AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수도 있습니다. 조직 내역을 만들려면 AWS Organizations 관리 계정으로 로그인해야 합니다.

AWS CLI 또는 AWS API를 사용하여 조직 트레일을 생성하기로 선택한 경우 신뢰할 수 있는 액세스를 수동으로 구성해야 합니다. 자세한 내용은 사용 AWS CloudTrail 설명서의 신뢰할 수 AWS Organizations있는 CloudTrail 서비스로 활성화를 참조하십시오.

> **Important**
>
> 가능하면 AWS CloudTrail 콘솔이나 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS CloudTrail 서비스로 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 활성화 AWSServiceAccess

CloudTrail와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS CloudTrail 조직 트레일 및 조직 이벤트 데이터 저장소를 사용하려면 신뢰할 수 있는 AWS Organizations 액세스가 필요합니다. 사용 AWS Organizations 중에 을 사용하여 신뢰할 수 있는 액세스를 비활성화하면 기관에 접근할 CloudTrail 수 없으므로 구성원 계정의 조직 트레일이 모두 삭제됩니다. AWS CloudTrail모든 관리 계정 조직 트레일 및 조직 이벤트 데이터 저장소는 계정 수준 트레일 및 이벤트 데이터 저장소로 변환됩니다. 계정 간의 CloudTrail 통합을 위해 생성된 `AWSServiceRoleForCloudTrail` 역할은 계정 내에서 AWS Organizations 유지됩니다. 신뢰할 수 있는 액세스를 다시 CloudTrail 활성화하면 기존 트레일 및 이벤트 데이터 저장소에 대해 조치를 취하지 않습니다. 관리 계정은 모든 계정 수준의 트레일 및 이벤트 데이터 저장소를 업데이트하여 조직에 적용해야 합니다.

계정 수준의 트레일 또는 이벤트 데이터 저장소를 조직 트레일 또는 조직 이벤트 데이터 저장소로 변환하려면 다음을 수행하십시오.

- CloudTrail 콘솔에서 트레일 또는 이벤트 데이터 저장소를 업데이트하고 내 조직의 모든 계정에 대해 활성화 옵션을 선택합니다.
- 에서 AWS CLI다음을 수행하십시오.
  - 트레일을 업데이트하려면 update-trail명령을 실행하고 `--is-organization-trail` 파라미터를 포함시키십시오.

- 이벤트 데이터 저장소를 업데이트하려면 update-event-data-store명령을 실행하고 `--organization-enabled` 파라미터를 포함시키십시오.

AWS Organizations 관리 계정의 관리자만 신뢰할 수 있는 액세스를 비활성화할 수 AWS CloudTrail있습니다. AWS Organizations 콘솔을 사용하거나 Organizations AWS CLI 명령을 실행하거나 SDK 중 하나에서 Organizations API 작업을 호출하여 Organizations 도구를 통해서만 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. AWS

AWS Organizations 콘솔을 사용하거나 Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS CloudTrail의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **`disable`**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 전용 AWS Organizations관리자인 경우 관리자에게 이제 콘솔이나 도구를 사용하여 해당 서비스를 사용하지 않도록 설정할 수 AWS CloudTrail 있다고 알려주십시오. AWS Organizations

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS CloudTrail 서비스로 사용하지 않도록 설정할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal cloudtrail.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 비활성화 AWSServiceAccess

다음에 대해 위임된 관리자 계정을 활성화합니다. CloudTrail

CloudTrail Organizations와 함께 사용하면 조직 내 모든 계정을 등록하여 조직을 대신하여 조직의 트레일 및 이벤트 데이터 저장소를 관리하는 CloudTrail 위임된 관리자 역할을 할 수 있습니다. 위임된 관리자는 관리 계정과 동일한 관리 작업을 수행할 수 있는 조직의 구성원 계정입니다. CloudTrail

> **최소 권한**
>
> Organizations 관리 계정의 관리자만 위임된 관리자를 등록할 수 있습니다. CloudTrail

CloudTrail 콘솔을 사용하거나 Organizations `RegisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 등록할 수 있습니다. CloudTrail 콘솔을 사용하여 위임된 관리자를 등록하려면 위임된 관리자 추가를 참조하십시오. CloudTrail

에 대해 위임된 관리자를 비활성화할 수 있습니다. CloudTrail

Organizations 관리 계정의 관리자만 의 위임된 관리자를 제거할 수 있습니다. CloudTrail CloudTrail 콘솔을 사용하거나 Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. CloudTrail 콘솔을 사용하여 위임된 관리자를 제거하는 방법에 대한 자세한 내용은 위임된 관리자 제거를 참조하십시오. CloudTrail

AWS Compute Optimizer 및 AWS Organizations

AWS Compute Optimizer는 AWS 리소스의 구성 및 사용률 지표를 분석하는 서비스입니다. 리소스의 예로는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 Auto Scaling 그룹이 있습니다. Compute Optimizer는 리소스가 최적 상태인지 여부를 보고하고, 최적화 권장 사항을 생성하여 비용을 절감하고 워크로드의 성능을 개선합니다. Compute Optimizer에 대한 자세한 내용은 AWS Compute Optimizer 사용 설명서를 참조하세요.

다음 정보는 AWS Compute Optimizer와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Compute Optimizer는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Compute Optimizer와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForComputeOptimizer`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Compute Optimizer가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `compute-optimizer.amazonaws.com`

Compute Optimizer와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Compute Optimizer 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Compute Optimizer 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Compute Optimizer가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Compute Optimizer에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
>
> AWS Compute Optimizer 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Compute Optimizer 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

조직의 관리 계정을 사용하여 Compute Optimizer 콘솔에 로그인해야 합니다. AWS Compute Optimizer 사용 설명서에 있는 계정 옵트인하기의 설명에 따라 조직을 대신해 옵트인합니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Compute Optimizer의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Compute Optimizer의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Compute Optimizer를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

Compute Optimizer와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 AWS Compute Optimizer와 상호 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Compute Optimizer를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Compute Optimizer에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 지정된 계정의 사용자 및 역할이 조직의 다른 멤버 계정의 AWS 계정 메타데이터를 관리할 수 있습니다. 위임된 관리자 계정을 활성화하지 않으면 조직의 관리 계정에서만 이러한 작업을 수행할 수 있습니다. 이렇게 하면 조직의 관리와 계정 세부 정보의 관리를 분리하는 데 도움이 됩니다.

> **최소 권한**
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Compute Optimizer에 대한 위임된 관리자로 구성할 수 있습니다

Compute Optimizer에 대한 위임된 관리자 계정 활성화에 대한 설명은 AWS Compute Optimizer 사용 설명서의 https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html 섹션을 참조하세요.

AWS CLI, AWS API

AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체 `account.amazonaws.com`을 파라미터로 식별합니다.

Compute Optimizer에 대한 위임된 관리자 비활성화

조직 관리 계정의 관리자만 Compute Optimizer에 대해 위임된 관리자를 구성할 수 있습니다.

Compute Optimizer 콘솔을 사용하여 위임된 관리자 Compute Optimizer 계정을 사용하지 않도록 설정하려면AWS Compute Optimizer사용 설명서의 https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html 섹션을 참조하세요.

AWS AWS CLI를 사용하여 위임된 관리자를 제거하려면 AWS AWS CLI명령 참조의 deregister-delegated-administrator를 참조하세요.

AWS Config 및 AWS Organizations

AWS Config의 다중 계정, 다중 리전 데이터 집계 기능을 사용하면 다중 계정 및 AWS 리전의 AWS Config 데이터를 단일 계정으로 집계할 수 있습니다. 다중 계정, 다중 리전 데이터 집계는 중앙 IT 관리자가 엔터프라이즈에서 여러 AWS 계정의 규정 준수를 모니터링하는 데 유용합니다. 집계자는 다중

소스 계정 및 리전의 AWS Config 데이터를 수집하는 AWS Config의 리소스 유형입니다. 집계된 AWS Config 데이터를 보려는 리전에서 집계자를 생성합니다. 집계를 생성할 때 개별 계정 ID 추가 또는 사용자 조직 추가 중에서 하나를 선택할 수 있습니다. AWS Config에 대한 자세한 내용은 AWS Config개발자 안내서 단원을 참조하세요.

AWS Config API를 사용하여 조직의 모든 AWS 계정에 걸쳐 AWS Config 규칙을 관리할 수도 있습니다. 자세한 내용은 AWS Config 개발자 안내서의 조직의 모든 계정에서 AWS Config 규칙 활성화를 참조하세요.

다음 정보는 AWS Config와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 계정에 생성됩니다. 이 역할을 통해 AWS Config는 계정 내에서 지원되는 작업을 수행할 수 있습니다.

- `AWSServiceRoleForConfig`

이 역할은 조직에서 AWS Config를 활성화할 때 다중 계정 집계자를 생성하여 생성됩니다. AWS Config는 역할을 선택하거나 생성하고 이름을 제공하도록 요청합니다. 자동으로 생성된 이름은 없습니다.

AWS Config와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

AWS Config와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Config 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Config 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Config가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Config에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.

AWS Config 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

AWS Config 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Config를 사용하여 AWS Organizations에 대한 신뢰할 수 있는 액세스를 활성화하려면 다중 계정 집계자를 생성하고 조직을 추가합니다. 다중 계정 집계자를 구성하는 방법에 대한 자세한 내용은 AWS Config 개발자 안내서의 콘솔을 사용하여 집계자 설정을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Config의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Config의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Config를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal config.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

AWS Config와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Config를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

AWS Cost Optimization Hub 및 AWS Organizations

AWS Cost Optimization Hub AWS Billing and Cost Management 기능을 사용하면 AWS 계정 및 AWS 지역 전반에서 비용 최적화 권장 사항을 통합하고 우선 순위를 지정하여 지출을 최대한 활용할 수 있습

니다. AWS Cost Optimization Hub와 함께 AWS Organizations 사용하면 Organizations 회원 계정 및 AWS 지역 전반에서 AWS 비용 최적화 권장 사항을 쉽게 식별, 필터링 및 집계할 수 있습니다.

자세한 내용은 AWS Cost Management 사용 설명서의 비용 최적화 허브를 참조하십시오.

다음 정보를 AWS Cost Optimization Hub 사용하면 쉽게 통합할 수 AWS Organizations있습니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Cost Optimization Hub는 조직의 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Cost Optimization Hub와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 구성원 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

자세한 내용은 사용 AWS Cost Management 설명서의 Cost Optimization Hub의 서비스 연결 역할 권한을 참조하십시오.

- `AWSServiceRoleForCostOptimizationHub`

비용 최적화 허브에서 사용하는 서비스 주체

비용 최적화 허브는 `cost-optimization-hub.bcm.amazonaws.com` 서비스 주체를 사용합니다.

비용 최적화 허브를 통해 신뢰할 수 있는 액세스 지원

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

조직의 관리 계정을 사용하여 옵트인하고 조직 내 모든 구성원 계정을 포함하면 Cost Optimization Hub에 대한 신뢰할 수 있는 액세스가 조직 계정에서 자동으로 활성화됩니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.

2. 서비스(Services) 페이지에서 AWS Cost Optimization Hub의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. only AWS Organizations관리자인 경우 관리자에게 이제 콘솔을 사용하여 해당 서비스를 사용할 수 있도록 설정할 수 있다고 알려주십시오. AWS Cost Optimization Hub AWS Organizations

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Cost Optimization Hub 서비스로 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: 활성화 AWSServiceAccess

트러스트된 액세스 사용 중지

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

> **Important**
>
> 옵트인한 후 비용 최적화 허브의 신뢰할 수 있는 액세스를 비활성화하면 비용 최적화 허브는 조직의 구성원 계정에 대한 권장 사항에 대한 액세스를 거부합니다. 또한 조직 내 구성원 계정

은 비용 최적화 허브에 옵트인되지 않습니다. AWS Cost Management 사용 설명서의 비용 최적화 허브 및 조직의 신뢰할 수 있는 액세스에서 자세히 알아보십시오.

Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Cost Optimization Hub 서비스로 사용하지 않도록 설정할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 비활성화 AWSServiceAccess

AWS Control Tower 및 AWS Organizations

AWS Control Tower는 규범적 모범 사례에 따라 AWS 다중 계정 환경을 설정하고 관리하는 간단한 방법을 제공합니다. AWS Control Tower 오케스트레이션은 AWS Organizations의 기능을 확장합니다. AWS Control Tower은 예방 및 탐지 제어 기능(가드레일)을 적용하여 조직 및 계정이 모범 사례를 이탈(드리프트)하지 않도록 도와줍니다.

AWS Control Tower 오케스트레이션은 AWS Organizations의 기능을 확장합니다.

자세한 내용은 AWS Control Tower 사용 설명서를 참조하세요.

다음 정보는 AWS Control Tower를 AWS Organizations와 통합하는 데 도움을 줍니다.

통합에 필요한 역할

등록된 모든 계정에 `AWSControlTowerExecution` 역할이 있어야 합니다. 이를 사용하면 AWS Control Tower에서 개별 계정을 관리하고 해당 계정에 대한 정보를 감사 및 로그 아카이브 계정에 보고할 수 있습니다.

AWS Control Tower에서 사용하는 역할에 대한 자세한 내용은 AWS Control Tower가 역할을 사용하여 계정을 생성 및 관리하는 방식과 AWS Control Tower에 대한 자격 증명 기반 정책(IAM 정책) 사용을 참조하세요.

AWS Control Tower에 의해 사용되는 서비스 보안 주체

AWS Control Tower는 `controltower.amazonaws.com` 서비스 보안 주체를 사용합니다.

AWS Control Tower와 상호 신뢰할 수 있는 액세스 활성화

AWS Control Tower는 신뢰할 수 있는 액세스를 사용하여 예방 제어를 위한 드리프트를 감지하고 드리프트를 유발하는 계정 및 OU 변경을 추적합니다.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

Organizations 콘솔에서 신뢰할 수 있는 액세스를 활성화하려면 AWS Control Tower 옆의 **Enable access**를 선택합니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Control Tower를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal controltower.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

AWS Control Tower와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

> **Important**
>
> AWS Control Tower의 신뢰할 수 있는 액세스를 비활성화하면 AWS Control Tower 랜딩 존에 드리프트가 발생합니다. 드리프트를 해결할 수 있는 유일한 방법은 AWS Control Tower의 랜딩 존 수리를 사용하는 것입니다. 조직에서 신뢰할 수 있는 액세스를 다시 활성화해도 드리프트가 해결되지는 않습니다. AWS Control Tower 사용 설명서에서 드리프트에 대해 자세히 알아보세요.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Control Tower를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal controltower.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Amazon Detective 및 AWS Organizations

Amazon Detective는 로그 데이터를 사용하여 시각화를 생성하며, 이 시각화를 사용하여 보안 결과 또는 의심스러운 활동의 근본 원인을 분석, 조사 및 식별할 수 있습니다.

AWS Organizations를 사용하면 Detective 동작 그래프가 모든 조직 계정의 활동에 대한 가시성을 제공하게 할 수 있습니다.

Detective 에 신뢰할 수 있는 액세스 권한을 부여하면 Detective 서비스가 조직 멤버십의 변화에 자동으로 대응할 수 있습니다. 위임된 관리자는 동작 그래프에서 모든 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 또한 Detective는 자동으로 새 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 조직 계정은 동작 그래프에서 자신을 연결 해제할 수 없습니다.

자세한 내용은 Amazon Detective 관리 안내서의 조직에서 Amazon Detective 사용을 참조하세요.

다음 정보는 Amazon Detective와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Detective는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Detective와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForDetective`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Detective가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `detective.amazonaws.com`

Detective에서 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

> **Note**
>
> Amazon Detective에 대해 위임된 관리자를 지정하면 조직의 Detective에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.
> 조직의 이 서비스에 대한 위임된 관리자로 멤버 계정을 지정하려면 Detective에 먼저 AWS Organizations에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 Amazon Detective의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 Amazon Detective의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

Detective에서 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 Amazon Detective에서 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 Amazon Detective의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **`disable`**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 Amazon Detective의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

Detective에 대한 위임된 관리자 계정 활성화

Detective에 대한 위임된 관리자 계정은 Detective 동작 그래프의 관리자 계정입니다. 위임된 관리자는 동작 그래프에서 멤버 계정으로 활성화하거나 비활성화할 조직 계정을 결정합니다. 위임된 관리자는 새 조직 계정이 조직에 추가될 때 자동으로 새 조직 계정을 멤버 계정으로 활성화하도록 Detective를 구성할 수 있습니다. 위임된 관리자가 조직 계정을 관리하는 방법에 대한 자세한 내용은 Amazon Detective 관리 안내서의 조직 계정을 멤버 계정으로 관리를 참조하세요.

조직 관리 계정의 관리자만 Detective에 대해 위임된 관리자를 구성할 수 있습니다.

Detective 콘솔이나 API에서 또는 Organizations CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 지정할 수 있습니다.

> 최소 권한
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Detective에 대한 위임된 관리자로 구성할 수 있습니다

Detective 콘솔 또는 API를 사용하여 위임된 관리자를 구성하려면 Amazon Detective 관리 안내서의 조직의 Detective 관리자 계정 지정을 참조하세요.

AWS CLI, AWS API

AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal detective.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체 `account.amazonaws.com`을 파라미터로 식별합니다.

Detective에 대해 위임된 관리자를 비활성화

Detective 콘솔이나 API에서 또는 Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. Detective 콘솔 또는 API를 사용하거나 Organizations API를 사용하여 위임된 관리자를 제거하는 방법에 대한 자세한 내용은 Amazon Detective 관리 안내서의 조직의 Detective 관리자 계정 지정을 참조하세요.

Amazon DevOps Guru 및 AWS Organizations

Amazon DevOps Guru는 운영 데이터와 애플리케이션 지표 및 이벤트를 분석하여 정상적인 운영 패턴에서 벗어나는 동작을 식별합니다. DevOps Guru가 운영 문제 또는 위험을 감지하면 사용자에게 알림이 전송됩니다.

DevOps Guru를 사용하면 AWS Organizations에서 다중 계정 지원을 활성화할 수 있으므로 전체 조직의 인사이트를 관리하는 멤버 계정을 지정할 수 있습니다. 그러면 이 위임된 관리자는 조직 내의 모든 계정에서 인사이트를 보고 정렬하고 필터링할 수 있으므로 추가적으로 사용자 정의할 필요 없이 조직 내에서 모니터링되는 모든 애플리케이션의 상태를 전체적으로 파악할 수 있습니다.

자세한 내용은 Amazon DevOps Guru 사용 설명서에서 조직 전체의 계정 모니터링을 참조하세요.

다음 정보는 Amazon DevOps Guru와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 DevOps Guru는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

DevOps Guru와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForDevOpsGuru`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. DevOps Guru가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `devops-guru.amazonaws.com`

자세한 내용은 Amazon DevOps Guru 사용 설명서에서 DevOps Guru에 서비스 연결 역할 사용을 참조하세요.

DevOps Guru에서 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

> **Note**
>
> Amazon DevOps Guru에 대해 위임된 관리자를 지정하면 조직의 DevOps Guru에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.
> 조직의 이 서비스에 대한 위임된 관리자로 멤버 계정을 지정하려면 DevOps Guru에 먼저 AWS Organizations에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

> **Important**
>
> 가능하면 항상 Amazon DevOps Guru 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 Amazon DevOps Guru가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. Amazon DevOps Guru에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.

AWS Organizations 콘솔 또는 DevOps Guru 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 Amazon DevOps Guru의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 Amazon DevOps Guru의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

DevOps Guru console

DevOps Guru 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

1. 관리 계정에서 관리자로 로그인하고 Amazon DevOps Guru 콘솔(Amazon DevOps Guru console)을 선택하여 DevOps Guru 콘솔을 엽니다.
2. 신뢰할 수 있는 액세스 활성화를 선택합니다.

DevOps Guru에서 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 Amazon DevOps Guru에서 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 Amazon DevOps Guru의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **`disable`**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 Amazon DevOps Guru의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

DevOps Guru에 대한 위임된 관리자 계정 활성화

DevOps Guru의 위임된 관리자 계정은 조직에서 DevOps Guru에 온보딩된 모든 멤버 계정의 인사이트 데이터를 볼 수 있습니다. 위임된 관리자가 조직 계정을 관리하는 방법에 대한 자세한 내용은 Amazon DevOps Guru 사용 설명서의 조직 전체의 계정 모니터링을 참조하세요.

조직 관리 계정의 관리자만 DevOps Guru에 대해 위임된 관리자를 구성할 수 있습니다.

DevOps Guru 콘솔에서 또는 Organizations `RegisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 지정할 수 있습니다.

> 최소 권한
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 DevOps Guru에 대한 위임된 관리자로 구성할 수 있습니다

DevOps Guru console

DevOps Guru 콘솔에서 위임된 관리자를 구성하려면

1. 관리 계정에서 관리자로 로그인하고 Amazon DevOps Guru 콘솔(Amazon DevOps Guru console)을 선택하여 DevOps Guru 콘솔을 엽니다.

2. 위임된 관리자 등록을 선택합니다. 관리 계정 또는 원하는 멤버 계정을 위임된 관리자로 선택할 수 있습니다.

AWS CLI, AWS API

AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체 `account.amazonaws.com`을 파라미터로 식별합니다.

DevOps Guru에 대해 위임된 관리자를 비활성화

DevOps Guru 콘솔을 사용하거나 Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. DevOps Guru 콘솔을 사용하여 위임된 관리자를 제거하는 방법에 대한 자세한 내용은 Amazon DevOps Guru 사용 설명서의 조직 전체의 계정 모니터링을 참조하세요.

AWS Directory Service 및 AWS Organizations

Microsoft Active Directory용 AWS Directory Service 또는 AWS Managed Microsoft AD를 사용하여 Microsoft Active Directory(AD)를 관리형 서비스로 실행할 수 있습니다. AWS Directory Service는 AWS 클라우드에서 디렉터리를 설정 및 실행하거나 AWS 리소스를 기존의 온프레미스 Microsoft Active Directory에 연결할 때 용이성을 제공합니다. AWS Managed Microsoft AD는 또한 AWS Organizations와 긴밀하게 통합되어 여러 AWS 계정과 리전의 VPC에 대해 디렉터리 공유를 원활하게 수행할 수 있습니다 자세한 정보는 AWS Directory Service 관리 안내서를 참조하세요.

다음 정보는 AWS Directory Service와 AWS Organizations를 통합하는 데 도움을 줍니다.

AWS Directory Service와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Directory Service 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Directory Service 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Directory Service가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Directory Service에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
>
> AWS Directory Service 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

AWS Directory Service 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 자동으로 활서오하하는 디렉터리를 공유하려면 AWS Directory Service 관리 안내서의 내 디렉터리 공유를 참조하세요. 단계별 지침은 자습서: AWS 관리형 Microsoft AD Directory 공유를 참조하세요.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Directory Service의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Directory Service의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS Directory Service와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Directory Service를 사용할 때 AWS Organizations를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 이전에 공유했던 디렉터리가 평소대로 계속 작동합니다. 하지만 신뢰할 수 있는 액세스를 다시 활성화할 때까지 조직 내에서 새 디렉터리를 더 이상 공유할 수 없습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Directory Service의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **`disable`**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 AWS Directory Service의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

AWS Firewall Manager 및 AWS Organizations

AWS Firewall Manager는 조직의 AWS 계정과 애플리케이션 전반에서 방화벽 규칙과 기타 보호 기능을 중앙에서 구성하고 관리하는 데 사용하는 보안 관리 서비스입니다. Firewall Manager를 사용하면 AWS WAF 규칙을 롤아웃하고, AWS Shield Advanced 보호 기능을 생성하고, Amazon Virtual Private Cloud(Amazon VPC) 보안 그룹을 구성 및 감사하고, AWS Network Firewall을 배포할 수 있습니다. Firewall Manager를 사용하여 보호 기능을 한 번만 설정하고, 조직 내 모든 계정과 리소스에 자동으로 적용합니다. 새로운 리소스와 계정이 추가될 때도 같습니다. AWS Firewall Manager에 대한 자세한 내용은 AWS Firewall Manager개발자 안내서 단원을 참조하세요.

다음 정보는 AWS Firewall Manager와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Firewall Manager는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Firewall Manager와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForFMS`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Firewall Manager가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `fms.amazonaws.com`

Firewall Manager와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Firewall Manager 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Firewall Manager 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Firewall Manager가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Firewall Manager에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
>
> AWS Firewall Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

사용자의 AWS Organizations 관리 계정으로 로그인하여 조직 내 계정을 AWS Firewall Manager 관리자 계정으로 구성해야 합니다. 자세한 내용은 AWS Firewall Manager 개발자 안내서의 AWS Firewall Manager 관리자 계정 설정을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Firewall Manager의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Firewall Manager의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Firewall Manager를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

Firewall Manager와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Firewall Manager 또는 AWS Organizations 도구를 사용해 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Firewall Manager 콘솔 또는 도구를 사용하여 Organizations 통합을 비활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Firewall Manager가 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등의 필요한 정리를 수행합니다. AWS Firewall Manager에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.
>
> AWS Firewall Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Firewall Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

AWS Firewall Manager 개발자 안내서의 다른 계정을 AWS Firewall Manager 관리자 계정으로 지정에 설명된 지침에 따라 AWS Firewall Manager 관리자 계정을 변경하거나 해지합니다.

관리자 계정을 취소하려면 AWS Organizations 관리 계정으로 로그인하고 AWS Firewall Manager의 새 관리자 계정을 설정해야 합니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Firewall Manager의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.

4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 AWS Firewall Manager의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Firewall Manager를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: DisableAWSServiceAccess

Firewall Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Firewall Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Firewall Manager 관리와 조직 관리를 분리하는 데 도움을 줍니다.

> 최소 권한
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Firewall Manager에 대한 위임된 관리자로 구성할 수 있습니다.

멤버 계정을 조직의 Firewall Manager 관리자로 지정하는 방법에 대한 설명은 AWS Firewall Manager 개발자 안내서의 AWS Firewall Manager 관리자 계정 설정을 참조하세요.

Amazon GuardDuty와 AWS Organizations

Amazon GuardDuty는 AWS 환경 내에서 예상치 못한 잠재적으로 악의적인 무단 활동을 식별하기 위해 위협 인텔리전스 피드와 기계 학습을 사용하여 다양한 데이터 원본을 분석 및 처리하는 지속적 보안 모니터링 서비스입니다. 여기에는 권한 에스컬레이션, 노출된 자격 증명 사용, 악의적인 IP 주소, URL 또는 도메인과의 통신, Amazon Elastic Compute Cloud 인스턴스 및 컨테이너 워크로드에 존재하는 맬웨어 같은 문제가 포함될 수 있습니다.

Organizations를 사용하여 조직의 모든 계정에서 GuardDuty를 관리하면 GuardDuty 관리를 단순화할 수 있습니다.

자세한 내용은 Amazon GuardDuty 사용 설명서의 AWS Organizations로 GuardDuty 계정 관리를 참조하세요.

다음 정보는 Amazon GuardDuty와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이러한역할을 통해 GuardDuty는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다. GuardDuty와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 역할을 삭제할 수 있습니다.

- `AWSServiceRoleForAmazonGuardDuty` 서비스 연결 역할은 GuardDuty가 Organizations와 통합된 계정에 자동으로 생성됩니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 Organizations로 GuardDuty 계정 관리를 참조하세요.
- `AmazonGuardDutyMalwareProtectionServiceRolePolicy` 서비스 연결 역할은 GuardDuty Malware Protection이 활성화된 계정에 자동으로 생성됩니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 GuardDuty Malware Protection을 위한 서비스 연결 역할 권한을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

- `AWSServiceRoleForAmazonGuardDuty` 서비스 연결 역할에서 사용하는 `guardduty.amazonaws.com`.
- `malware-protection.guardduty.amazonaws.com` 서비스 연결 역할에서 사용하는 `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

GuardDuty와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Amazon GuardDuty로만 활성화할 수 있습니다.

멤버 계정을 조직의 GuardDuty 관리자로 지정하려면 먼저 Amazon GuardDuty에게 AWS Organizations에 대한 신뢰할 수 있는 액세스가 필요합니다. GuardDuty 콘솔을 사용해 위임된 관리자를 구성하는 경우 GuardDuty가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

그러나 AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 EnableAWSServiceAccess 작업을 명시적으로 호출하고 파라미터로 서비스 보안 주체를 제공해야 합니다. 그러면 EnableOrganizationAdminAccount를 호출해 GuardDuty 관리자 계정을 위임할 수 있습니다.

GuardDuty와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 Amazon GuardDuty를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

GuardDuty에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 GuardDuty에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 GuardDuty 관리와 조직 관리를 분리하는 데 도움을 줍니다.

> **최소 권한**
>
> 멤버 계정을 위임된 관리자로 지정하는 데 필요한 권한에 관한 내용은 Amazon GuardDuty 사용 설명서의 위임된 관리자를 지정하는 데 필요한 권한을 참조하세요.

멤버 계정을 GuardDuty에 대한 위임된 관리자로 지정하려면

위임된 관리자 지정 및 멤버 계정 추가(콘솔) 및 위임된 관리자 지정 및 멤버 계정 추가(API)를 참조하세요.

AWS Health 및 AWS Organizations

AWS Health 리소스 성과와 AWS 서비스 및 계정의 가용성에 대한 지속적인 가시성을 제공합니다. AWS Health AWS 리소스 및 서비스가 문제의 영향을 받거나 향후 변경 사항의 영향을 받을 때 이벤트를 제공합니다. 조직 보기를 활성화하면 조직의 관리 계정에 있는 사용자가 조직 내 모든 계정의 AWS Health 이벤트를 집계할 수 있습니다. 조직 보기에서는 기능이 활성화된 이후에 전달된 AWS Health 이벤트만 표시하고 90일 동안 보관합니다.

AWS Health 콘솔, AWS Command Line Interface (AWS CLI) 또는 AWS Health API를 사용하여 조직 보기를 활성화할 수 있습니다.

자세한 내용은 AWS Health 사용 설명서의 AWS Health 이벤트 집계를 참조하십시오.

다음 정보를 사용하여 AWS Health 통합할 수 있습니다. AWS Organizations

통합을 위한 서비스 연결 역할

`AWSServiceRoleForHealth_Organizations`서비스 연결 역할을 사용하면 AWS Health 조직의 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다.

이 역할은 EnableHealthServiceAccessForOrganizationAPI 작업을 호출하여 신뢰할 수 있는 액세스를 활성화하면 조직의 관리 계정에 자동으로 생성됩니다. 그렇지 않으면 IAM 사용 설명서의 서비스 연결 역할 생성에 설명된 대로 AWS Health 콘솔, API 또는 CLI를 사용하여 역할을 생성하십시오.

Organizations 간의 AWS Health 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 구성원 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. 에서 사용하는 서비스 연결 역할은 다음 서비스 주체에게 액세스 AWS Health 권한을 부여합니다.

- `health.amazonaws.com`

AWS Health와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

에 대한 AWS Health조직 보기 기능을 활성화하면 신뢰할 수 있는 액세스도 자동으로 활성화됩니다.

AWS Health 콘솔이나 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다. AWS Organizations

> **Important**
>
> 가능하면 AWS Health 콘솔이나 도구를 사용하여 Organizations와 통합하는 것이 좋습니다. 이를 통해 서비스에 필요한 리소스를 만드는 등 필요한 모든 구성을 AWS Health 수행할 수 있습니다. AWS Health에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
> AWS Health 콘솔이나 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면 이 단계를 완료할 필요가 없습니다.

AWS Health 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Health 및 다음 옵션 중 하나를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

- AWS Health 콘솔을 사용하십시오. 자세한 내용은 AWS Health 사용 설명서의 조직 보기(콘솔)을 참조하세요.
- AWS CLI를 사용합니다. 자세한 내용은 AWS Health 사용 설명서의 조직 보기(CLI)를 참조하세요.
- EnableHealthServiceAccessForOrganization API 작업을 호출합니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Health 서비스로 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: 활성화 AWSServiceAccess

AWS Health와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

조직 보기 기능을 비활성화하면 조직의 다른 모든 계정에 대한 이벤트 집계가 AWS Health 중지됩니다. 또한 신뢰할 수 있는 액세스도 자동으로 비활성화됩니다.

AWS Health 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 가능하면 AWS Health 콘솔이나 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등 필요한 정리 AWS Health 작업을 수행할 수 있습니다. AWS Health에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.
> AWS Health 콘솔이나 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 이 단계를 완료할 필요가 없습니다.

AWS Health 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

다음 옵션 중 하나를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

- AWS Health 콘솔 사용. 자세한 내용은 AWS Health 사용 설명서의 조직 보기 비활성화(콘솔)를 참조하세요.
- AWS CLI를 사용합니다. 자세한 내용은 AWS Health 사용 설명서의 조직 보기 비활성화(CLI)를 참조하세요.
- DisableHealthServiceAccessForOrganization API 작업을 호출합니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 AWS Health 서비스로 사용하지 않도록 설정할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 비활성화 AWSServiceAccess

위임된 관리자 계정 활성화 AWS Health

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 AWS Health 에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 AWS Health관리와 조직 관리를 분리하는 데 도움이 됩니다.

멤버 계정을 AWS Health에 대한 위임된 관리자로 지정하려면

조직 보기에 대한 위임된 관리자 등록 참조

AWS Health에 대한 위임된 관리자 제거

조직 보기에서 위임된 관리자 제거 참조

Amazon Inspector 및 AWS Organizations

Amazon Inspector는 Amazon EC2 및 컨테이너 워크로드에서 소프트웨어 취약성 및 의도하지 않은 네트워크 노출을 지속적으로 스캔하는 자동화된 취약성 관리 서비스입니다.

Amazon Inspector에 관리자 계정을 위임하기만 하면 Amazon Inspector를 사용하여 AWS Organizations를 통해 연결된 여러 계정을 관리할 수 있습니다. 위임된 관리자는 조직의 Amazon Inspector를 관리하며 조직을 대신하여 다음과 같은 작업을 수행할 수 있는 특별 권한을 부여받습니다.

- 멤버 계정에 대한 스캔 활성화 또는 비활성화
- 전체 조직의 집계된 결과 데이터 보기
- 억제 규칙 생성 및 관리

자세한 내용은 Amazon Inspector 사용 설명서의 AWS Organizations로 여러 계정 관리를 참조하세요.

다음 정보는 Amazon Inspector와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Amazon Inspector는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Amazon Inspector와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForAmazonInspector2`

자세한 내용은 Amazon Inspector 사용 설명서의 Amazon Inspector에 대한 서비스 연결 역할 사용을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Amazon Inspector가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `inspector2.amazonaws.com`

Amazon Inspector에서 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

조직의 이 서비스에 대한 위임된 관리자로 멤버 계정을 지정하려면 Amazon Inspector에 먼저 AWS Organizations에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

Amazon Inspector에 대해 위임된 관리자를 지정하면 조직의 Amazon Inspector에 대해 신뢰할 수 있는 액세스가 자동으로 활성화됩니다.

그러나 AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 `EnableAWSServiceAccess` 작업을 명시적으로 호출하고 파라미터로 서비스 보안 주체를 제공해야 합니다. 그런 다음 `EnableDelegatedAdminAccount`를 호출하여 Inspector 관리자 계정을 위임할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

다음 명령을 실행하면 Organizations에서 신뢰할 수 있는 서비스로 Amazon Inspector를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

> **Note**
>
> `EnableAWSServiceAccess` API를 사용 중인 경우 `EnableDelegatedAdminAccount`를 호출하여 Inspector 관리자 계정도 위임해야 합니다.

Amazon Inspector에서 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 Amazon Inspector에서 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations에서 신뢰할 수 있는 서비스로 Amazon Inspector를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Amazon Inspector에 대한 위임된 관리자 계정 활성화

Amazon Inspector를 사용하면 AWS Organizations 서비스에서 위임된 관리자를 사용하여 조직의 여러 계정을 관리할 수 있습니다.

AWS Organizations 관리 계정이 조직 내 계정을 Amazon Inspector의 위임된 관리자 계정으로 지정합니다. 위임된 관리자는 조직의 Amazon Inspector를 관리하며 조직을 대신하여 멤버 계정에 대한 스캔 활성화 또는 비활성화, 전체 조직의 집계된 결과 데이터 보기, 억제 규칙 생성 및 관리와 같은 작업을 수행할 수 있는 특별 권한을 부여받습니다.

위임된 관리자가 조직 계정을 관리하는 방법에 대한 자세한 내용은 Amazon Inspector 사용 설명서에서 관리자 계정과 멤버 계정 간의 관계 이해를 참조하세요.

조직 관리 계정의 관리자만 Amazon Inspector에 대해 위임된 관리자를 구성할 수 있습니다.

Amazon Inspector 콘솔이나 API에서 또는 Organizations CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 지정할 수 있습니다.

> 최소 권한
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Amazon Inspector에 대한 위임된 관리자로 구성할 수 있습니다

Amazon Inspector 콘솔을 사용하여 위임된 관리자를 구성하려면 Amazon Inspector 사용 설명서에서 1단계: Amazon Inspector - 다중 계정 환경 활성화를 참조하세요.

> Note
>
> Amazon Inspector를 사용하는 각 리전의 `inspector2:enableDelegatedAdminAccount`에 연락해야 합니다.

AWS CLI, AWS API

AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체 `account.amazonaws.com`을 파라미터로 식별합니다.

Amazon Inspector에 대해 위임된 관리자를 비활성화

AWS Organizations 관리 계정의 관리자만 조직에서 위임된 관리자 계정을 제거할 수 있습니다.

Amazon Inspector 콘솔이나 API에서 또는 Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. Amazon Inspector 콘솔을 사용하여 위임된 관리자를 제거하려면 Amazon Inspector 사용 설명서에서 위임된 관리자 제거를 참조하세요.

AWS License Manager 및 AWS Organizations

AWS License Manager는 소프트웨어 공급업체 라이선스를 클라우드로 가져오는 프로세스를 간소화합니다. AWS에서 클라우드 인프라를 구축할 때 BYOL(bring-your-own-license, 기존 보유 라이선스 사용) 기회를 이용하면, 즉 기존 라이선스 인벤토리를 클라우드 리소스와 함께 사용할 목적으로 용도 변경하면 비용을 절감할 수 있습니다. 라이선스 소비에 대한 역할 기반 제어를 이용하면, 관리자는 신규 및 기존 클라우드 배포에 하드 또는 소프트 제한을 설정해 비호환 서버 사용을 사전에 차단할 수 있습니다.

License Manager에 관한 자세한 내용은 License Manager 사용 설명서를 참조하세요.

AWS Organizations(으)로 License Manager에 연결하면 다음과 같은 작업을 할 수 있습니다.

- 조직 전체의 컴퓨팅 리소스에 대한 교차 계정 발견을 활성화할 수 있습니다.
- AWS에 보유해 실행하는 상용 Linux 구독을 확인하고 관리할 수 있습니다. 자세한 내용은 AWS License Manager의 Linux 구독을 참조하세요.

다음 정보는 AWS License Manager를 AWS Organizations와 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 License Manager는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

License Manager와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 역할을 삭제하거나 수정할 수 있습니다.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

자세한 내용은 License Manager—관리 계정 역할, License Manager—멤버 계정 역할, License Manager—Linux 구독 역할을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. License Manager가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

License Manager와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스는 AWS License Manager로만 활성화할 수 있습니다.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

License Manager와 상호 신뢰할 수 있는 액세스를 활성화하려면

AWS Organizations 관리 계정을 사용해 License Manager 콘솔에 로그인하고 License Manager 계정과 연결해야 합니다. 자세한 내용은 AWS License Manager 설정을 참조하세요.

License Manager와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS License Manager를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-manager.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

  신뢰할 수 있는 액세스 비활성화:

  ```
  $  aws organizations disable-aws-service-access \
      --service-principal license-manager-linux-subscriptions.amazonaws.com
  ```

- AWS API: DisableAWSServiceAccess

License Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 License Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 License Manager 관리와 조직 관리를 분리하는 데 도움을 줍니다.

멤버 계정을 License Manager에 대한 관리자로 지정하려면 License Manager 사용 설명서의 위임된 관리자 등록에 설명된 단계를 따릅니다.

Amazon Macie와 AWS Organizations

Amazon Macie는 기계 학습과 패턴 일치를 사용하여 Amazon Simple Storage Service(Amazon S3)에서 민감한 데이터를 검색, 모니터링, 보호하는 완전관리형 데이터 보안 및 데이터 개인 정보 보호 서비스입니다. Macie는 개인 식별 정보(PII) 및 지적 재산권과 같은 민감한 데이터의 검색을 자동화하여 조직이 Amazon S3에 저장하는 데이터를 더 잘 이해할 수 있도록 합니다.

자세한 내용은 Amazon Macie 사용 설명서의 AWS Organizations로 Amazon Macie 계정들 관리를 참조하세요.

다음 정보는 Amazon Macie와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 위임된 Macie 관리자 계정에 자동으로 생성됩니다. 이 역할을 통해 Macie는 조직의 계정에 대해 지원되는 작업을 수행할 수 있습니다.

Macie와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제할 수 있습니다.

- `AWSServiceRoleRorAmazonMacie`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Macie가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `macie.amazonaws.com`

Macie와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

Amazon Macie 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 Amazon Macie 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 Amazon Macie가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. Amazon Macie에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
> Amazon Macie 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Macie 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

멤버 계정을 조직의 Macie 관리자로 지정하려면 먼저 Amazon Macie에게 AWS Organizations에 대한 신뢰할 수 있는 액세스가 필요합니다. Macie 관리 콘솔을 사용해 위임된 관리자를 구성하는 경우 Macie가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

자세한 내용은 Amazon Macie 사용 설명서의 Amazon Macie에서 조직 통합 및 구성을 참조하십시오.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon Macie를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal macie.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

Macie에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Macie에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Macie 관리와 조직 관리를 분리하는 데 도움을 줍니다.

> **최소 권한**
>
> 다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Macie에 대한 위임된 관리자로 구성할 수 있습니다.
>
> - `organizations:EnableAWSServiceAccess`
> - `macie:EnableOrganizationAdminAccount`

멤버 계정을 Macie에 대한 위임된 관리자로 지정하려면

멤버 계정을 조직의 Macie 관리자로 지정하려면 먼저 Amazon Macie에게 AWS Organizations에 대한 신뢰할 수 있는 액세스가 필요합니다. Macie 관리 콘솔을 사용해 위임된 관리자를 구성하는 경우 Macie가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

자세한 내용은 https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin 섹션을 참조하세요.

AWS Marketplace 및 AWS Organizations

AWS Marketplace는 솔루션을 구축하고 비즈니스를 운영하는 데 필요한 타사 소프트웨어, 데이터, 서비스를 찾아 구매, 배포 및 관리까지 할 수 있도록 큐레이션 프로세스를 거친 디지털 카탈로그입니다.

AWS Marketplace는 AWS License Manager를 사용해 AWS Marketplace에서의 구매에 대해 라이선스를 생성하고 관리합니다. 조직의 다른 계정과 라이선스를 공유(액세스 권한을 부여)하면 AWS Marketplace가 해당 계정에 대해 새 라이선스를 생성하고 관리합니다.

자세한 내용은 AWS Marketplace 구매자 설명서의 AWS Marketplace에 대한 서비스 연결 역할을 참조하세요.

다음 정보는 AWS Marketplace와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AWS Marketplace는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS Marketplace와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForMarketplaceLicenseManagement`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. AWS Marketplace가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `license-management.marketplace.amazonaws.com`

AWS Marketplace와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Marketplace 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Marketplace 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Marketplace가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Marketplace에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
> AWS Marketplace 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

AWS Marketplace 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Marketplace 구매자 가이드에서 AWS Marketplace에 대한 서비스 연결 역할 생성을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Marketplace의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Marketplace의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Marketplace를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

AWS Marketplace와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Marketplace를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: DisableAWSServiceAccess

AWS Marketplace 프라이빗 마켓플레이스 및 AWS Organizations

AWS Marketplace 솔루션을 구축하고 비즈니스를 운영하는 데 필요한 타사 소프트웨어, 데이터 및 서비스를 검색, 구매, 배포 및 관리하는 데 사용할 수 있는 엄선된 디지털 카탈로그입니다. 프라이빗 마켓플레이스는 에서 AWS Marketplace사용할 수 있는 광범위한 제품 카탈로그와 해당 제품에 대한 세밀한 관리를 제공합니다.

AWS Marketplace Private Marketplace를 사용하면 조직 전체, 하나 이상의 OU 또는 조직 내 하나 이상의 계정과 관련된 여러 개의 비공개 마켓플레이스 경험을 만들 수 있으며 각 계정에는 승인된 제품 세트가 있습니다. 또한 AWS 관리자는 회사 또는 팀의 로고, 메시지 및 색 구성표를 사용하여 각 비공개 마켓플레이스 환경에 회사 브랜딩을 적용할 수 있습니다.

자세한 내용은 AWS Marketplace 구매자 안내서의 역할을 사용하여 Private Marketplace 구성을 참조하십시오. AWS Marketplace

다음 정보를 사용하면 AWS Marketplace Private Marketplace와 통합하는 데 도움이 AWS Organizations됩니다.

통합 활성화 시 서비스 연결 역할 생성

Private AWS Marketplace Marketplace 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하면 조직의 관리 계정에 다음과 같은 서비스 연결 역할이 자동으로 생성됩니다. 이 역할을 통해 Private Marketplace는 조직의 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다. AWS Marketplace Private Marketplace와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하고 조직의 모든 프라이빗 마켓플레이스 경험을 분리한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Organizations 콘솔, CLI 또는 SDK에서 직접 신뢰할 수 있는 액세스를 활성화하는 경우 서비스 연결 역할은 자동으로 생성되지 않습니다.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Private Marketplace에서 사용하는 서비스 연결 역할은 다음 서비스 주체에 대한 액세스 권한을 부여합니다.

- `private-marketplace.marketplace.amazonaws.com`

Private Marketplace를 통한 신뢰할 수 있는 액세스 지원

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Marketplace Private Marketplace 콘솔 또는 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 AWS Organizations 수 있습니다.

> **Important**
>
> 가능하면 AWS Marketplace Private Marketplace 콘솔 또는 도구를 사용하여 Organizations와 통합하는 것이 좋습니다. 이렇게 하면 AWS Marketplace Private Marketplace에서 필요한 모

든 구성 (예: 서비스에 필요한 리소스 생성) 을 수행할 수 있습니다. AWS Marketplace Private Marketplace에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행하십시오. 자세한 내용은 이 메모를 참조하십시오.
AWS Marketplace Private Marketplace 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우 이 단계를 완료할 필요가 없습니다.

Private Marketplace 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Marketplace 구매자 안내서의 프라이빗 마켓플레이스 시작하기를 참조하십시오.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 페이지에서 AWS Marketplace Private Marketplace의 행을 찾아 서비스 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. only의 관리자인 경우 AWS Marketplace Private Marketplace 관리자에게 이제 콘솔을 사용하여 해당 서비스를 사용할 수 있도록 설정할 수 있다고 알려주십시오 AWS Organizations. AWS Organizations

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

다음 명령을 실행하여 Organizations에서 AWS Marketplace Private Marketplace를 신뢰할 수 있는 서비스로 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal private-marketplace.marketplace.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 활성화 AWSServiceAccess

Private Marketplace를 통한 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하여 Organizations에서 AWS Marketplace Private Marketplace를 신뢰할 수 있는 서비스로 사용하지 않도록 설정할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: 비활성화 AWSServiceAccess

Private Marketplace에서 위임된 관리자 계정 활성화

관리 계정 관리자는 Private Marketplace 관리 권한을 위임된 관리자라고 하는 지정된 구성원 계정에 위임할 수 있습니다. 계정을 프라이빗 마켓플레이스의 위임 관리자로 등록하려면 관리 계정 관리자는 신뢰할 수 있는 액세스와 서비스 연결 역할이 활성화되어 있는지 확인하고, 새 관리자 등록을 선택하고, 12자리 AWS 계정 번호를 제공하고, 제출을 선택해야 합니다.

관리 계정 및 위임된 관리자 계정은 경험 생성, 브랜드 설정 업데이트, 대상 연결 또는 연결 해제, 제품 추가 또는 제거, 보류 중인 요청 승인 또는 거부와 같은 Private Marketplace 관리 작업을 수행할 수 있습니다.

Private Marketplace 콘솔을 사용하여 위임된 관리자를 구성하려면 AWS Marketplace 구매자 안내서의 비공개 마켓플레이스 생성 및 관리를 참조하십시오.

Organizations `RegisterDelegatedAdministrator` API를 사용하여 위임된 관리자를 구성할 수도 있습니다. 자세한 내용은 RegisterDelegatedAdministratorOrganizations 명령 참조서를 참조하십시오.

Private Marketplace의 위임 관리자 비활성화

조직 관리 계정의 관리자만 Private Marketplace에 위임된 관리자를 구성할 수 있습니다.

프라이빗 마켓플레이스 콘솔 또는 API를 사용하거나 Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

Private Marketplace 콘솔을 사용하여 위임된 관리자 Private Marketplace 계정을 비활성화하려면 AWS Marketplace 구매자 안내서의 비공개 마켓플레이스 생성 및 관리를 참조하십시오.

AWS 네트워크 관리자 및 AWS Organizations

Network Manager를 사용하면 AWS 계정, 지역 및 온프레미스 위치에서 AWS Cloud WAN 코어 네트워크와 AWS Transit Gateway 네트워크를 중앙에서 관리할 수 있습니다. 다중 계정 지원을 통해 모든 계정에 대해 단일 글로벌 네트워크를 생성하고 Network Manager 콘솔을 사용하여 여러 계정의 전송 게이트웨이를 글로벌 네트워크에 등록할 수 있습니다. AWS

Network Manager와 Organizations 사이의 신뢰할 수 있는 액세스가 활성화되면 멤버 계정에 배포된 서비스 연결 역할을 등록된 위임된 관리자와 관리 계정에서 활용하여 글로벌 네트워크에 연결된 리소스를 설명할 수 있습니다. 등록된 위임된 관리자와 관리 계정에서는 Network Manager 콘솔에서 멤버 계정에 배포된 사용자 정의 IAM 역할을 맡을 수 있습니다(다중 계정 모니터링 및 이벤트 처리의 경우

CloudWatch-CrossAccountSharingRole, 다중 계정 리소스를 보고 관리하는 콘솔 전환 역할 액세스의 경우 IAMRoleForAWSNetworkManagerCrossAccountResourceAccess).

> **Important**
>
> - 다중 계정 설정(신뢰할 수 있는 액세스 활성화/비활성화 및 위임된 관리자 등록/등록 취소)을 관리하려면 Network Manager 콘솔을 사용하는 것이 좋습니다. 콘솔에서 이러한 설정을 관리하면 필요한 모든 서비스 연결 역할과 사용자 정의 IAM 역할이 다중 계정 액세스에 필요한 멤버 계정에 자동으로 배포되고 관리됩니다.
> - Network Manager 콘솔에서 Network Manager에 대한 신뢰할 수 있는 액세스를 활성화하면 콘솔에서 서비스도 AWS CloudFormation StackSets 활성화됩니다. Network Manager는 다중 계정 관리에 필요한 사용자 지정 IAM 역할을 배포하는 StackSets 데 사용합니다.

Organizations와 Network Manager 통합에 대한 자세한 내용은 Amazon VPC 사용 설명서의 AWS Organizations로 Network Manager에서 여러 계정 관리를 참조하세요.

다음 정보를 사용하면 AWS Network Manager를 통합하는 데 도움이 됩니다. AWS Organizations

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 나열된 조직 계정에 자동으로 생성됩니다. 조직의 계정 내에서 지원되는 작업을 Network Manager에서 이러한 역할을 통해 수행할 수 있습니다. 신뢰할 수 있는 액세스를 비활성화하는 경우 Network Manager에서는 조직의 계정에서 이러한 역할을 삭제하지 않습니다. IAM 콘솔을 사용하여 해당 역할을 수동으로 삭제할 수 있습니다.

관리 계정

- AWSServiceRoleForNetworkManager
- AWSServiceRoleForCloudFormationStackSetsOrgAdmin
- AWSServiceRoleForCloudWatchCrossAccount

멤버 계정

- AWSServiceRoleForNetworkManager
- AWSServiceRoleForCloudFormationStackSetsOrgMember

멤버 계정을 위임된 관리자로 등록하면 위임된 관리자 계정에 다음과 같은 추가 역할이 자동으로 생성됩니다.

- `AWSServiceRoleForCloudWatchCrossAccount`

서비스 연결 역할이 사용하는 서비스 보안 주체

서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다.

- `AWSServiceRoleForNetworkManager service-linked` 역할의 경우, `networkmanager.amazonaws.com`이 액세스 권한이 있는 유일한 서비스 보안 주체입니다.
- `AWSServiceRoleForCloudFormationStackSetsOrgMember` 서비스 연결 역할의 경우, `member.org.stacksets.cloudformation.amazonaws.com`이 액세스 권한이 있는 유일한 서비스 보안 주체입니다.
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin` 서비스 연결 역할의 경우, `stacksets.cloudformation.amazonaws.com`이 액세스 권한이 있는 유일한 서비스 보안 주체입니다.
- `AWSServiceRoleForCloudWatchCrossAccount` 서비스 연결 역할의 경우, `cloudwatch-crossaccount.amazonaws.com`이 액세스 권한이 있는 유일한 서비스 보안 주체입니다.

이러한 역할을 삭제하면 Network Manager의 다중 계정 기능이 손상됩니다.

Network Manager와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

Organizations 관리 계정의 관리자만 다른 AWS 서비스를 통해 신뢰할 수 있는 액세스를 활성화할 수 있는 권한을 갖습니다. 권한 문제를 방지하려면 Network Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화해야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 AWS Organizations로 Network Manager에서 여러 계정 관리를 참조하세요.

Network Manager와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

Organizations 관리 계정의 관리자만 다른 AWS 서비스에 대한 신뢰할 수 있는 액세스를 비활성화할 수 있는 권한을 갖습니다.

> **Important**
>
> 신뢰할 수 있는 액세스를 비활성화하려면 Network Manager 콘솔을 사용하는 것이 좋습니다. API 또는 AWS CloudFormation 콘솔을 사용하는 AWS CLI등 다른 방법으로 신뢰할 수 있는 액세스를 비활성화하면 배포된 AWS CloudFormation StackSets 사용자 지정 IAM 역할이 제대로 정리되지 않을 수 있습니다. 신뢰할 수 있는 서비스 액세스를 비활성화하려면 Network Manager 콘솔에 로그인하세요.

Network Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Network Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Network Manager 관리와 조직 관리를 분리하는 데 도움이 됩니다.

조직에서 멤버 계정을 Network Manager의 위임된 관리자로 지정하는 방법에 관한 지침은 Amazon VPC 사용 설명서의 위임된 관리자 등록을 참조하세요.

아마존 Q 개발자 (아마존 Q) 및 AWS Organizations

Amazon Q Developer는 애플리케이션을 이해, 구축, 확장 및 운영하는 데 도움이 되는 생성적 인공 지능 (AI) 기반 대화형 도우미입니다. AWS Amazon Q의 유료 구독 버전에는 Organizations 통합이 필요합니다. 자세한 내용은 Amazon Q 사용 설명서의 계정, IAM ID 센터 및 조직 설정을 참조하십시오.

다음 정보를 사용하면 Amazon Q Developer와 통합하는 데 도움이 AWS Organizations됩니다.

서비스 연결 역할

`AWSServiceRoleForAmazonQDeveloper`서비스 연결 역할을 통해 Amazon Q는 조직의 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다. IAM 사용 설명서의 서비스 연결 역할 생성에 설명된 대로 Amazon Q 콘솔, API 또는 CLI를 사용하여 역할을 생성합니다.

Amazon Q와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 구성원 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Amazon Q에서 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Amazon Q에서 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `q.amazonaws.com`

Amazon Q를 통한 신뢰할 수 있는 액세스 지원

Amazon Q는 신뢰할 수 있는 액세스를 사용하여 Orgs 수준에서 만든 설정을 멤버 계정과 공유합니다. 예를 들어 Organizations 수준의 관리자가 Feature X를 활성화하면 Feature X를 동일한 조직의 모든 구성원 계정에서 사용할 수 있습니다. 자세한 내용은 Amazon Q Developer 사용 설명서의 조직 설정을 참조하십시오.

Amazon Q Developer만 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

Amazon Q 콘솔에서 Amazon Q에 대한 신뢰할 수 있는 액세스를 활성화하려면 Amazon Q 개발자 사용 설명서의 구독에 있는 지침을 따르십시오. 6단계에서 회원 계정과 설정 프로필 공유를 선택합니다.

Amazon Q를 통한 신뢰할 수 있는 액세스 비활성화

Amazon Q Developer 도구만 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Amazon Q에 대한 신뢰할 수 있는 액세스를 비활성화하려면 Amazon Q 콘솔에서 Amazon Q 개발자 사용 설명서의 구독에 있는 지침을 따르십시오. 6단계에서 회원 계정과 설정 프로필 공유를 선택 취소합니다.

AWS Resource Access Manager 및 AWS Organizations

AWS Resource Access Manager(AWS RAM)을 사용하면 다른 AWS 계정 계정으로 소유한 AWS 리소스를 지정하여 공유할 수 있습니다. 이 서비스는 서로 다른 유형의 AWS 리소스를 여러 계정에서 공유할 수 있는 일관된 환경을 제공하는 중앙 관리형 서비스입니다.

AWS RAM에 대한 자세한 내용은 AWS RAM 사용 설명서를 참조하세요.

다음 정보는 AWS Resource Access Manager와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AWS RAM는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS RAM와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForResourceAccessManager`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. AWS RAM가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `ram.amazonaws.com`

AWS RAM와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Resource Access Manager 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Resource Access Manager 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Resource Access Manager가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Resource Access Manager에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
>
> AWS Resource Access Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

AWS RAM 콘솔 또는 CLI를 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS RAM 사용 설명서의 AWS Organizations를 사용하여 공유 사용을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Resource Access Manager의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Resource Access Manager의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Resource Access Manager를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

AWS RAM와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Resource Access Manager 또는 AWS Organizations 도구를 사용해 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Resource Access Manager 콘솔 또는 도구를 사용하여 Organizations 통합을 비활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Resource Access Manager가 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등의 필요한 정리를 수행합니다. AWS Resource Access Manager에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.
>
> AWS Resource Access Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

AWS Resource Access Manager 콘솔 또는 CLI를 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

AWS RAM 사용 설명서의 AWS Organizations를 사용하여 공유 사용을 참조하세요.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Resource Access Manager의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **`disable`**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.

5. 본인이 AWS Organizations에서만 관리자인 경우 AWS Resource Access Manager의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Resource Access Manager를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: DisableAWSServiceAccess

AWS 리소스 탐색기 및 AWS Organizations

AWS 리소스 탐색기은(는) 리소스 검색 및 검색 서비스입니다. 리소스 탐색기를 사용하면 인터넷 검색 엔진과 유사한 환경을 사용하여 Amazon Elastic Compute Cloud 인스턴스, Amazon Kinesis Data Streams 또는 Amazon DynamoDB 테이블과 같은 리소스를 탐색할 수 있습니다. 이름, 태그, ID와 같은 리소스 메타데이터를 사용하여 리소스를 검색할 수 있습니다. Resource Explorer는 계정의 여러 AWS 리전에서 작동하여 지역 간 워크로드를 단순화합니다.

Resource Explorer와 AWS Organizations을(를) 통합하면 평가 범위 안에 조직의 여러 AWS 계정을(를) 포함시켜 더 광범위한 소스에서 증거를 수집할 수 있습니다.

다음 정보는 AWS 리소스 탐색기를 AWS Organizations와 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Resource Explorer은(는) 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Resource Explorer와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Resource Explorer가 이 역할을 사용하는 방식에 대한 자세한 내용은 AWS 리소스 탐색기 사용 설명서의 서비스 연결 역할 사용을 참조하세요.

- `AWSServiceRoleForResourceExplorer`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Resource Explorer이 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `resource-explorer-2.amazonaws.com`

AWS 리소스 탐색기에서 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

멤버 계정을 조직의 위임된 관리자로 지정하려면 먼저 Resource Explorer에게 AWS Organizations에 대한 신뢰할 수 있는 액세스가 필요합니다.

Resource Explorer 콘솔 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다. 가능하면 항상 Resource Explorer 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS 리소스 탐색기가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다.

Resource Explorer 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하는 방법

신뢰할 수 있는 액세스를 활성화하는 방법에 대한 지침은 AWS 리소스 탐색기 사용 설명서의 Resource Explorer를 사용하기 위한 사전 요구 사항을 참조하십시오.

> **Note**
>
> AWS 리소스 탐색기 콘솔을 사용해 위임된 관리자를 구성하는 경우 AWS 리소스 탐색기가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS 리소스 탐색기를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

Resource Explorer에서 신뢰할 수 있는 액세스를 비활성화하는 방법

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 AWS 리소스 탐색기와 상호 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS 리소스 탐색기 또는 AWS Organizations 도구를 사용해 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS 리소스 탐색기 콘솔 또는 도구를 사용하여 Organizations 통합을 비활성화할 것을 적극 권장합니다. 이렇게 하면 AWS 리소스 탐색기가 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등의 필요한 정리를 수행합니다. AWS 리소스 탐색기에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.

AWS 리소스 탐색기 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS 리소스 탐색기를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Resource Explorer에 대한 위임된 관리자 계정 활성화

위임된 관리자 계정을 사용하여 다중 계정 리소스 보기를 만들고 조직 단위 또는 전체 조직으로 범위를 지정할 수 있습니다. 리소스 공유를 생성하여 AWS Resource Access Manager을(를) 통해 조직의 모든 계정과 다중 계정 보기를 공유할 수 있습니다.

최소 권한

다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Resource Explorer에 대한 위임된 관리자로 구성할 수 있습니다. `resource-explorer:RegisterAccount`

Resource Explorer에 대한 위임된 관리자 계정 활성화에 대한 설명은 AWS 리소스 탐색기 사용 설명서의 설정을 참조하세요.

AWS 리소스 탐색기 콘솔을 사용해 위임된 관리자를 구성하는 경우 Resource Explorer가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

AWS CLI, AWS API

AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 `resource-explorer-2.amazonaws.com`를 파라미터로 식별합니다.

Resource Explorer에 대해 위임된 관리자를 비활성화

Organizations 관리 계정 또는 Resource Explorer의 위임된 관리자 계정의 관리자만 Resource Explorer의 위임된 관리자를 제거할 수 있습니다. 신뢰할 수 있는 액세스는 Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용해 비활성화할 수 있습니다.

AWS Security Hub 및 AWS Organizations

AWS Security Hub 보안 상태를 포괄적으로 파악하고 보안 업계 표준 AWS 및 모범 사례와 비교하여 환경을 점검할 수 있도록 지원합니다.

Security Hub는 사용자 AWS 계정, 사용하는 AWS 서비스 및 지원되는 타사 파트너 제품 전반에서 보안 데이터를 수집합니다. 이 서비스는 보안 추세를 분석하고 우선 순위가 가장 높은 보안 문제를 식별하는 데 도움을 줍니다.

Security Hub를 둘 다 사용하는 경우 새 계정을 포함하여 모든 계정에 대해 Security Hub를 자동으로 활성화할 수 있습니다. AWS Organizations 이렇게 하면 Security Hub 검사 및 결과의 적용 범위가 늘어나 전반적인 보안 상태를 보다 포괄적이고 정확하게 파악할 수 있습니다.

Security Hub에 대한 자세한 내용은 AWS Security Hub 사용 설명서를 참조하세요.

다음 정보를 활용하면 AWS Security Hub 통합하는 데 도움이 AWS Organizations됩니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Security Hub는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Security Hub와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForSecurityHub`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Security Hub가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `securityhub.amazonaws.com`

Security Hub와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

Security Hub에 대해 위임된 관리자를 지정하면 Security Hub가 조직의 Security Hub에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

Security Hub에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Security Hub에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Security Hub 관리와 조직 관리를 분리하는 데 도움을 줍니다.

자세한 내용은 AWS Security Hub 사용 설명서의 Security Hub 관리자 계정 지정을 참조하세요.

멤버 계정을 Security Hub에 대한 위임된 관리자로 지정하려면

1. Organizations의 관리 계정을 사용하여 로그인합니다.

2. 다음 중 하나를 수행합니다.

   - 관리 계정에 Security Hub가 활성화되어 있지 않으면 Security Hub 콘솔에서 Security Hub로 이동(Go to Security Hub)을 선택합니다.
   - 관리 계정에 Security Hub가 활성화되어 있는 경우 Security Hub 콘솔의 일반에서 설정을 선택합니다.

3. 위임된 관리자(Delegated Administrator)에 계정 ID를 입력합니다.

Amazon S3 Storage Lens와 AWS Organizations

Amazon S3 Storage Lens에 신뢰할 수 있는 액세스 권한을 조직에 제공하면 조직 AWS 계정 내 모든 영역에서 지표를 수집하고 집계할 수 있습니다. 이를 위해 S3 Storage Lens는 조직에 속한 계정 목록에 액세스하여 모든 계정의 스토리지, 사용량 및 활동 지표를 수집하고 분석합니다.

자세한 내용은 Amazon S3 Storage Lens 사용 설명서의 Amazon S3 Storage Lens에 대한 서비스 연결 역할 사용을 참조하세요.

다음 정보를 사용하면 Amazon S3 스토리지 렌즈를 통합하는 데 도움이 AWS Organizations됩니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하고 Storange Lens 구성이 조직에 적용되면 다음 서비스 연결 역할이 조직의 위임된 관리자 계정에 자동으로 생성됩니다. 이 역할을 통해 Amazon S3 Storage Lens는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Amazon S3 Storage Lens와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForS3StorageLens`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Amazon S3 Storage Lens가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `storage-lens.s3.amazonaws.com`

Amazon S3 Storage Lens와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

Amazon S3 Storage Lens 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 Amazon S3 Storage Lens 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 Amazon S3 Storage Lens가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. Amazon S3 Storage Lens에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 이 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
>
> Amazon S3 Storage Lens 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Amazon S3 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

Amazon 심플 스토리지 서비스 사용 설명서의 S3 Storage Lens에 대한 신뢰할 수 있는 액세스 활성화를 참조하십시오.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 Amazon S3 Storage Lens의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.

4. 전용 AWS Organizations관리자인 경우 Amazon S3 Storage Lens 관리자에게 이제 콘솔을 사용하여 해당 서비스를 사용할 수 있도록 설정할 수 있다고 알려주십시오 AWS Organizations.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon S3 Storage Lens를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: 활성화 AWSServiceAccess

Amazon S3 Storage Lens와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Amazon S3 Storage Lens 도구로만 비활성화할 수 있습니다.

Amazon S3 콘솔, AWS CLI 또는 AWS SDK를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Amazon S3 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

Amazon 심플 스토리지 서비스 사용 설명서의 S3 Storage Lens에 대한 신뢰할 수 있는 액세스 비활성화를 참조하십시오.

Amazon S3 Storage Lens에 대한 위임된 관리자 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Amazon S3 Storage Lens에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는

역할만 관리 작업을 수행할 수 있습니다. 이는 Amazon S3 Storage Lens 관리와 조직 관리를 분리하는 데 도움을 줍니다.

> **최소 권한**
>
> 다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Amazon S3 스토리지 렌즈에 대한 위임된 관리자로 구성할 수 있습니다.
> `organizations:RegisterDelegatedAdministrator`
> `organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens는 조직 내에서 위임된 관리자 계정을 최대 5개까지 지원합니다.

멤버 계정을 Amazon S3 Storage Lens에 대한 위임된 관리자로 지정하려면

Amazon S3 콘솔, AWS CLI 또는 AWS SDK를 사용하여 위임된 관리자를 등록할 수 있습니다. Amazon S3 콘솔을 사용하여 멤버 계정을 조직의 위임 관리자 계정으로 등록하려면 Amazon Simple Storage Service 사용 설명서의 S3 Storage Lens에 위임 관리자 등록을 참조하십시오.

Amazon S3 Storage Lens에 대한 위임된 관리자의 등록을 취소하려면

Amazon S3 콘솔, AWS CLI 또는 SDK를 사용하여 위임된 관리자의 등록을 취소할 수 있습니다. AWS Amazon S3 콘솔을 사용하여 위임된 관리자의 등록을 취소하려면 Amazon Simple Storage 서비스 사용 설명서의 S3 Storage Lens에 대한 위임 관리자 등록 취소를 참조하십시오.

Amazon Security Lake 및 AWS Organizations

Amazon Security Lake는 클라우드, 온프레미스 및 사용자 지정 소스의 보안 데이터를 계정에 저장된 데이터 레이크로 중앙 집중화합니다. Organizations와 통합하면 계정 전체에서 로그와 이벤트를 수집하는 데이터 레이크를 생성할 수 있습니다. 자세한 내용은 Amazon Security Lake User Guide의 Managing multiple accounts with AWS Organizations를 참조하세요.

다음 정보를 사용하면 Amazon Security Lake와 통합하는 데 도움이 AWS Organizations됩니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Amazon Security Lake는 조직 내 조직 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Amazon Security Lake와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 구성원 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForSecurityLake`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Amazon Security Lake에서 사용하는 서비스 연결 역할은 다음 서비스 주체에 대한 액세스 권한을 부여합니다.

- `securitylake.amazonaws.com`

Amazon Security Lake를 통한 신뢰할 수 있는 액세스 지원

Security Lake와 상호 신뢰할 수 있는 액세스를 활성화하면 Security Lake가 조직 멤버십의 변경 사항에 자동으로 대응할 수 있습니다. 위임된 관리자는 모든 조직 계정의 지원되는 서비스에서 AWS 로그 수집을 활성화할 수 있습니다. 자세한 내용은 Amazon Security Lake User Guide의 Service-linked role for Amazon Security Lake를 참조하세요.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 페이지에서 Amazon Security Lake의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.

4. only AWS Organizations관리자인 경우 Amazon Security Lake 관리자에게 이제 콘솔을 사용하여 해당 서비스를 사용할 수 있도록 설정할 수 있다고 알려주십시오 AWS Organizations.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations에서 신뢰할 수 있는 서비스로 Amazon Security Lake를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: 활성화 AWSServiceAccess

Amazon Security Lake를 통한 신뢰할 수 있는 액세스 비활성화

Organizations 관리 계정의 관리자만 Amazon Security Lake를 통한 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나 Organizations AWS CLI 명령을 실행하거나 AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 페이지에서 Amazon Security Lake의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.

4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. only AWS Organizations관리자인 경우 Amazon Security Lake 관리자에게 이제 콘솔이나 도구를 사용하여 해당 서비스를 사용하지 않도록 설정할 수 있다고 알려주십시오 AWS Organizations.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations에서 신뢰할 수 있는 서비스로 Amazon Security Lake를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: 비활성화 AWSServiceAccess

아마존 시큐리티 레이크에 위임된 관리자 계정 활성화

Amazon Security Lake의 위임 관리자는 조직의 다른 계정을 구성원 계정으로 추가합니다. 위임된 관리자는 Amazon Security Lake를 활성화하고 멤버 계정에 대한 Amazon Security Lake 설정을 구성할 수 있습니다. 위임된 관리자는 Amazon Security Lake가 활성화된 모든 AWS 지역의 조직 전체에서 로그를 수집할 수 있습니다 (현재 사용 중인 지역 엔드포인트와 관계 없음).

위임된 관리자가 조직의 새 계정을 멤버로 자동 추가하도록 설정할 수도 있습니다. Amazon Security Lake의 위임 관리자는 관련 멤버 계정의 로그 및 이벤트에 액세스할 수 있습니다. 따라서 Amazon Security Lake를 설정하여 관련 회원 계정이 소유한 데이터를 수집할 수 있습니다. 연결된 멤버 계정이 소유한 데이터를 사용할 수 있는 권한을 구독자에게 부여할 수도 있습니다.

자세한 내용은 Amazon Security Lake User Guide의 Managing multiple accounts with AWS Organizations를 참조하세요.

최소 권한

조직 관리 계정의 관리자만 조직 내 Amazon Security Lake의 위임 관리자로 멤버 계정을 구성할 수 있습니다.

Amazon Security Lake 콘솔, Amazon Security Lake `CreateDatalakeDelegatedAdmin` API 작업 또는 `create-datalake-delegated-admin` CLI 명령을 사용하여 위임된 관리자 계정을 지정할 수 있습니다. Organizations `RegisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용할 수도 있습니다. Amazon Security Lake에서 위임된 관리자 계정을 활성화하는 방법에 대한 지침은 Amazon Security Lake 사용 설명서의 위임된 Security Lake 관리자 지정 및 구성원 계정 추가를 참조하십시오.

AWS CLI, AWS API

AWS CLI 또는 SDK 중 AWS 하나를 사용하여 위임된 관리자 계정을 구성하려는 경우 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \ --service-principal securitylake.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 오퍼레이션과 회원 계정의 ID 번호를 호출하고 계정 서비스 주체를 `account.amazonaws.com` 매개변수로 식별합니다.

Amazon Security Lake의 위임 관리자 비활성화

Organizations 관리 계정 또는 Amazon Security Lake의 위임 관리자 계정의 관리자만 조직에서 위임된 관리자 계정을 제거할 수 있습니다.

Amazon Security Lake `DeleteDatalakeDelegatedAdmin` API 작업, CLI 명령을 사용하거나 `DeregisterDelegatedAdministrator` Organizations의 `delete-datalake-delegated-admin` CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 제거할 수 있습니다. Amazon Security Lake를 사용하여 위임된 관리자를 제거하려면 Amazon Security Lake 사용 설명서의 Amazon Security Lake 위임 관리자 제거를 참조하십시오.

AWS Service Catalog 및 AWS Organizations

Service Catalog를 사용하면 AWS에서 사용이 승인된 IT 서비스 카탈로그를 생성하고 관리할 수 있습니다.

Service Catalog와 AWS Organizations를 통합할 경우 조직 전반의 포트폴리오 공유 및 제품 복사 작업이 간소화됩니다. Service Catalog 관리자는 포트폴리오를 공유하는 경우 AWS Organizations의 기존 조직을 참조할 수 있고 조직의 트리 구조에서 신뢰할 수 있는 조직구성단위(OU)와 포트폴리오를 공유할 수 있습니다. 따라서 포트폴리오 ID를 공유할 필요가 없고, 수신하는 계정은 포트폴리오를 가져올 때 포트폴리오 ID를 수동으로 참조하지 않아도 됩니다. 이 메커니즘을 통해 공유된 포트폴리오는 Service Catalog에서 관리자의 가져온 포트폴리오(Imported Portfolio) 보기에 공유 대상 계정으로 나열됩니다.

Service Catalog에 대한 자세한 내용은 Service Catalog 관리자 안내서를 참조하세요.

다음 정보는 AWS Service Catalog를 AWS Organizations와 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

AWS Service Catalog는 신뢰할 수 있는 액세스를 활성화하는 과정에서 서비스 연결 역할을 만들지 않습니다.

권한을 부여하는 데 사용되는 서비스 보안 주체

신뢰할 수 있는 액세스를 활성화하려면 다음 서비스 보안 주체를 지정해야 합니다.

- `servicecatalog.amazonaws.com`

Service Catalog와 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Service Catalog 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Service Catalog 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Service Catalog가 서비스에 필요한 리소스 생성

등 모든 필수 구성을 수행합니다. AWS Service Catalog에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오. AWS Service Catalog 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Service Catalog CLI 또는 AWS SDK를 사용하여 신뢰할 수 있는 액세스를 활성화하려면

다음 명령 또는 작업 중 하나를 호출합니다.

- AWS CLI: aws servicecatalog enable-aws-organizations-access
- AWS SDKs: AWSServiceCatalog::EnableAWSOrganizationsAccess

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Service Catalog의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Service Catalog의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Service Catalog를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal servicecatalog.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

Service Catalog와 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

Service Catalog를 사용하는 동안 AWS Organizations를 사용하여 신뢰할 수 있는 액세스를 비활성화하면, 현재 공유가 삭제되지는 않지만 조직에서 신규 공유를 생성할 수는 없습니다. 이 작업을 호출한 후 조직 구조가 변경되면, 현재 공유는 조직 구조와 동기화되지 않습니다.

AWS Service Catalog 또는 AWS Organizations 도구를 사용해 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Service Catalog 콘솔 또는 도구를 사용하여 Organizations 통합을 비활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Service Catalog가 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등의 필요한 정리를 수행합니다. AWS Service Catalog에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.
>
> AWS Service Catalog 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Service Catalog CLI 또는 AWS SDK를 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

다음 명령 또는 작업 중 하나를 호출합니다.

- AWS CLI: aws servicecatalog disable-aws-organizations-access

- AWS SDKs: DisableAWSOrganizationsAccess

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Service Catalog의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 AWS Service Catalog의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Service Catalog를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Service Quotas와 AWS Organizations

Service Quotas는 중앙 위치에서 할당량을 보고 관리할 수 있는 AWS 서비스입니다. 제한이라고도 하는 할당량은 AWS 계정의 리소스, 작업, 항목의 최대값입니다.

Service Quotas를 AWS Organizations와 연결하면 계정 생성 시 할당량 요청 템플릿을 만들어 할당량 증가를 자동으로 요청할 수 있습니다.

서비스 할당량에 대한 자세한 내용은 Service Quotas 사용 설명서를 참조하세요.

다음 정보는 Service Quotas와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Service Quotas는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Service Quotas와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForServiceQuotas`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Service Quotas가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `servicequotas.amazonaws.com`

Service Quotas와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Service Quotas로만 활성화할 수 있습니다.

Service Quotas 콘솔, AWS CLI 또는 SDK를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

- Service Quotas 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Organizations 관리 계정에 로그인한 후 Service Quotas 콘솔에서 템플릿을 구성합니다. 자세한 내용은 Service Quotas 사용 설명서의 Service Quotas 템플릿 사용을 참조하세요.

- Service Quotas AWS CLI 또는 SDK를 사용하여 신뢰할 수 있는 액세스를 활성화하려면

  다음 명령 또는 작업을 호출합니다.

  - AWS CLI: aws service-quotas associate-service-quota-template
  - AWS SDKs: AssociateServiceQuotaTemplate

AWS IAM Identity Center 및 AWS Organizations

AWS IAM Identity Center은 모든 AWS 계정 및 클라우드 애플리케이션에 대한 Single Sign-On(SSO) 서비스를 제공합니다. AWS Directory Service를 통해 Microsoft Active Directory와 연결하여 해당 디렉터리에 있는 사용자가 기존 Active Directory 사용자 이름 및 암호를 사용하여 개인화된 AWS 액세스 포털에 로그인할 수 있도록 합니다. 사용자는 AWS 액세스 포털에서 권한이 있는 모든 AWS 계정 및 클라우드 애플리케이션에 액세스할 수 있습니다.

IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서를 참조하세요.

다음 정보는 AWS IAM Identity Center를 AWS Organizations와 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 IAM Identity Center는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

IAM Identity Center와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForSSO`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. IAM Identity Center가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `sso.amazonaws.com`

IAM Identity Center와의 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS IAM Identity Center 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS IAM Identity Center 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS IAM Identity Center가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS IAM Identity Center에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
>
> AWS IAM Identity Center 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

IAM Identity Center가 작동하려면 AWS Organizations와의 신뢰할 수 있는 액세스가 필요합니다. 신뢰할 수 있는 액세스는 IAM Identity Center를 설정할 때 활성화합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 시작하기 - 1단계: AWS IAM Identity Center 활성화를 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS IAM Identity Center의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 AWS IAM Identity Center의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS IAM Identity Center를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: EnableAWSServiceAccess

IAM Identity Center와의 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

IAM Identity Center가 작동하려면 AWS Organizations와의 신뢰할 수 있는 액세스가 필요합니다. AWS Organizations를 사용하는 동안 IAM Identity Center를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 조직에 액세스하지 못해 작동이 중단됩니다. 사용자는 IAM Identity Center를 사용하여 계정에 액세스할 수 없게 됩니다. IAM Identity Center가 생성한 역할은 그대로 남아 있지만 IAM Identity Center 서비스가 해당 역할에 액세스할 수 없습니다. IAM Identity Center 서비스 연결 역할은 그대로 유지됩니다. 신뢰할 수 있는 액세스를 다시 활성화하면 IAM Identity Center가 이전과 같이 계속 작동하므로 서비스를 다시 구성할 필요가 없습니다.

조직에서 계정을 제거한 경우 IAM Identity Center는 서비스 연결 역할과 같은 모든 메타데이터 및 리소스를 자동으로 정리합니다. 조직에서 제거된 독립 실행형 계정은 더 이상 IAM Identity Center에서 사용할 수 없습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS IAM Identity Center의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 AWS IAM Identity Center의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS IAM Identity Center를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: DisableAWSServiceAccess

IAM Identity Center에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 IAM Identity Center에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 IAM Identity Center 관리와 조직 관리를 분리하는 데 도움이 됩니다.

> **최소 권한**
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 IAM Identity Center에 대한 위임된 관리자로 구성할 수 있습니다.

IAM Identity Center에 대한 위임된 관리자 계정을 활성화하는 방법에 대한 지침은 AWS IAM Identity Center 사용 설명서의 위임된 관리를 참조하세요.

AWS Systems Manager 및 AWS Organizations

AWS Systems Manager는 AWS 리소스를 보고 제어할 수 있는 기능 모음입니다. 다음 Systems Manager 기능은 조직의 모든 AWS 계정에 걸쳐 Organizations과 함께 사용할 수 있습니다.

- Systems Manager Explorer는 AWS 리소스에 대한 정보를 보고하는 사용자 지정 가능한 작업 대시보드입니다. Organizations와 Systems Manager Explorer를 사용해 조직의 모든 AWS 계정 계정 간에 작업 데이터를 동기화할 수 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 Systems Manager Explorer를 참조하세요.
- Systems Manager Change Manager는 애플리케이션 구성 및 인프라에 대한 운영 변경을 요청, 승인, 구현 및 보고하기 위한 엔터프라이즈 변경 관리 프레임워크입니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 AWS Systems Manager Change Manager를 참조하세요.
- Systems Manager OpsCenter는 운영 엔지니어 및 IT 전문가가 AWS 리소스와 관련된 운영 작업 항목(OpsItem)을 보고, 조사하고, 해결할 수 있는 중앙 위치를 제공합니다. Organizations와 함께 OpsCenter를 사용하면 단일 세션 동안 관리 계정(Organizations 관리 계정 또는 Systems Manager 위임 관리자 계정) 및 다른 계정 하나의 OpsItem에 대한 작업을 수행할 수 있습니다. 구성되면 사용자는 다음 유형의 작업을 수행할 수 있습니다.
  - 다른 계정의 OpsItem을 만들고 보고 업데이트합니다.
  - 다른 계정의 OpsItem에 지정된 AWS 리소스에 대한 세부 정보를 봅니다.
  - Systems Manager 자동화 런북을 시작하여 다른 계정의 AWS 리소스 관련 문제를 해결합니다.

  자세한 내용은 AWS Systems Manager 사용 설명서의 AWS Systems Manager OpsCenter을 참조하세요.

다음 정보는 AWS Systems Manager를 AWS Organizations와 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Systems Manager는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Systems Manager와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Systems Manager가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `ssm.amazonaws.com`

Systems Manager와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Systems Manager의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.

4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Systems Manager의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Systems Manager를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

Systems Manager와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

Systems Manager는 조직의 AWS 계정 전반에서 작업 데이터를 동기화하기 위해 AWS Organizations와 상호 신뢰할 수 있는 액세스가 필요합니다. 신뢰할 수 있는 액세스를 비활성화하면 Systems Manager에서 작업 데이터가 동기화되지 않고 오류가 보고됩니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Systems Manager의 행을 찾은 다음 서비스의 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.
5. 본인이 AWS Organizations에서만 관리자인 경우 AWS Systems Manager의 관리자에게 콘솔 또는 도구에서 해당 서비스를 비활성화하여 AWS Organizations와 연동할 수 없다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Systems Manager를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: DisableAWSServiceAccess

Systems Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Systems Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Systems Manager 관리와 조직 관리를 분리하는 데 도움을 줍니다.

조직 전체에서 Systems Manager를 사용하는 경우 위임된 관리자 계정을 사용합니다. 이 계정은 Change Manager에서 변경 템플릿, 변경 요청, 변경 실행서 및 승인 워크플로를 관리하기 위한 계정으로 지정한 AWS 계정입니다. 위임된 계정은 조직 전체의 변경 활동을 관리합니다. Change Manager에서 사용할 조직을 설정할 때 이 역할을 수행하는 계정을 지정합니다. 조직의 관리 계정일 필요는 없습니다. 계정 하나만으로 Change Manager를 사용하는 경우 위임된 관리자 계정이 필요하지 않습니다.

멤버 계정을 위임된 관리자로 지정하려면 AWS Systems Manager사용 설명서에서 다음 주제를 참조하세요.

- Explorer 및 OpsCenter의 경우 위임된 관리자 구성을 참조하세요.
- Change Manager의 경우, Change Manager에 대해 조직 및 위임된 계정 설정을 참조하세요.

태그 정책 및 AWS Organizations

태그 정책은 조직의 계정에 있는 리소스 전체에서 태그를 표준화하는 데 도움이 될 수 있는 AWS Organizations 정책의 한 유형입니다. 태그 정책에 대한 자세한 내용은 태그 정책 단원을 참조하세요.

다음 정보는 태그 정책과 AWS Organizations를 통합하는 데 도움을 줍니다.

서비스 연결 역할이 사용하는 서비스 보안 주체

Organizations는 다음 서비스 보안 주체를 사용하여 리소스에 연결된 태그와 상호 작용합니다.

- `tagpolicies.tag.amazonaws.com`

태그 정책에 대해 신뢰할 수 있는 액세스 활성화

조직에서 태그 정책을 활성화하거나 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 태그 정책을 활성화하여 신뢰할 수 있는 액세스를 활성화하는 것이 좋습니다. 이렇게 하면 Organizations가 필요한 설정 작업을 수행합니다.

AWS Organizations 콘솔에서 태그 정책 유형을 활성화하여 태그 정책에 대한 신뢰할 수 있는 액세스를 활성화할 수 있습니다. 자세한 정보는 정책 유형 활성화을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 태그 정책의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 태그 정책의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 태그 정책을 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal tagpolicies.tag.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

태그 정책과 상호 신뢰할 수 있는 액세스 비활성화

AWS Organizations 콘솔에서 태그 정책 유형을 비활성화하여 태그 정책에 대한 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. 자세한 정보는 정책 유형 비활성화을 참조하십시오.

AWS Trusted Advisor 및 AWS Organizations

AWS Trusted Advisor는 고객의 AWS 환경을 검사하여 비용 절감, 시스템 가용성 및 성능 개선 또는 보안 격차를 해결할 기회가 있으면 이를 권장합니다. Organizations와 통합하면 조직의 모든 계정에 대한 Trusted Advisor 검사 결과를 수신할 수 있고, 보고서를 다운로드하여 검사 요약 및 영향을 받는 리소스를 확인할 수 있습니다.

자세한 내용은 AWS Support 사용 설명서의 AWS Trusted Advisor에 대한 조직 보기를 참조하세요.

다음 정보는 AWS Trusted Advisor와 AWS Organizations를 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Trusted Advisor는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Trusted Advisor와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForTrustedAdvisorReporting`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Trusted Advisor가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `reporting.trustedadvisor.amazonaws.com`

Trusted Advisor와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

신뢰할 수 있는 액세스는 AWS Trusted Advisor로만 활성화할 수 있습니다.

Trusted Advisor 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Support 사용 설명서의 조직 보기 사용을 참조하세요.

Trusted Advisor와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

이 기능을 비활성화하면 Trusted Advisor는 조직의 다른 모든 계정에 대해 검사 정보 기록을 중지합니다. 기존 보고서를 보거나 다운로드하거나 새 보고서를 만들 수 없습니다.

AWS Trusted Advisor 또는 AWS Organizations 도구를 사용해 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Trusted Advisor 콘솔 또는 도구를 사용하여 Organizations 통합을 비활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Trusted Advisor가 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등의 필요한 정리를 수행합니다. AWS Trusted Advisor에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.
>
> AWS Trusted Advisor 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Trusted Advisor 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

AWS Support 사용 설명서의 조직 보기 사용 안 함을 참조하세요.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Trusted Advisor를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Trusted Advisor에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 지정된 계정의 사용자 및 역할이 조직의 다른 멤버 계정의 AWS 계정 메타데이터를 관리할 수 있습니다. 위임된 관리자 계정을 활성화하지 않으면 조직의 관리 계정에서만 이러한 작업을 수행할 수 있습니다. 이렇게 하면 조직의 관리와 계정 세부 정보의 관리를 분리하는 데 도움이 됩니다.

> 최소 권한
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Trusted Advisor 에 대한 위임된 관리자로 구성할 수 있습니다

Trusted Advisor에 대한 위임된 관리자 계정 활성화에 대한 지침은 AWS Support 사용 설명서의 위임된 관리자 등록을 참조하세요.

AWS CLI, AWS API

AWS CLI 또는 AWS SDK 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator` 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체 `account.amazonaws.com`을 파라미터로 식별합니다.

Trusted Advisor에 대해 위임된 관리자를 비활성화

Trusted Advisor 콘솔을 사용하거나 Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. Trusted Advisor 콘솔을 사용하여 위임된 관리자 Trusted Advisor 계정을 비활성화하는 방법에 대한 자세한 내용은 AWS Support 사용 설명서의 위임된 관리자 등록 취소를 참조하세요.

AWS Well-Architected Tool 및 AWS Organizations

AWS Well-Architected Tool은 워크로드 상태를 문서화하고 최신 AWS 아키텍처 모범 사례와 비교하는 데 도움이 됩니다.

AWS Well-Architected Tool을 Organizations와 함께 사용하면 AWS Well-Architected Tool 및 Organizations 고객 모두가 다른 조직의 구성원과 AWS Well-Architected Tool 리소스를 공유하는 프로세스를 간소화할 수 있습니다.

자세한 내용은 AWS Well-Architected Tool 사용 설명서의 AWS Well-Architected Tool 리소스 공유를 참조하세요.

다음 정보는 AWS Well-Architected Tool를 AWS Organizations와 통합하는 데 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AWS WA Tool는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS WA Tool와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForWellArchitected`

서비스 역할 정책은 `AWSWellArchitectedOrganizationsServiceRolePolicy`입니다.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. AWS WA Tool가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `wellarchitected.amazonaws.com`

AWS WA Tool와 상호 신뢰할 수 있는 액세스 활성화

조직의 계층적 변경 사항을 반영하도록 AWS WA Tool을 업데이트할 수 있습니다.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Well-Architected Tool 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Well-Architected Tool 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Well-Architected Tool가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. AWS Well-Architected Tool에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 이 메모를 참조하십시오.
> AWS Well-Architected Tool 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

AWS WA Tool 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Well-Architected Tool사용 설명서의 AWS Well-Architected Tool 리소스 공유를 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스(Services) 페이지에서 AWS Well-Architected Tool의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.

4. 본인이 AWS Organizations에서만 관리자인 경우 AWS Well-Architected Tool의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 AWS Well-Architected Tool를 활성화할 수 있습니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: EnableAWSServiceAccess

AWS WA Tool와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Well-Architected Tool 또는 AWS Organizations 도구를 사용해 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

> **Important**
>
> 가능하면 항상 AWS Well-Architected Tool 콘솔 또는 도구를 사용하여 Organizations 통합을 비활성화할 것을 적극 권장합니다. 이렇게 하면 AWS Well-Architected Tool가 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등의 필요한 정리를 수행합니다. AWS Well-Architected Tool에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.
>
> AWS Well-Architected Tool 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

AWS WA Tool 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

AWS Well-Architected Tool사용 설명서의 AWS Well-Architected Tool 리소스 공유를 참조하세요.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로서 AWS Well-Architected Tool를 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: DisableAWSServiceAccess

Amazon VPC IP 주소 관리자(IPAM) 및 AWS Organizations

Amazon VPC IP 주소 관리자(IPAM)는 AWS 워크로드의 IP 주소를 보다 쉽게 계획, 추적 및 모니터링할 수 있게 해주는 VPC 기능입니다.

AWS Organizations를 사용하면 조직 전체의 IP 주소 사용량을 모니터링하고 멤버 계정 간에 IP 주소 풀을 공유할 수 있습니다.

자세한 내용은 Amazon VPC IPAM 사용 설명서의 AWS Organizations와 IPAM 통합을 참조하십시오.

다음 정보를 사용하면 Amazon VPC IP Address Manager(IPAM)와 AWS Organizations를 통합하는 데 도움이 됩니다.

통합 활성화 시 서비스 연결 역할 생성

다음 서비스 연결 역할은 IPAM 콘솔을 사용하거나 IPAM의 `EnableIpamOrganizationAdminAccount` API를 사용하여 IPAM을 AWS Organizations와 통합할 때 조직의 관리 계정 및 각 멤버 계정에 자동으로 생성됩니다.

- `AWSServiceRoleForIPAM`

자세한 내용은 Amazon VPC IPAM 사용 설명서의 IPAM에 대한 서비스 연결 역할을 참조하십시오.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. IPAM에서 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `ipam.amazonaws.com`

IPAM에서 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

> **Note**
>
> IPAM에 대해 위임된 관리자를 지정하면 조직의 IPAM에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.
> 조직의 이 서비스에 대한 위임된 관리자로 멤버 계정을 지정하려면 IPAM에 먼저 AWS Organizations에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

Amazon VPC IP 주소 관리자(IPAM) 도구만 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

IPAM 콘솔 또는 IPAM `EnableIpamOrganizationAdminAccount` API를 사용하여 IPAM을 AWS Organizations와 통합하는 경우 IPAM에 대한 신뢰할 수 있는 액세스 권한을 자동으로 부여합니다. 신뢰할 수 있는 액세스 권한을 부여하면 관리 계정과 조직의 모든 멤버 계정에 서비스 연결 역할 `AWSServiceRoleForIPAM`가 생성됩니다. IPAM은 서비스 연결 역할을 사용하여 조직의 EC2 네트워킹 리소스와 연결된 CIDR을 모니터링하고 Amazon CloudWatch에 IPAM과 관련된 지표를 저장합니다. 자세한 내용은 Amazon VPC IPAM 사용 설명서의 IPAM에 대한 서비스 연결 역할을 참조하십시오.

신뢰할 수 있는 액세스 활성화에 대한 지침은 Amazon VPC IPAM 사용 설명서의 AWS Organizations와 IPAM 통합을 참조하십시오

> **Note**
>
> AWS Organizations 콘솔 또는 `EnableAWSServiceAccess` API를 사용하여 IPAM에서 신뢰할 수 있는 액세스를 활성화할 수 없습니다.

IPAM에서 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 AWS Organizations `disable-aws-service-access` API를 사용하여 IPAM에서 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

IPAM 계정 권한 비활성화 및 서비스 연결 역할 삭제에 대한 자세한 내용은 Amazon VPC IPAM 사용 설명서의 IPAM에 대한 서비스 연결 역할을 참조하십시오.

Organizations AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 Organizations API 작업을 호출하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: disable-aws-service-access

  다음 명령을 실행하여 Amazon VPC IP 주소 관리자(IPAM)를 조직에서 신뢰할 수 있는 서비스로 비활성화할 수 있습니다.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.
- AWS API: DisableAWSServiceAccess

IPAM에 대한 위임된 관리자 계정 활성화

IPAM에 대해 위임된 관리자 계정은 IPAM 및 IP 주소 풀 생성, 조직의 IP 주소 사용 관리 및 모니터링, 멤버 계정 간에 IP 주소 풀 공유를 담당합니다. 자세한 내용은 Amazon VPC IPAM 사용 설명서의 AWS Organizations와 IPAM 통합을 참조하십시오.

조직 관리 계정의 관리자만 IPAM에 대해 위임된 관리자를 구성할 수 있습니다.

IPAM 콘솔에서 또는 `enable-ipam-organization-admin-account` API를 사용하여 위임된 관리자 계정을 지정할 수 있습니다. 자세한 내용은 AWSAWS CLI 명령 참조에서 enable-ipam-organization-admin-account를 참조하세요.

> **최소 권한**
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 IPAM에 대한 위임된 관리자로 구성할 수 있습니다

IPAM 콘솔을 사용하여 위임된 관리자를 구성하려면 Amazon VPC IPAM 사용 설명서에서 AWS Organizations와 IPAM 통합을 참조하세요.

IPAM에 대해 위임된 관리자를 비활성화

조직 관리 계정의 관리자만 IPAM에 대해 위임된 관리자를 구성할 수 있습니다.

AWS AWS CLI를 사용하여 위임된 관리자를 제거하려면 AWSAWS CLI 명령 참조의 disable-ipam-organization-admin-account를 참조하세요.

IPAM 콘솔을 사용하여 위임된 관리자 IPAM 계정을 비활성화하려면 Amazon VPC IPAM 사용 설명서에서 AWS Organizations와 IPAM 통합을 참조하세요.

Amazon VPC Reachability Analyzer 및 AWS Organizations

Reachability Analyzer는 Virtual Private Cloud(VPC)에서 소스 리소스와 대상 리소스 간의 연결을 테스트할 수 있는 구성 분석 도구입니다.

AWS Organizations와 Reachability Analyzer를 함께 사용하면 조직 내의 여러 계정에 걸쳐 경로를 추적할 수 있습니다.

자세한 내용은 Reachability Analyzer 사용 설명서에서 Reachability Analyzer의 계정 간 분석을 참조하세요.

다음은 Reachability Analyzer를 AWS Organizations와 통합하는 데 유용한 정보입니다.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Reachability Analyzer는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Reachability Analyzer와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForReachabilityAnalyzer`

자세한 내용은 Reachability Analyzer 사용 설명서에서 Reachability Analyzer의 계정 간 분석을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Reachability Analyzer가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `reachabilityanalyzer.networkinsights.amazonaws.com`

Reachability Analyzer를 통한 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한 단원을 참조하세요.

Reachability Analyzer에 대해 위임된 관리자를 지정하면 조직의 Reachability Analyzer에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

조직의 이 서비스에 대한 위임된 관리자로 멤버 계정을 지정하려면, 먼저 Reachability Analyzer에 AWS Organizations에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

> **Important**
>
> - Reachability Analyzer 콘솔 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다. 하지만 Organizations와의 통합을 설정하는 데에는 Reachability Analyzer 콘솔이나 `EnableMultiAccountAnalysisForAwsOrganization` API를 사용

하는 것이 좋습니다. 이렇게 하면 Reachability Analyzer가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다.

- 신뢰할 수 있는 액세스 권한을 부여하면 관리 계정과 조직의 모든 멤버 계정에 서비스 연결 역할 `AWSServiceRoleForReachabilityAnalyzer`가 생성됩니다. Reachability Analyzer는 서비스 연결 역할을 사용하여 관리자와 위임된 관리자가 조직 내 모든 리소스 간의 연결에 대한 분석을 실행할 수 있도록 합니다. Reachability Analyzer는 조직 내 계정의 네트워킹 요소에 대한 스냅샷을 생성하여 연결 쿼리에 응답할 수 있습니다.
- 자세한 내용과 Reachability Analyzer를 통한 신뢰할 수 있는 액세스를 활성화하는 방법에 대한 지침은 Reachability Analyzer 사용 설명서에서 Reachability Analyzer의 계정 간 분석을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDK 중 하나에서 API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 서비스 페이지에서 VPC Reachability Analyzer에 대한 행을 찾아 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **`enable`**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 본인이 AWS Organizations에서만 관리자인 경우 Reachability Analyzer의 관리자에게 콘솔에서 해당 서비스를 활성화하여 AWS Organizations와 연동할 수 있다고 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하면 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: enable-aws-service-access

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Reachability Analyzer를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: EnableAWSServiceAccess

Reachability Analyzer를 통한 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한 단원을 참조하세요.

Reachability Analyzer 콘솔(권장) 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. Reachability Analyzer 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면 Reachability Analyzer 사용 설명서에서 Reachability Analyzer의 계정 간 분석을 참조하세요.

Reachability Analyzer에 대해 위임된 관리자 계정 활성화

위임된 관리자 계정은 조직 내의 모든 리소스에 대해 연결 분석을 실행할 수 있습니다. 자세한 내용은 Reachability Analyzer 사용 설명서에서 Reachability Analyzer와 AWS Organizations 통합을 참조하세요.

조직 관리 계정의 관리자만 Reachability Analyzer에 대해 위임된 관리자를 구성할 수 있습니다.

Reachability Analyzer 콘솔에서 또는 `RegisterDelegatedAdministrator` API를 사용하여 위임된 관리자 계정을 지정할 수 있습니다. 자세한 내용은 Organizations 명령 참조에서 RegisterDelegatedAdministrator를 참조하세요.

> 최소 권한
>
> Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Reachability Analyzer에 대한 위임된 관리자로 구성할 수 있습니다

Reachability Analyzer 콘솔을 사용하여 위임된 관리자를 구성하려면 Reachability Analyzer 사용 설명서에서 Reachability Analyzer와 AWS Organizations 통합을 참조하세요.

Reachability Analyzer에 대해 위임된 관리자 비활성화

조직 관리 계정의 관리자만 Reachability Analyzer에 대해 위임된 관리자를 구성할 수 있습니다.

Reachability Analyzer 콘솔이나 API에서 또는 Organizations `DeregisterDelegatedAdministrator` CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

Reachability Analyzer 콘솔을 사용하여 Reachability Analyzer의 위임된 관리자 계정을 비활성화하려면 Reachability Analyzer 사용 설명서에서 Reachability Analyzer의 계정 간 분석을 참조하세요.

Organizations과 연동되는 AWS 서비스의 위임된 관리자

AWS Organizations 관리 계정과 그 사용자 및 역할은 해당 계정으로 수행해야 하는 작업에 대해서만 사용하는 것이 좋습니다. 또한 AWS 리소스를 조직의 다른 멤버 계정에 저장하고 관리 계정에는 저장하지 않는 것이 좋습니다. 이는 Organizations 서비스 제어 정책(SCP)과 같은 보안 기능이 관리 계정의 사용자나 역할을 제한하지 않기 때문입니다. 관리 계정에서 리소스를 분리하면 인보이스의 요금을 파악하는 데도 도움이 될 수 있습니다.

Organizations과 통합되는 많은 AWS 서비스를 통해 관리 계정의 사용을 줄일 수 있습니다. 이러한 서비스를 통해 하나 이상의 멤버 계정을 관리자로 등록하여 서비스에 사용되는 모든 조직 계정을 관리하도록 할 수 있습니다. 이러한 계정을 해당 특정 서비스의 위임된 관리자라고 합니다. 멤버 계정을 AWS 서비스의 위임된 관리자로 등록하면 해당 계정은 해당 서비스에 대한 일부 관리 권한과 Organizations 읽기 전용 작업에 대한 권한을 가질 수 있습니다.

계정을 서비스의 위임된 관리자로 등록하기 전 다음 사항을 수행합니다.

- 서비스가 위임된 관리자를 지원하는지 확인합니다. 어떤 서비스가 위임된 관리자를 지원하지 알아보려면 AWS 함께 사용할 수 있는 서비스 AWS Organizations의 표를 참조하십시오.
- 해당 서비스에 대해 신뢰할 수 있는 액세스를 활성화합니다.

> **Note**
>
> 서비스의 위임된 관리자를 활성화하는 방법을 알아보려면, AWS 함께 사용할 수 있는 서비스 AWS Organizations의 표를 참조하여 해당 서비스에 대한 위임된 관리자 지원 열에서 자세히 알아보기 링크를 선택하십시오.

위임된 관리자 계정에 부여된 권한

각 서비스별 위임 관리자 계정에는 해당 서비스에서 부여하는 권한이 있습니다. 자세한 내용은 AWS 함께 사용할 수 있는 서비스 AWS Organizations의 표를 참조하여 해당 서비스에 대한 위임된 관리자 지원 열에서 자세히 알아보기 링크를 선택하십시오.

위임된 관리자 계정에는 다음과 같은 읽기 전용 권한도 있습니다.

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`

이러한 권한을 사용하여 다음 콘솔 항목을 볼 수 있으며 변경할 수는 없습니다.

- Organizations 구조, 모든 계정 및 OU, 조직 정책
- 멤버십
- 모든 계정 및 OU.
- Organizations 정책

보안 내부 AWS Organizations

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

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

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오. AWS Organizations
- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Organizations 사용 시 책임 분담 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Organizations를 구성하는 방법을 보여줍니다. 또한 Organizations 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- AWS PrivateLink ... 에 대한 AWS Organizations
- AWS Identity and Access Management 및 AWS Organizations
- AWS Organizations의 로깅 및 모니터링
- AWS Organizations의 규정 준수 확인
- AWS Organizations의 복원성
- AWS Organizations의 인프라 보안

AWS PrivateLink ... 에 대한 AWS Organizations

AWS PrivateLink for 를 AWS Organizations사용하면 공용 인터넷을 사용하지 않고도 VPC (가상 사설 클라우드) 내에서 AWS Organizations 서비스에 액세스할 수 있습니다.

Amazon VPC를 사용하면 사용자 지정 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. VPC를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC에 대한 자세한 내용은 Amazon VPC 사용 설명서를 참조하세요.

Amazon VPC를 연결하려면 먼저 인터페이스 VPC 엔드포인트 (인터페이스 엔드포인트) 를 정의해야 합니다. AWS Organizations인터페이스 엔드포인트는 VPC의 서브넷에서 프라이빗 IP 주소가 할당된 하나 이상의 탄력적 네트워크 인터페이스(ENI)로 표시됩니다. VPC에서 인터페이스 엔드포인트를 AWS Organizations 통한 요청은 Amazon 네트워크에 그대로 유지됩니다.

인터페이스 엔드포인트에 대한 일반 정보는 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트를 사용한 AWS 서비스 액세스를 참조하십시오.

주제

- 의 제한 및 제한 AWS PrivateLinkAWS Organizations
- VPC 엔드포인트 생성
- AWS Organizations에 대한 VPC 엔드포인트 정책 생성

의 제한 및 제한 AWS PrivateLinkAWS Organizations

에는 VPC 제한이 적용됩니다. AWS PrivateLink AWS Organizations자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트를 사용한 AWS 서비스 액세스 및 AWS PrivateLink 할당량을 참조하십시오. 또한 다음과 같은 제한 사항이 적용됩니다.

- 해당 지역에서만 사용할 수 있습니다. `us-east-1`
- 전송 계층 보안 (TLS) 1.1을 지원하지 않습니다.

VPC 엔드포인트 생성

Amazon VPC 콘솔 () 또는 을 사용하여 VPC에 AWS Organizations 엔드포인트를 생성할 수 있습니다. AWS Command Line Interface AWS CLI AWS CloudFormation

Amazon VPC 콘솔 또는 를 사용하여 엔드포인트를 생성하고 구성하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트 생성을 참조하십시오. AWS CLI 를 사용하여 엔드포인트를 생성하고 구성하는 방법에 대한 자세한 내용은 사용 AWS CloudFormation설명서의 AWS: :EC2: :VPCendPoint 리소스를 참조하십시오.AWS CloudFormation

AWS Organizations 엔드포인트를 생성할 때는 다음을 서비스 이름으로 사용하십시오.

```
com.amazonaws.us-east-1.organizations
```

액세스 시 FIPS 140-2 검증을 거친 암호화 모듈이 필요한 경우 다음 FIPS 서비스 AWS이름을 사용하십시오. AWS Organizations

```
com.amazonaws.us-east-1.organizations-fips
```

AWS Organizations에 대한 VPC 엔드포인트 정책 생성

Organizations에 대한 액세스를 제어하는 엔드포인트 정책을 VPC 엔드포인트에 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

자세한 내용은 Amazon VPC 사용 설명서의 엔드포인트 정책을 사용하여 VPC 엔드포인트에 대한 액세스 제어를 참조하십시오.

예제: AWS Organizations 작업에 대한 VPC 엔드포인트 정책

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Identity and Access Management 및 AWS Organizations

AWS Organizations에 액세스하려면 보안 인증이 필요합니다. 이러한 자격 증명은 Amazon Simple Storage Service(Amazon S3) 버킷, Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스나 AWS

Organizations 조직 단위(OU) 같은 AWS 리소스에 대한 액세스 권한이 있어야 합니다. 다음 단원에서는 AWS Identity and Access Management(IAM)를 사용하여 조직에 대한 액세스 보안을 확보하고 조직 관리자를 제어하는 방법을 자세히 설명합니다.

누가 조직의 어떤 부분을 관리할 수 있는지 결정하기 위해 AWS Organizations는 다른 AWS 서비스와 동일한 IAM 기반 권한 모델을 사용합니다. 조직의 관리 계정에 속한 관리자는 정책을 관리 계정의 사용자, 그룹, 역할에 연결해 AWS Organizations 작업을 수행할 IAM 기반 권한을 부여할 수 있습니다. 이 정책은 상기의 주체가 수행할 수 있는 작업을 지정합니다. IAM 권한 정책을 사용자가 멤버인 그룹에 연결하거나 사용자 또는 역할에 직접 연결합니다. 모범 사례는 정책을 사용자 대신 그룹에 연결하는 것입니다. 또한 여러분은 다른 사용자에 전체 관리 권한을 부여할 수도 있습니다.

대부분의 AWS Organizations 관리자 작업을 수행하려면 관리 계정의 사용자 또는 그룹에 권한을 연결해야 합니다. 멤버 계정의 사용자가 조직의 관리 작업을 수행하려면 AWS Organizations 권한을 관리 계정의 IAM 역할에 부여하고 멤버 계정의 사용자가 역할을 수임할 수 있도록 해야 합니다. IAM 권한 정책에 대한 일반적인 정보는 IAM 사용 설명서의 IAM 정책 개요를 참조하세요.

주제

인증

다음과 같은 유형의 자격 증명으로 AWS에 액세스할 수 있습니다.

- AWS 계정 루트 사용자 – AWS에 가입할 때 AWS 계정과 연결된 이메일 주소 및 암호를 입력합니다. 이 두 가지가 루트 보안 인증 정보이며 모든 AWS 리소스에 대한 전체 액세스 권한을 제공합니다.

> **Important**
>
> AWS 계정에 가입하면 AWS 계정 루트 사용자이(가) 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스및 리소스에 액세스하는 권한이 있습니다. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 루트 사용자만 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

- IAM 사용자 – IAM 사용자는 간단히 설명해 특정 사용자 정의 권한(예: Amazon Elastic File System에서 파일 시스템를 생성할 수 있는 권한)이 있는 AWS 계정 내의 자격 증명입니다. IAM 사용자 이름과 암호를 사용하여 AWS Management Console, AWS 토론 포럼 또는 AWS 지원 센터 같은 보안 AWS 웹 페이지에 로그인할 수 있습니다.

  사용자 이름과 암호 외에 각 사용자에 대해 액세스 키를 생성할 수 있습니다. 여러 SDK 중 하나를 통해 또는 AWS Command Line Interface(AWS CLI)를 사용하여 AWS 서비스에 프로그래밍 방식으로 액세스할 때 이러한 키를 사용할 수 있습니다. SDK 및 AWS CLI 도구는 액세스 키를 사용하여 암호화 방식으로 요청에 서명합니다. AWS 도구를 사용하지 않으면 요청에 직접 서명해야 합니다. AWS Organizations에서는 인바운드 API 요청 인증용 프로토콜인 서명 버전 4를 지원합니다. 요청 인증에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.
- IAM 역할 – IAM 역할은 계정에 만들 수 있는, 특정 권한을 지닌 또 다른 IAM 자격 증명입니다. IAM 사용자와 유사하지만 특정 개인과 연결되지 않습니다. IAM 역할을 사용하면 AWS 서비스 및 리소스에 액세스할 수 있는 임시 액세스 키를 얻을 수 있습니다. 임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.
  - 페더레이션 사용자 액세스 – IAM 사용자를 생성하는 대신 AWS Directory Service의 기존 사용자 자격 증명, 엔터프라이즈 사용자 디렉터리 또는 웹 자격 증명 공급자를 사용할 수 있습니다. 이 사용자를 페더레이션 사용자라고 합니다. AWS에서는 자격 증명 공급자를 통해 액세스가 요청되면 페더레이션 사용자에게 역할을 할당합니다. 연합된 사용자에 대한 자세한 정보는 IAM 사용 설명서의 연합된 사용자 및 역할을 참조하세요.
  - 교차 계정 액세스 – 계정의 IAM 역할을 사용하여 계정 리소스에 액세스할 권한을 다른 AWS 계정에 부여할 수 있습니다. 그 예로는 IAM 사용 설명서의 튜토리얼: IAM 역할을 이용한 AWS 계정 간의 액세스 권한 위임을 참조하십시오.
  - AWS 서비스 액세스 – 계정의 IAM 역할을 사용하여 계정의 리소스에 액세스할 권한을 AWS 서비스에 부여할 수 있습니다. 예를 들어 Amazon Redshift가 사용자를 대신하여 Amazon S3 버킷에 액세스하도록 허용하는 역할을 생성한 다음, 버킷에 저장된 데이터를 Amazon Redshift 클러스터에 로드할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - Amazon EC2에서 실행되는 애플리케이션 – 인스턴스에서 실행되고 AWS API 요청을 하는 애플리케이션에서 사용할 수 있도록 EC2 인스턴스에 액세스 키를 저장하는 대신에, IAM 역할을 사용하여 이러한 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 인스턴스에 연결된 인스턴스 프로파일을 만들 수 있습니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

액세스 제어

요청을 인증하는 데 유효한 자격 증명이 있더라도 권한이 없다면 AWS Organizations 리소스를 관리하거나 액세스할 수 없습니다. 예를 들어 사용자는 OU를 생성하거나 서비스 제어 정책(SCP)을 계정에 연결할 권한이 있어야 합니다.

다음 단원에서는 AWS Organizations에 대한 권한을 관리하는 방법을 설명합니다.

- AWS 조직에 대한 액세스 권한 관리 개요
- AWS Organizations에 대한 자격 증명 기반 정책(IAM 정책) 사용
- 태그와 AWS Organizations를 사용한 속성 기반 액세스 제어

AWS 조직에 대한 액세스 권한 관리 개요

조직 내 루트, OU, 계정, 정책을 포함한 모든 AWS 리소스는 AWS 계정이 소유하며, 리소스 생성 및 액세스 권한은 권한 정책이 관장합니다. 조직의 경우, 조직의 관리 계정이 모든 리소스를 소유합니다. 계정 관리자는 권한 정책을 IAM 자격 증명(사용자, 그룹 및 역할)에 연결해 AWS 리소스에 대한 액세스를 제어할 수 있습니다.

> **Note**
>
> 계정 관리자(또는 관리자 사용자)는 관리자 권한이 있는 사용자입니다. 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하십시오.

권한을 부여하려면 권한을 부여 받을 사용자, 권한 대상이 되는 리소스, 해당 리소스에 허용되는 특정 작업을 결정합니다.

기본적으로 IAM 사용자, 그룹 및 역할에는 어떠한 권한도 없습니다. 조직의 관리 계정에 속한 관리자는 관리 업무를 수행하거나 관리 계정의 다른 IAM 사용자나 역할에 관리 권한을 위임할 수 있습니다. 이렇게 하려면 IAM 권한 정책을 IAM 사용자, 그룹 또는 역할에 연결해야 합니다. 기본적으로 사용자는 어떤 권한도 가지지 않습니다. 이를 묵시적 거부라고 합니다. 이 정책은 사용자가 수행할 수 있는 작업과 사용자가 작업을 수행할 수 있는 리소스를 지정하는 명시적 허용으로 묵시적 거부를 무시합니다. 권한을 역할에 부여하면, 해당 역할은 조직 내 다른 계정 사용자가 맡을 수 있습니다.

AWS Organizations 리소스 및 작업

이 단원에서는 AWS Organizations 개념이 IAM의 대응 개념에 매핑되는 방식을 설명합니다.

리소스

AWS Organizations에서 다음 모든 리소스에 대한 액세스를 제어할 수 있습니다.

- 조직의 계층적 구조를 구성하는 루트 및 OU
- 조직의 멤버가 되는 계정
- 조직 내 다음 개체에 연결하는 정책
- 조직 상태를 변경할 때 사용하는 핸드셰이크

각 리소스에는 관련된 고유 Amazon 리소스 이름(ARN)이 있습니다. IAM 권한 정책의 `Resource` 요소에 ARN을 지정하면 리소스에 대한 액세스를 제어할 수 있습니다. 에서 AWS Organizations 사용되는 리소스의 ARN 형식 전체 목록은 서비스 권한 부여 참조에 AWS Organizations 정의된 리소스 유형을 참조하십시오.

운영

AWS는 조직 내 리소스를 다루는 다양한 작업을 제공합니다. 이를 통해 리소스 콘텐츠 생성, 나열, 수정, 액세스 및 리소스 삭제 같은 일을 할 수 있습니다. 대부분의 작업을 IAM 정책의 `Action` 요소에 참조해 해당 작업을 사용하는 사람을 제어할 수 있습니다. IAM 정책에서 권한으로 사용할 수 있는 AWS Organizations 작업 목록은 서비스 권한 부여 참조의 AWS Organizations에서 정의한 작업을 참조하십시오.

`Action`과 `Resource`를 단일 권한 정책 `Statement`로 결합하면, 특정 작업 모음을 사용할 수 있는 리소스를 정확하게 제어할 수 있습니다.

조건 키

AWS는 특정 작업에 대한 보다 세부적인 제어를 제공하기 위해 쿼리할 수 있는 조건 키를 제공합니다. IAM 정책의 `Condition` 요소에서 이러한 조건 키를 참조하여 문을 일치로 간주하기 위해 충족해야 하는 추가적인 상황을 지정할 수 있습니다.

다음은 AWS Organizations에 특히 유용한 조건 키입니다.

- `aws:PrincipalOrgID` - 리소스 기반 정책의 `Principal` 요소 지정을 간소화합니다. 이 전역 키는 조직 내 모든 AWS 계정의 계정 ID를 전부 나열하는 대안을 제공합니다. 조직의 멤버인 모든 계정을 나열하는 대신 `Condition` 요소에 조직 ID를 지정할 수 있습니다.

> **Note**
>
> 이 전역 조건은 조직의 관리 계정에도 적용됩니다.

자세한 내용은 IAM 사용 설명서의 `PrincipalOrgID` AWS글로벌 조건 내 컨텍스트 키 설명을 참조하십시오.

- `aws:PrincipalOrgPaths` - 이 조건 키를 사용하여 특정 조직 루트, OU 또는 해당 하위 항목의 멤버를 일치시킵니다. 요청을 수행하는 보안 주체(루트, IAM 사용자 또는 역할)가 지정된 조직 경로에 있는 경우 `aws:PrincipalOrgPaths` 조건 키는 true를 반환합니다. 경로는 AWS Organizations 엔터티 구조의 텍스트 표현입니다. 경로에 대한 자세한 내용은 IAM 사용 설명서의 AWS Organizations 개체 경로 이해를 참조하십시오. 이 조건 키 사용에 대한 자세한 내용은 IAM 사용 설명서의 PrincipalOrgPaths aws:를 참조하십시오.

  예를 들어, 다음 조건 요소는 동일한 조직에 있는 두 OU 중 하나의 멤버에 대해 일치합니다.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "aws:PrincipalOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
        ]
    }
}
```

- `organizations:PolicyType` – 이 조건 키를 사용하여 Organizations 정책 관련 API 작업이 특정 유형의 Organizations 정책에서만 동작하도록 제한할 수 있습니다. 이 조건 키는 Organizations 정책과 상호 작용하는 작업이 포함된 모든 정책 문에 적용할 수 있습니다.

  이 조건 키에는 다음 값을 사용할 수 있습니다.

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_POLICY`

예를 들어 다음 예제 정책은 사용자가 모든 Organizations 작업을 수행할 수 있도록 허용합니다. 그러나 사용자가 정책을 인수하는 작업을 수행하는 경우 지정된 정책이 태그 지정 정책인 경우에만 작업이 허용됩니다. 사용자가 다른 유형의 정책을 지정하면 작업이 실패합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal`— 활성화 AWSServiceAccess 또는 비활성화 AWSServiceAccess 작업을 사용하여 다른 AWS 서비스를 통한 신뢰할 수 있는 액세스를 활성화하거나 비활성화하는 경우 조건으로 사용할 수 있습니다. `organizations:ServicePrincipal`을 사용하여 승인된 서비스 보안 주체 이름의 목록에 대하여 이런 작업 요청을 제한할 수 있습니다.

  예를 들어, 다음 정책은 AWS Organizations를 사용하여 신뢰할 수 있는 액세스를 활성화하고 비활성화할 때 사용자가 AWS Firewall Manager만 지정하도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

IAM 정책에서 권한으로 사용할 수 있는 모든 AWS Organizations 특정 조건 키 목록은 서비스 권한 부여 AWS Organizations 참조의 조건 키를 참조하십시오.

리소스 소유권 이해

AWS 계정은 리소스를 누가 생성했는지와 상관없이 계정에서 생성된 리소스를 소유합니다. 특히, 리소스 소유자는 리소스 생성 요청을 인증하는 보안 주체 엔터티(즉, 루트 사용자, IAM 사용자 또는 IAM 역할)의 AWS 계정입니다. AWS 조직의 경우, 이는 언제나 관리 계정이 됩니다. 멤버 계정에서 조직 리소스를 생성 또는 액세스하는 작업은 대부분 호출할 수 없습니다. 다음 예에서는 이러한 작동 방식을 설명합니다.

- 관리 계정의 루트 계정 자격 증명을 사용하여 OU를 생성하는 경우, 관리 계정이 리소스 소유자가 됩니다. (AWS Organizations에서 리소스는 OU입니다.)
- 관리 계정에서 IAM 사용자를 만들고 사용자에 OU 생성 권한을 부여하면, 해당 사용자는 OU를 만들 수 있습니다. 하지만 사용자가 속한 관리 계정이 OU 리소스를 소유합니다.
- 관리 계정에서 OU를 생성할 권한이 있는 IAM 역할을 만드는 경우, 해당 역할을 담당할 수 있는 사람은 누구나 OU를 만들 수 있습니다. 역할(역할을 담당하는 사용자가 아님)이 속하게 될 관리 계정이 OU 리소스를 소유합니다.

리소스 액세스 관리

권한 정책은 누가 무엇에 액세스 할 수 있는지를 나타냅니다. 다음 섹션에서는 권한 정책을 만드는 데 사용 가능한 옵션에 대해 설명합니다.

> **Note**
>
> 이 섹션에서는 AWS Organizations의 맥락에서 IAM을 사용하는 방법에 대해 설명하며, IAM 서비스에 대한 자세한 정보는 다루지 않습니다. IAM 설명서 전체 내용은 IAM 사용 설명서를 참조

하세요. IAM 정책 구문 및 설명에 대한 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 참조를 참조하십시오.

IAM 자격 증명에 연결된 정책을 자격 증명 기반 정책(IAM 정책)이라고 합니다. 리소스에 연결된 정책은 리소스 기반 정책이라고 합니다. AWS Organizations는 자격 증명 기반 정책(IAM 정책)만 지원합니다.

주제

- 자격 증명 기반 권한 정책(IAM 정책)
- 리소스 기반 정책

자격 증명 기반 권한 정책(IAM 정책)

IAM 자격 증명에 정책을 연결하여 해당 자격 증명으로 AWS 리소스에 대한 작업을 수행하도록 허용할 수 있습니다. 예를 들어 다음을 수행할 수 있습니다.

- 계정 내 사용자 또는 그룹에 권한 정책 연결 – 서비스 제어 정책(SCP)이나 OU 같은 AWS Organizations 리소스를 생성할 권한을 사용자에게 부여하려면, 권한 정책을 특정 사용자 또는 해당 사용자가 속한 그룹에 연결하면 됩니다. 사용자나 그룹은 조직의 관리 계정에 있어야 합니다.
- 역할에 권한 정책 연결(교차 계정 권한 부여) – 자격 증명 기반 권한 정책을 IAM 역할에 연결하여 조직에 대한 교차 계정 액세스를 부여할 수 있습니다. 예를 들어 관리 계정 관리자는 다음과 같이 멤버 계정 사용자에게 교차 계정 권한을 부여하는 역할을 만들 수 있습니다.
  1. 관리 계정 관리자는 IAM 역할을 생성하고 조직의 리소스에 권한을 부여하는 역할에 권한 정책을 연결합니다.
  2. 관리 계정 관리자는 멤버 계정 ID를 역할 수임 가능 `Principal`로 식별하는 역할에 신뢰 정책을 연결합니다.
  3. 이후 멤버 계정 관리자는 멤버 계정의 모든 사용자에게 역할을 맡는 권한을 위임할 수 있습니다. 이렇게 하면 멤버 계정 사용자는 관리 계정과 조직의 리소스를 생성하거나 리소스에 액세스할 수 있습니다. 역할을 수임할 수 있는 권한을 AWS 서비스에 부여하고 싶다면, 신뢰 정책의 보안 주체는 AWS 서비스 보안 주체도 될 수 있습니다.

  IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 액세스 관리를 참조하세요.

다음은 사용자가 조직에서 `CreateAccount` 작업을 수행하도록 허용하는 정책의 예입니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

정책의 Resource 요소에 리소스 유형을 가리키는 부분 ARN을 제공할 수도 있습니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

또한 생성 중인 계정에 특정 태그를 포함하지 않는 계정의 생성을 거부할 수도 있습니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
```

```
        }
      }
   ]
}
```

사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM 사용 설명서의 IAM ID (사용자, 사용자 그룹, 역할) 를 참조하십시오.

리소스 기반 정책

Amazon S3와 같은 일부 서비스는 리소스 기반 권한 정책을 지원합니다. 예를 들어, 정책을 Amazon S3 버킷에 연결하여 해당 버킷에 대한 액세스 권한을 관리할 수 있습니다. 현재 AWS Organizations는 리소스 기반 정책을 지원하지 않습니다.

정책 요소 지정: 작업, 조건, 효과, 리소스

각 AWS Organizations 리소스에 대해, 서비스는 API 작업 모음을 정의하거나 특정 방식으로 리소스와 상호작용하거나 리소스를 조작하는 작업을 정의합니다. 이러한 작업에 대한 권한을 부여하기 위해 AWS Organizations에서는 정책에서 지정할 수 있는 작업을 정의합니다. 예를 들어 OU 리소스의 경우 AWS Organizations는 다음처럼 작업을 정의합니다.

- `AttachPolicy` 및 `DetachPolicy`
- `CreateOrganizationalUnit` 및 `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` 및 `DescribeOrganizationalUnit`

단 일부 인스턴스에서는 API 작업을 수행하려면 하나 이상의 작업에 대한 권한과, 하나 이상의 리소스에 대한 권한이 필요할 수도 있다는 점을 기억하세요.

다음은 IAM 권한 정책에서 사용할 수 있는 가장 기본적인 요소입니다.

- 작업(Action) – 이 키워드를 사용하여 허용 또는 거부할 작업을 식별합니다. 예를 들어 지정한 `Effect`에 따라 `organizations:CreateAccount`은 AWS Organizations `CreateAccount` 작업을 수행할 수 있는 사용자 권한을 허용하거나 거부합니다. 자세한 내용은 IAM JSON 정책 요소: IAM 사용 설명서의 작업을 참조하십시오.
- 리소스(Resource) – 이 키워드를 사용하여 정책 문을 적용할 리소스의 ARN을 지정합니다. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 리소스를 참조하십시오.
- 조건(Condition) – 이 키워드를 사용하여 정책 문이 적용되기 위해 충족해야 하는 조건을 지정합니다. `Condition`은 일반적으로 정책이 일치하려면 충족해야 하는 추가 상황을 지정합니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.

- 효과(Effect) – 이 키워드를 사용하여 정책 문이 리소스에 대한 작업을 허용 또는 거부할지를 지정합니다. 명시적으로 리소스에 대한 액세스 권한을 부여(또는 허용)하지 않는다면, 액세스는 암시적으로 거부됩니다. 사용자가 특정 리소스에 대한 특정 작업을 수행하지 못하게 하도록, 다른 정책이 부여한 액세스를 포함한 리소스에 대한 액세스를 명시적으로 거부할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 효과를 참조하십시오.
- 보안 주체(Principal) – 자격 증명 기반 정책(IAM 정책)에서, 해당 정책이 연결된 사용자는 자동으로 묵시적으로 보안 주체가 됩니다. 리소스 기반 정책의 경우 사용자, 계정, 서비스 또는 권한의 수신자인 기타 개체를 지정합니다(리소스 기반 정책에만 해당). 현재 AWS Organizations는 리소스 기반 정책 대신 자격 증명 기반 정책만 지원합니다.

IAM 정책 구문 및 설명에 대한 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 참조를 참조하십시오.

AWS Organizations에 대한 자격 증명 기반 정책(IAM 정책) 사용

조직의 관리 계정 관리자는 권한 정책을 조직 내의 AWS Identity and Access Management(IAM) 자격 증명(사용자, 그룹, 역할)에 연결해 AWS 리소스에 대한 액세스를 제어할 수 있습니다. 권한을 부여하려면 권한을 부여 받을 사용자, 권한 대상이 되는 리소스, 해당 리소스에 허용되는 특정 작업을 결정합니다. 권한을 역할에 부여하면, 해당 역할은 조직 내 다른 계정 사용자가 맡을 수 있습니다.

기본적으로 사용자에게는 어떠한 권한이 없습니다. 모든 권한은 정책에 의해 명시적으로 부여돼야 합니다. 명시적으로 부여되지 않은 권한은 묵시적으로 거부됩니다. 권한이 명시적으로 거부된다면, 권한을 허용한 다른 정책도 모두 무효가 됩니다. 즉, 사용자는 명시적으로 부여되고 명시적으로 거부되지 않은 권한만 가집니다.

이 주제에서 설명한 기본적인 방법 외에도 조직 루트, 조직 단위(OU), 계정, 정책과 같은 조직의 리소스에 적용되는 태그를 사용하여 조직에 대한 액세스를 제어할 수 있습니다. 자세한 정보는 태그와 AWS Organizations를 사용한 속성 기반 액세스 제어을 참조하세요.

사용자에게 전체 관리자 권한 부여

조직의 IAM 사용자에게 전체 AWS Organizations 관리자 권한을 부여하는 IAM 정책을 생성할 수 있습니다. IAM 콘솔에서 JSON 정책 편집기를 사용하여 이 작업을 수행할 수 있습니다.

JSON 정책 편집기를 사용하여 정책을 생성하려면

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.

2. 왼쪽의 탐색 창에서 정책을 선택합니다.

   정책을 처음으로 선택하는 경우 관리형 정책 소개 페이지가 나타납니다. 시작하기를 선택합니다.

3. 페이지 상단에서 정책 생성을 선택합니다.
4. 정책 편집기 섹션에서 JSON 옵션을 선택합니다.
5. 다음 JSON 정책 문서를 입력합니다.

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

6. 다음을 선택합니다.

> **Note**
>
> 언제든지 시각적 편집기 옵션과 JSON 편집기 옵션 간에 전환할 수 있습니다. 그러나 변경을 적용하거나 시각적 편집기에서 다음을 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 정책 재구성을 참조하십시오.

7. 검토 및 생성 페이지에서 생성하는 정책에 대한 정책 이름과 설명(선택 사항)을 입력합니다. 이 정책에 정의된 권한을 검토하여 정책이 부여한 권한을 확인합니다.
8. 정책 생성을 선택하고 새로운 정책을 저장합니다.

IAM 정책 생성에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

작업에 따른 제한적 액세스 부여

전체 권한이 아닌 제한적 권한을 부여하려면, IAM 권한 정책의 `Action` 요소에서 허용할 개별 권한을 나열하는 정책을 만들어야 합니다. 다음 예제와 같이 와일드카드(*) 문자를 사용해 `Describe*`와 `List*` 권한만 부여함으로써 조직에 읽기 전용 액세스를 제공할 수 있습니다.

> **Note**
>
> 서비스 제어 정책(SCP)에서 `Action` 요소에 와일드카드(*) 문자를 단독으로 또는 문자열 끝에 사용할 수 있습니다. 문자열 처음이나 중간에는 표시할 수 없습니다. 따라서 `"servicename:action*"`은 유효하지만 `"servicename:*action"`과 `"servicename:some*action"`은 SCP에서 유효하지 않습니다.

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

IAM 정책에서 할당할 수 있는 모든 권한 목록은 서비스 권한 부여 참조의 AWS Organizations에서 정의한 작업을 참조하십시오.

특정 리소스에 대한 액세스 권한 부여

특정 작업에 대한 액세스를 제한하는 것 외에도 조직의 특정 엔터티에 대한 액세스를 제한할 수 있습니다. 이전 섹션 예제에 등장하는 `Resource` 요소는 모두 와일드카드 문자("*")를 지정하는데, 이는 "작업이 액세스할 수 있는 모든 리소스"라는 뜻입니다. "*"를 액세스를 허용할 특정 엔터티의 Amazon 리소스 이름(ARN)으로 바꿔도 됩니다.

예: 단일 OU에 권한 부여

다음 정책의 첫 번째 문은 IAM 사용자에게 전체 조직에 대한 읽기 전용 액세스 권한을 부여하지만, 두 번째 문은 사용자가 지정된 단일 조직 단위(OU) 내의 AWS Organizations 관리 작업만 수행할 수 있게 합니다. 이는 하위 OU로 확장되지 않습니다. 결제 액세스는 부여되지 않습니다. 이 정책은 OU의 AWS 계정에 대한 관리 액세스 권한을 부여하지 않습니다. 특정한 OU 내에서 계정의 AWS Organizations 작업을 수행할 수 있는 권한만 부여합니다.

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
    }
  ]
}
```

OU와 조직의 ID는 AWS Organizations 콘솔에서 얻거나 `List*` API를 호출해 얻습니다. 이 정책을 적용하는 사용자나 그룹은 특정 OU에 직접적으로 포함된 모든 엔터티에서 모든 작업(`"organizations:*"`)을 수행할 수 있습니다. OU는 Amazon 리소스 이름(ARN)으로 식별합니다.

다양한 리소스의 ARN에 대한 자세한 내용은 서비스 권한 부여 AWS Organizations 참조에 정의된 리소스 유형을 참조하십시오.

제한된 서비스 보안 주체에게 신뢰할 수 있는 액세스를 활성화할 수 있는 권한 부여

정책 문의 `Condition` 요소를 사용하여 정책 문이 일치하는 상황을 추가로 제한할 수 있습니다.

예: 지정된 하나의 서비스에 신뢰할 수 있는 액세스를 활성화하는 권한 부여

다음 문은 사용자가 지정한 서비스에 대해서만 신뢰할 수 있는 액세스를 활성화하도록 권한을 제한하는 방법을 보여 줍니다. 다음과 같이 사용자가 AWS IAM Identity Center의 하나가 아닌 다른 서비스 보안 주체를 사용하여 API를 호출하려 하면 이 정책은 일치하지 않으며 호출이 거부됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

다양한 리소스의 ARN에 대한 자세한 내용은 서비스 권한 부여 AWS Organizations 참조에 정의된 리소스 유형을 참조하십시오.

태그와 AWS Organizations를 사용한 속성 기반 액세스 제어

속성 기반 액세스 제어를 사용하면 AWS 리소스와 AWS 자격 증명 모두에 연결된 태그와 같이 관리자가 관리하는 속성을 사용하여 해당 리소스에 대한 액세스를 제어할 수 있습니다. 예를 들어 사용자와 리소스 모두 특정 태그에 대해 동일한 값을 가질 때 사용자가 리소스에 액세스할 수 있도록 지정할 수 있습니다.

AWS Organizations에서 태그를 지원하는 리소스에는 AWS 계정, 조직의 루트, 조직 단위(OU) 또는 정책이 있습니다. Organizations 리소스에 태그를 연결하면 해당 태그를 사용하여 해당 리소스에 액세스할 수 있는 사용자를 제어할 수 있습니다. 이를 위해 작업을 허용하기 전에 특정 태그 키와 값이 존재하는지 여부를 확인하는 AWS Identity and Access Management(IAM) 권한 정책 문에 `Condition` 요소를 추가합니다. 이렇게 하면 "키 X와 값 Y를 가진 태그가 있는 OU만 사용자가 관리하도록 허용" 또는 "키 Z로 태그 지정되고 사용자의 연결된 태그 키 Z와 동일한 값을 갖는 OU만 사용자가 관리하도록 허용"이라고 효과적으로 언급하는 IAM 정책을 생성할 수 있습니다.

관리자는 IAM 정책의 다양한 태그 참조 유형을 `Condition` 테스트할 수 있습니다.

- 요청에 지정된 리소스에 연결된 태그 확인
- 요청을 수행하는 IAM 사용자 또는 역할에 연결된 태그 확인
- 요청에 파라미터로 포함된 태그 확인

정책에서 액세스 제어를 위해 태그를 사용하는 방법에 대한 자세한 내용은 리소스 태그를 사용하여 IAM 사용자 및 역할에 대한 액세스 제어를 참조하세요. IAM 권한 정책의 전체 구문은 IAM JSON 정책 참조를 참조하세요.

요청에 지정된 리소스에 연결된 태그 확인

AWS Management Console, AWS Command Line Interface(AWS CLI) 또는 AWS SDK 중 하나를 사용해 요청을 할 때 해당 요청으로 액세스하려는 리소스를 지정하게 됩니다. 사용 가능한 특정 유형의

리소스를 나열하거나, 리소스를 읽거나, 쓰거나, 수정하거나, 업데이트할 때 액세스할 리소스를 요청에 파라미터로 지정합니다. 이러한 요청은 사용자 및 역할에 연결한 IAM 권한 정책에 의해 제어됩니다. 이러한 정책에서, 요청된 리소스에 연결된 태그를 비교하고 해당 태그의 키와 값에 따라 액세스를 허용하거나 거부하도록 선택할 수 있습니다.

리소스에 연결된 태그를 확인하려면 태그 키 이름 앞에 `aws:ResourceTag/` 문자열을 추가하여 `Condition` 요소의 태그를 참조합니다.

예를 들어 다음 정책 샘플은 해당 리소스에 키 `department`와 값 `security`를 가진 태그가 없는 한 사용자 또는 역할이 모든 AWS Organizations 작업을 수행하도록 허용합니다. 해당 키와 값이 있는 경우 정책은 `UntagResource` 작업을 명시적으로 거부합니다.

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
    ]
}
```

이 요소를 사용하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 리소스에 대한 액세스 제어 및 aws:ResourceTag를 참조하세요.

요청을 수행하는 IAM 사용자 또는 역할에 연결된 태그 확인

요청을 하는 사람(보안 주체)이 자신의 IAM 사용자 또는 역할에 연결된 태그를 기반으로 수행할 수 있는 대상을 제어할 수 있습니다. 이렇게 하려면 `aws:PrincipalTag/`*`key-name`* 조건 키를 사용하여 호출하는 사용자 또는 역할에 연결해야 할 태그와 값을 지정합니다.

다음 예제는 작업을 호출하는 보안 주체와 작업이 액세스하는 리소스 모두에 대해 지정된 태그(cost-center)가 동일한 값을 갖는 경우에만 작업을 허용하는 방법을 보여줍니다. 이 예제에서 호출하는 사용자는 인스턴스에 사용자와 동일한 cost-center 값으로 태그가 지정된 경우에만 Amazon EC2 인스턴스를 시작하고 중지할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

이 요소를 사용하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 보안 주체에 대한 액세스 제어 및 aws:PrincipalTag를 참조하세요.

요청에 파라미터로 포함된 태그 확인

몇 가지 작업을 통해 태그를 요청의 일부로 지정할 수 있습니다. 예를 들어 리소스를 만들 때 새 리소스에 연결되는 태그를 지정할 수 있습니다. aws:TagKeys를 사용하여 특정 태그 키 또는 키 집합이 요청에 포함되는지 여부에 따라 작업을 허용하거나 거부하는 Condition 요소를 지정할 수 있습니다. 이 비교 연산자는 태그에 포함된 값을 고려하지 않습니다. 지정된 키를 가진 태그가 있는지 여부만 확인합니다.

태그 키 또는 키 목록을 확인하려면 Condition 요소를 다음과 같은 구문으로 지정합니다.

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

ForAllValues:를 사용하면 비교 연산자를 앞에 삽입하여 요청의 모든 키가 정책에 지정된 키 중 하나와 일치하도록 할 수 있습니다. 예를 들어, 다음 정책 샘플은 지정된 태그 키 3개가 모두 요청에 존재하는 경우에만 Organizations 작업을 허용합니다.

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

```
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

또는 ForAnyValue:를 사용해 비교 연산자를 앞에 삽입하여 요청의 하나 이상의 키가 정책에 지정된 키 중 하나와 일치하도록 할 수 있습니다. 예를 들어, 다음 정책은 지정된 태그 키 중 하나 이상이 요청에 존재하는 경우에만 Organizations 작업을 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}
```

몇 가지 작업을 통해 요청에 태그를 지정할 수 있습니다. 예를 들어 리소스를 만들 때 새 리소스에 연결되는 태그를 지정할 수 있습니다. 정책의 태그 키-값 페어를 요청에 함께 포함된 키-값 페어와 비교할 수 있습니다. 이렇게 하려면 태그 키 이름 앞에 문자열(aws:RequestTag/*key-name*)을 삽입하고 존재해야 하는 태그 값을 지정하여 Condition 요소의 태그를 참조합니다.

예를 들어 다음 정책 샘플은 요청에 costcenter 태그가 누락되거나 해당 태그에 1, 2 또는 3 이외의 값이 제공된 경우 AWS 계정을 생성하기 위한 사용자 또는 역할의 모든 요청을 거부합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

이러한 요소를 사용하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 aws:TagKeys 및 aws:RequestTag를 참조하세요.

AWS Organizations의 로깅 및 모니터링

조직에서 변경 사항이 기록되고 있는지 모니터링하는 것이 좋습니다. 그러면 예기치 않은 변경 사항을 검토하고 원치 않는 모든 변경 사항을 롤백할 수 있습니다. AWS Organizations은 현재 2개의 AWS 서비스를 지원하며 이러한 서비스를 통해 조직 및 조직에서 발생하는 작업을 모니터링할 수 있습니다.

주제

AWS CloudTrail를 사용하여 AWS Organizations API 호출 로깅

AWS Organizations(은)는 AWS Organizations에서 사용자, 역할, 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail(와)과 통합됩니다. CloudTrail은 AWS Organizations 콘솔의 호출 및 AWS Organizations API에 대한 코드 호출을 포함하여 AWS Organizations에 대한 모든 API 호출을 이벤트로 캡처합니다. 추적을 생성하면 AWS Organizations 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 AWS Organizations에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

> **Important**
>
> AWS Organizations에 대한 모든 CloudTrail 정보는 미국 동부(버지니아 북부) 리전에서만 볼 수 있습니다. CloudTrail 콘솔에 AWS Organizations 활동이 표시되지 않는 경우에는 오른쪽 상단 모서리의 메뉴를 사용하여 미국 동부(버지니아 북부)로 콘솔을 설정합니다. AWS CLI 또는 SDK 도구로 CloudTrail을 쿼리하는 경우에는 미국 동부(버지니아 북부) 엔드포인트로 쿼리를 보냅니다.

CloudTrail의 AWS Organizations 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. AWS Organizations에서 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 정보는 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AWS Organizations에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. AWS 계정에서 CloudTrail 로깅을 활성화하면 AWS Organizations 작업에 대한 API 호출이 CloudTrail 로그 파일에서 추적되어 다른 AWS 서비스 레코드와 함께 여기에 기록됩니다. 기타 AWS 서비스를 구

성하여 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리할 수도 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에서 Amazon SNS 알림 구성

모든 AWS Organizations 작업은 CloudTrail에서 로깅되고 AWS Organizations API 참조에 기록됩니다. 예를 들어 `CreateAccount`(`CreateAccountResult` 이벤트 포함), `ListHandshakesForAccount`, `CreatePolicy`, `InviteAccountToOrganization`을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 로그 항목은 누가 요청을 생성했는가에 대한 정보가 들어 있습니다. 로그 항목의 사용자 신원 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자로 했는지 IAM 사용자 자격 증명으로 했는지 여부
- IAM 역할 또는 연합된 사용자용 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청했는지 여부

자세한 설명은 CloudTrail userIdentity 요소를 참조하세요.

AWS Organizations 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

로그 항목 예: CloseAccount

다음 예제는 API가 호출되고 계정을 생성하기 위한 워크플로가 백그라운드에서 처리를 시작할 때 해지되는 `CloseAccount` 호출 샘플에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
```

```
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

다음 예제는 계정 해지를 위한 백그라운드 워크플로가 성공적으로 완료된 후 `CloseAccountResult` 호출에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
```

```
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

로그 항목 예: CreateAccount

다음 예제는 API가 호출되고 계정을 생성하기 위한 워크플로가 백그라운드에서 처리를 시작할 때 생성되는 `CreateAccount` 호출 샘플의 CloudTrail 로그 항목을 보여 줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

다음 예제는 계정 생성을 위한 백그라운드 워크플로가 성공적으로 완료된 후 `CreateAccount` 호출의 CloudTrail 로그 항목을 보여줍니다.

```
{
```

```
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

다음 예제는 계정 생성을 위한 백그라운드 워크플로가 성공적으로 완료된 후 `CreateAccount` 호출의 CloudTrail 로그 항목을 보여 줍니다.

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
```

```
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

로그 항목의 예: CreateOrganizationalUnit

다음 예제에서는 샘플 `CreateOrganizationalUnit` 호출의 CloudTrail 로그 항목을 보여 줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
```

```
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

로그 항목의 예: InviteAccountToOrganization

다음 예제에서는 샘플 `InviteAccountToOrganization` 호출의 CloudTrail 로그 항목을 보여 줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
```

```
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
```

```
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

로그 항목의 예: AttachPolicy

다음 예제에서는 샘플 `AttachPolicy` 호출의 CloudTrail 로그 항목을 보여 줍니다. 요청한 정책 유형이 연결 요청을 시도한 루트에서 활성화되지 않았기 때문에 응답에서 호출이 실패했다고 표시됩니다.

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
```

```
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Amazon EventBridge

AWS Organizations가 Amazon EventBridge(이전 Amazon CloudWatch Events)와 함께 작동하여 관리자가 지정한 작업이 조직에서 발생하면 이벤트를 트리거합니다. 예를 들어 작업의 중요성 때문에 대부분의 관리자는 사용자가 조직에 새 계정을 만들 때마다 또는 멤버 계정의 관리자가 조직을 탈퇴하려고 할 때 경고를 표시하려고 합니다. 이 작업을 찾는 EventBridge 규칙을 구성한 후 관리자가 정의한 대상으로 생성된 이벤트를 보낼 수 있습니다. 대상은 해당 구독자에게 이메일 또는 문자 메시지를 보내는 Amazon SNS 주제가 될 수 있습니다. 나중에 검토할 수 있도록 작업의 세부 정보를 로깅하는 AWS Lambda 함수를 만들 수도 있습니다.

EventBridge에서 조직의 주요 활동을 모니터링하도록 설정하는 방법을 보여 주는 자습서는 자습서: Amazon EventBridge를 사용하여 조직에 대한 중요 변경 사항 모니터링을(를) 참조하세요.

구성 및 활성화 방법 등 EventBridge에 대해 자세히 알아보려면 Amazon EventBridge 사용 설명서를 참조하세요.

AWS Organizations의 규정 준수 확인

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

AWS Organizations의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전에서는 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 대기 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 가용 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.

AWS Organizations의 인프라 보안

관리형 서비스인 AWS Organizations는 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 호출을 사용하여 네트워크를 통해 Organizations에 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.

명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하세요.

AWS Organizations 참조

이 단원의 항목을 통해 AWS Organizations의 다양한 요소에 대한 자세한 참조 자료를 찾아보십시오.

주제

- 에 대한 할당량 AWS Organizations
- AWS Organizations에 사용할 수 있는 AWS 관리형 정책

에 대한 할당량 AWS Organizations

이 단원에서는 AWS Organizations에 영향을 미치는 할당량을 설명합니다.

이름 지정 지침

다음은 계정 이름 AWS Organizations, 조직 단위 (OU), 루트 및 정책을 포함하여 생성하는 이름에 대한 지침입니다.

- 유니코드 문자로 구성되어야 합니다
- 이름의 최대 문자열 길이는 객체에 따라 다릅니다. 각각에 대한 실제 제한을 보려면 AWS Organizations API 참조에서 객체를 생성하는 API 작업을 찾아보세요. 해당 작업의 `Name` 파라미터에 대한 세부 정보를 확인합니다. 예: 계정 이름 또는 OU 이름.

최대 및 최소 값

다음은 에 있는 엔티티의 AWS Organizations기본 최대값입니다.

> **Note**
>
> Service Quotas 콘솔을 사용하여 이러한 값 중 일부에 대해 상향을 요청할 수 있습니다. Organizations는 미국 동부(버지니아 북부) 리전(`us-east-1`)에 물리적으로 호스팅되어 있는 글로벌 서비스입니다. 따라서 Service Quotas 콘솔, AWS CLI또는 SDK를 사용할 때 조직 할당량에 액세스하는 `us-east-1` 데 사용해야 합니다. AWS

조직 내 인원수 AWS 계정	10는 조직에 허용된 기본 최대 계정 수입니다. 더 필요한 경우 Service Quotas 콘솔을 사용하여 증가를 요청할 수 있습니다.

	계정으로 전송되는 초대 개수는 이 할당량을 기준으로 계산됩니다. 초대된 계정에서 초대를 거부하면 해당 카운트가 반환되고 관리 계정이 초대를 취소하거나 초대가 만료됩니다. 새로 생성된 계정 및 조직의 경우 할당량이 기본값인 계정 10개 미만일 수 있습니다.
조직의 루트 개수	1
조직의 OU 개수	1000
조직 내 각 유형별 정책 개수	AI 서비스 옵트아웃 정책: 1000 백업 정책: 1000 서비스 제어 정책: 2000 태그 정책: 1000
정책 문서의 최대 크기	AI 서비스 옵트아웃 정책: 2,500자 백업 정책: 10,000자 서비스 제어 정책: 5,120자 태그 정책: 10,000자 참고: 를 사용하여 정책을 저장하면 JSON 요소 사이 및 따옴표 밖의 추가 공백 (예: 공백 및 줄 바꿈) 은 제거되며 계산에 포함되지 않습니다. AWS Management Console SDK 작업 또는 를 사용하여 정책을 저장하면 정책은 제공된 그대로 저장되며 문자가 자동으로 제거되지 않습니다. AWS CLI
루트의 OU 최대 중첩 수	루트 아래 5개 레벨의 OU 깊이

24시간 동안 수행할 수 있는 최대 초대 횟수입니다.	20개, 또는 조직에 허용된 최대 계정 수 중 더 큰 수입니다. 수락된 초대는 이 할당량에 포함되지 않습니다. 하나의 초대가 수락되는 즉시 다른 초대를 같은 날에 전송할 수 있습니다. 조직에 허용되는 최대 계정 수가 20개 미만인 경우 조직이 수용할 수 있는 것보다 더 많은 계정을 초대하려고 하면 "계정 제한 초과" 예외가 발생합니다. 그러나 초대를 취소하고 하루에 최대 20회까지 새 초대장을 보낼 수 있습니다.
동시에 만들 수 있는 멤버 계정의 수	5 — 한 계정의 생성이 끝나면 바로 다른 계정 생성을 시작할 수 있지만, 한 번에 5개의 계정 생성만 진행 가능.
30일 동안 해지할 수 있는 멤버 계정의 수	조직 구성원 계정의 10%, 최대 1000개 • 100개 미만의 계정 - 멤버 계정을 최대 10개까지 해지할 수 있습니다. • 계정 100~10,000개 — 회원 계정의 최대 10% 를 폐쇄할 수 있습니다. • > 10,000개 계정 — 최대 1,000개의 회원 계정을 폐쇄할 수 있습니다. 예를 들어 회원 계정이 10,500개인 경우 30일 기간 동안 최대 1,000개(1050개 아님) 의 계정을 폐쇄할 수 있습니다. 이 할당량에 도달한 후에는 AWS Billing 콘솔에서 계정을 추가로 해지하거나 해당 할당량이 초기화될 때까지 대기할 수 있습니다. 자세한 내용은 계정 관리 가이드의 계정을 폐쇄하기 전에 알아야 할 사항을 참조하십시오.AWS
동시에 해지할 수 있는 멤버 계정의 수	3 - 동시에 3개까지만 해지할 수 있습니다. 한 계정의 해지를 완료한 후, 곧바로 다른 계정을 해지할 수 있습니다.
정책에 연결할 수 있는 엔터티 개수	무제한
루트, OU 또는 계정에 연결할 수 있는 태그 수	50
리소스 기반 위임 정책의 최대 크기	4만 자

핸드셰이크 만료 시간

악수 시작 제한 시간은 다음과 같습니다. AWS Organizations

조직 참여 초대	15일
조직의 모든 기능 활성화 요청	90일
핸드셰이크가 삭제되고 더 이상 목록에 표시되지 않습니다.	30일 이후에 핸드셰이크가 실행됩니다.

엔터티에 연결할 수 있는 정책 수

최소값 및 최대값은 정책 유형과 정책을 연결하는 엔터티에 따라 다릅니다. 다음 표는 각 정책 유형과 각 유형을 연결할 수 있는 개체 수를 보여줍니다.

> **Note**
>
> 이러한 수는 OU 또는 계정에 직접 연결된 정책에만 적용됩니다. 상속이 OU 또는 계정에 영향을 미치는 정책은 이러한 제한에 포함되지 않습니다.

정책 유형	앤터티에 연결된 최소값	루트에 연결된 최대값	OU별로 연결된 최대값	계정별로 연결된 최대값
서비스 제어 정책	1 — 모든 엔터티에는 언제나 SCP가 하나 이상 연결되어 있어야 합니다. 개체의 마지막 SCP는 제거할 수 없습니다.	5	5	5
AI 서비스 옵트아웃 정책	0	5	5	5

정책 유형	앤터티에 연결된 최소값	루트에 연결된 최대값	OU별로 연결된 최대값	계정별로 연결된 최대값
백업 정책	0	10	10	10
태그 정책	0	10	10	10

> **Note**
> 현재 조직은 루트를 하나만 가질 수 있습니다.

제한 한계

다음 표에는 관리 범주별 AWS Organizations API가 나열되어 있으며 계정 및 조직 수준에서의 각 스로틀 비율이 나와 있습니다.

AWS Organizations API	계정당 한도 (속도, 버스트)	조직당 한도 (속도, 버스트)
계정 관리		
CloseAccount	0.5, 1	
CreateAccount, CreateGovCloudAccount	0.1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10
핸드셰이크 관리		
AcceptHandshake, DescribeHandshake	1, 1	

AWS Organizations API	계정당 한도 (속도, 버스트)	조직당 한도 (속도, 버스트)
CancelHandshake	2, 3	
DeclineHandshake	1, 3	
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10
조직 관리		
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	
DescribeOrganizationalUnit	2, 2	2, 3
ListAccounts	8, 12	9, 15
ListChildren	6, 10	7, 12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5, 8	6, 10
ListRoots	1, 2	1, 3
ListTagsForResource	10, 15	12, 18
RemoveAccountFromOrganization	2, 2	

AWS Organizations API	계정당 한도 (속도, 버스트)	조직당 한도 (속도, 버스트)
TagResource, UntagResource	4, 6	
정책 관리		
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	2, 2	2, 3
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5, 8	6, 10
UpdatePolicy	2, 3	
서비스 관리		
활성화AWSServiceAccess, 비활성화 AWSServiceAccess	1, 2	
목록AWSServiceAccessForOrganization, ListDelegatedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator	1, 2	

AWS Organizations에 사용할 수 있는 AWS 관리형 정책

이 단원에서는 사용자가 조직을 관리하는 데 사용할 수 있는 AWS 관리형 정책을 살펴봅니다. AWS 관리 정책을 수정 또는 삭제할 순 없지만, 필요에 따라 조직에 엔터티를 연결하거나 분리할 수는 있습니다.

AWS Organizations(IAM)에 사용할 수 있는 AWS Identity and Access Management 관리형 정책

IAM 관리형 정책은 AWS에서 제공하고 관리합니다. 관리형 정책은 관리형 정책을 적절한 IAM 사용자 또는 역할 객체에 연결하여 사용자에게 할당할 수 있는 일반 작업에 대한 권한을 제공합니다. 정책을 직접 작성할 필요가 없으며 새로운 서비스를 지원하기 위해 AWS가 적절하게 정책을 업데이트하면 자동으로 즉시 업데이트의 이점을 얻을 수 있습니다. AWS 관리형 정책 목록은 IAM 콘솔의 정책(Policies) 페이지에서 볼 수 있습니다. 정책 필터 드롭다운을 사용해 AWS 관리형을 선택합니다.

다음의 관리형 정책을 사용하여 조직의 사용자에게 권한을 부여할 수 있습니다.

정책 이름	설명	ARN
AWSOrganizationsFullAccess	조직을 생성하고 완전히 관리하는 데 필요한 모든 권한을 제공합니다. 이 정책 설명의 내용은 다음 코드 조각에 나와 있습니다.	arn:AWS:iam: :AWS:정책/AWSOrganizationsFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSOrganizationsFullAccess",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*"
        },
        {
            "Sid": "AWSOrganizationsFullAccessAccount",
            "Effect": "Allow",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:GetAlternateContact",
```

정책 이름	설명	ARN

```
                "account:
GetContactInformation",
                "account:
PutContactInformation",
                "account:
ListRegions",
                "account:
EnableRegion",
                "account:
DisableRegion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSOrgan
izationsFullAccessCreateSLR
",
            "Effect": "Allow",
            "Action":
 "iam:CreateServiceLinkedRol
e",
            "Resource": "*",
            "Condition": {
                "StringEq
uals": {
                    "iam:AWSS
erviceName": "organiza
tions.amazonaws.com"
                }
            }
        }
    ]
}
```

정책 이름	설명	ARN

AWSOrganizationsReadOnlyAccess	조직 관련 정보에 대한 읽기 전용 액세스를 제공합니다. 사용자가 변경할 수 없습니다. 이 정책 설명의 내용은 다음 코드 조각에 나와 있습니다.
	
	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Sid": "AWSOrganizationsReadOnly",
	"Effect":"Allow",
	"Action":[
	"organizations:Describe*",
	"organizations:List*"
	],
	"Resource": "*"
	},
	{
	"Sid": "AWSOrganizationsReadOnlyAccount",
	"Effect":"Allow",
	"Action":[
	"account:GetAlternateContact",
	"account:GetContactInformation",
	"account:ListRegions"
	],
	"Resource": "*"
	}
	]
	}
		arn:aws:iam: :aws:policy/AWSOrganizationsReadOnlyAccess

Organizations AWS 관리형 정책으로 업데이트

다음 표에는 이 서비스가 변경 사항을 추적하기 시작한 이후의 AWS 관리형 정책 업데이트에 대해 상세히 설명되어 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Organizations 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSOrganizationsFullAccess— 정책 설명을 설명하는 요소를 포함하도록 업데이트되었습니다. `Sid`	Organizations는 `AWSOrganizationsFullAccess` 관리형 정책에 대한 `Sid` 요소를 추가했습니다.	2024년 2월 6일
AWSOrganizationsReadOnlyAccess— 정책 설명을 설명하는 `Sid` 요소를 포함하도록 업데이트되었습니다.	Organizations는 `AWSOrganizationsReadOnlyAccess` 관리형 정책에 대한 `Sid` 요소를 추가했습니다.	2024년 2월 6일
AWSOrganizationsFullAccess— Organizations 콘솔을 AWS 리전 통해 활성화하거나 비활성화하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정에 대해 리전을 활성화하거나 비활성화하기 위한 쓰기 액세스를 활성화할 수 있도록 Organizations의 정책에 `account:ListRegions` , `account:EnableRegion` 및 `account:DisableRegion` 작업이 추가되었습니다.	2022년 12월 22일
AWSOrganizationsReadOnlyAccess— Organizations 콘솔을 AWS 리전 통해 목록에 등록하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 리전을 보기 위한 액세스를 활성화할 수 있도록 Organizations의 정책에 `account:ListRegions` 작업이 추가되었습니다.	2022년 12월 22일
AWSOrganizationsFullAccess— Organizations 콘솔을 통해 계정 연락처를 추가하거나 편집하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 연락처를 수정하기 위한 쓰기 액세스를 활성화할 수 있도록 Organizations의 정책에 `account:GetContactInformation` 및 `account:PutContactInformation` 작업이 추가되었습니다.	2022년 10월 21일

변경 사항	설명	날짜
AWSOrganizationsReadOnlyAccess— Organizations 콘솔을 통해 계정 연락처를 보는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 연락처를 보기 위한 액세스를 활성화할 수 있도록 Organizations의 정책에 `account:GetContactInformation` 작업이 추가되었습니다.	2022년 10월 21일
AWSOrganizationsFullAccess— 조직을 만들 수 있도록 업데이트되었습니다.	Organizations가 조직을 생성하는 데 필요한 서비스 연결 역할 생성을 지원하기 위해 `CreateServiceLinkedRole` 권한을 정책에 추가했습니다. 이 권한은 `organizations.amazonaws.com` 서비스에서만 사용할 수 있는 역할을 생성하는 것으로 제한됩니다.	2022년 8월 24일
AWSOrganizationsFullAccess— Organizations 콘솔을 통해 계정 대체 연락처를 추가, 편집 또는 삭제하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 대체 연락처를 수정하기 위한 쓰기 액세스를 활성화할 수 있도록 Organizations의 정책에 `account:GetAlternateContact`, `account:DeleteAlternateContact`, `account:PutAlternateContact` 작업이 추가되었습니다.	2022년 2월 7일
AWSOrganizationsReadOnlyAccess— Organizations 콘솔을 통해 계정 대체 연락처를 보는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 대체 연락처를 보기 위한 액세스를 활성화할 수 있도록 Organizations의 정책에 `account:GetAlternateContact` 작업이 추가되었습니다.	2022년 2월 7일

AWS Organizations 관리 서비스 제어 정책

서비스 제어 정책(SCP)은 IAM 권한 정책과 비슷하지만, IAM이 아닌 AWS Organizations의 기능입니다. SCP를 사용하여 영향을 받는 엔터티의 최대 권한을 지정합니다. SCP는 조직 내의 루트, 조직 단위

(OU)나 계정에 연결할 수 있습니다. 직접 생성할 수도 있고, IAM이 정의하는 정책을 사용할 수도 있습니다. Organizations 콘솔의 정책(Policies) 페이지에서 조직의 정책 목록을 확인할 수 있습니다.

> **Important**
>
> 모든 루트, OU와 계정에는 언제나 하나 이상의 SCP가 연결돼 있어야 합니다.

정책 이름	설명	ARN
전체 AWSAccess	멤버 계정에 대한 AWS Organizations 관리 계정 액세스를 제공합니다.	arn:AWS:조직: :AWS:정책/서비스_제어_정책/P-전체 AWSAccess

AWS Organizations 문제 해결

AWS Organizations 작업 시 문제가 발생한다면 이 섹션의 주제를 참조하세요.

주제

일반적인 문제 해결

이 문서의 정보를 사용하여 AWS Organizations 작업 시 발생할 수 있는 액세스 거부 또는 기타 일반적인 문제를 진단하고 해결할 수 있습니다.

주제

AWS Organizations에 요청하면 "액세스 거부" 메시지가 표시됩니다.

- 요청한 작업 및 리소스를 호출할 권한이 있는지 확인하세요. 관리자가 IAM 정책을 자신의 사용자, 그룹 또는 역할에 연결해 권한을 부여해야 합니다. 이러한 권한을 부여하는 정책 명령문에 시간이나 IP 주소 제한 정책이 포함된다면, 요청을 전송할 때 이러한 요구사항을 충족해야 합니다. 사용자, 그룹 또는 역할에 대한 정책을 확인 또는 수정하는 방법은 IAM 사용 설명서에 있는 정책 작업 섹션을 참조하세요.
- (AWS SDK를 사용하지 않고) API 요청에 수동으로 서명할 경우, 요청에 올바르게 서명했는지 확인합니다.

임시 보안 자격 증명으로 요청하면 "액세스 거부" 메시지가 표시됩니다

- 요청을 위해 사용 중인 사용자나 역할에 올바른 권한이 있는지 확인합니다. 임시 보안 자격 증명의 권한은 사용자 또는 역할에서 파생되므로 사용자 또는 역할에 부여된 권한으로 제한됩니다. 임시 보안 자격 증명의 권한이 결정되는 방법에 대한 자세한 내용은 IAM 사용 설명서의 임시 보안 자격 증명을 위한 권한 제어 섹션을 참조하세요.
- 요청에 올바르게 서명했고 요청이 잘 구성되었는지 확인합니다. 자세한 내용은 선택한 SDK의 도구 키트 문서나 IAM 사용 설명서의 임시 보안 자격 증명을 이용해 AWS 리소스에 대한 액세스 요청 단원을 참조하세요.
- 임시 보안 자격 증명이 만료되지 않았는지 확인합니다. 자세한 내용은 IAM 사용 설명서의 임시 보안 자격 증명 요청 섹션을 참조하세요.

멤버 계정으로 조직을 나가거나 관리 계정으로 멤버 계정을 제거하려고 하면 "액세스 거부" 메시지가 표시됩니다

- 멤버 계정에서 결제에 대한 IAM 사용자 액세스를 활성화한 후에만 멤버 계정을 제거할 수 있습니다. 자세한 내용은 AWS Billing 사용 설명서의 Billing and Cost Management 콘솔에 대한 액세스 활성화를 참조하세요.
- 계정에 독립형 계정으로 실행하는 데 필요한 정보가 있는 경우에만 조직에서 계정을 제거할 수 있습니다. AWS Organizations 콘솔, API 또는 AWS CLI 명령을 사용하여 조직에서 계정을 생성한 경우에는 정보가 자동으로 수집되지 않습니다. 독립형으로 만들려는 각 계정마다 AWS 고객 계약서에 동의하고 지원 계획을 선택하고 필요한 계약 정보를 제공 및 확인하며 현재 결제 방법을 제공해야 합니다. AWS에서는 이 결제 수단을 사용해 해당 계정이 조직에 연결되어 있지 않을 때 발생하는 모든 청구 가능한 AWS 활동(AWS 프리 티어 이외)에 대해 비용을 청구합니다. 자세한 정보는 멤버 계정에서 조직 탈퇴을 참조하세요.

조직에 계정을 추가하려고 하면 "할당량 초과" 메시지가 표시됩니다.

조직에서 최대로 보유할 수 있는 계정 수는 제한되어 있습니다. 삭제 또는 종료된 계정은 이 할당량을 기준으로 계속 계산됩니다.

가입 초대는 조직의 최대 계정 수를 기준으로 계산됩니다. 초대된 계정에서 초대를 거부하면 해당 카운트가 반환되고 관리 계정이 초대를 취소하거나 초대가 만료됩니다.

- AWS 계정을 해지하거나 삭제하기 전에 조직에서 계정을 제거해야 합니다. 그래야 해당 계정이 할당량에 포함되어 계산되지 않습니다.

- 할당량 증가를 요청하는 방법에 대한 자세한 내용은 최대 및 최소 값 단원을 참조하세요.

계정을 추가 또는 제거할 때 "이 작업에는 대기 시간이 필요합니다."라는 메시지가 표시됩니다.

일부 작업에는 대기 기간이 필요합니다. 예를 들어 새로 생성한 계정을 즉시 제거할 수는 없습니다. 며칠 후에 다시 작업을 시도하세요. 계정을 추가 및 제거하는 동안 계정 할당량에 관한 문제가 발생할 경우 최대 및 최소 값에서 할당량 증가를 요청하는 방법을 확인하세요.

조직에 계정을 추가하려고 하면 "조직이 아직 초기화 중임"이라는 메시지가 표시됩니다.

조직을 생성한 지 1시간 이상 지난 상태에서 이 오류를 수신한 경우 AWS Support에 문의하세요.

내 조직에 계정을 초대하려고 할 때 “초대장이 비활성화되었습니다.”라는 메시지가 표시됩니다.

이 문제는 조직에서 모든 기능을 활성화하는 경우에 발생합니다. 이 작업은 시간이 걸릴 수 있으며 모든 멤버 계정이 응답해야 합니다. 작업이 완료될 때까지 새 계정을 조직에 가입하도록 초대할 수 없습니다.

변경 사항이 매번 즉시 표시되는 것은 아닙니다.

사용자들이 전세계 데이터 센터의 컴퓨터들을 통해 액세스하는 서비스인 AWS Organizations은 최종 일관성이라고 하는 분산 컴퓨팅 모델을 사용합니다. AWS Organizations에서 변경한 사항을, 가능한 모든 엔드포인트에서 보게 될 때까지는 시간이 걸립니다. 일부 지연은 서버에서 서버로, 또는 복제 영역에서 복제 영역으로 데이터를 보내는 데 걸리는 시간으로 인해 발생합니다. 또한 AWS Organizations는 캐싱을 사용하여 성능을 개선하지만 이 경우 중 몇몇 경우는 더 많은 시간이 소요될 수 있습니다. 이러한 변화는 이전에 캐싱된 데이터가 끝날 때까지 가시화되지 않을 수 있습니다.

한 위치에서 변경한 내용이 다른 위치에서 즉시 보이지 않을 때조차도 전역 애플리케이션이 이러한 잠재적 지연을 설명하고 예상대로 작동하도록 설계하세요.

이로 인해 일부 다른 AWS 서비스가 받게 되는 영향에 대한 자세한 정보는 다음 자료를 참고하세요.

- Amazon Redshift 데이터베이스 개발자 안내서의 데이터 일관성 관리
- Amazon Simple Storage Service 사용 설명서의 Amazon S3 데이터 일관성 모델

- AWS 빅 데이터 블로그의 ETL 워크플로에 대해 Amazon S3 및 Amazon Elastic MapReduce 사용 시 일관성 유지
- Amazon EC2 API 참조의 EC2 최종 일관성

AWS Organizations 정책 문제 해결

이 곳의 정보를 사용하여 AWS Organizations 정책에서 발견되는 일반적인 오류를 진단하고 해결하세요.

서비스 제어 정책

AWS Organizations의 서비스 제어 정책(SCP)은 IAM 정책과 유사하며 같은 구문을 사용합니다. 이 구문은 JavaScript Object Notation(JSON) 규칙으로 시작합니다. JSON은 객체를 구성하는 이름과 값 쌍으로 객체를 설명합니다. IAM 정책 문법은 정책을 사용하여 권한을 부여하는 AWS 서비스에 따라 이름과 값의 의미를, 그리고 인식할 수 있는 이름과 값을 지정함으로써 JSON을 기반으로 생성됩니다.

AWS Organizations는 IAM 구문과 문법의 하위 집합을 사용합니다. 자세한 내용은 단원을 참조하세요SCP 구문

공통 정책 오류

- 정책 객체가 하나 이상인 경우
- Statement 요소가 하나 이상인 경우
- 정책 문서가 최대 크기를 초과함

정책 객체가 하나 이상인 경우

SCP는 단 하나의 JSON 객체로 구성되어야 합니다. 객체는 중괄호 { }로 묶어 표시합니다. 대괄호 [ ] 안에 중괄호 { }를 추가로 삽입하여 JSON 객체 내에 다른 객체를 중첩시킬 수도 있지만 정책에 따라 중괄호 { }를 묶는 대괄호 [ ]는 하나로 제한됩니다. 다음 예제는 올바르지 않은데, 최상위 레벨에 (###으로 호출한) 객체 2개가 있기 때문입니다.

```
{
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
```

```
      "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

하지만 올바른 정책 문법을 사용하여 이전 예제의 의도를 만족하는 방법도 있습니다. 2개의 정책 객체에 Statement 요소를 각각 추가하지 않고 두 블록을 단일 Statement 요소로 결합하면 됩니다. 그러면 다음 예제와 같이 Statement 요소가 두 객체 배열을 값으로 인식합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

이 예제는 서로 효과가 다른 요소 2개가 있어 요소가 하나인 Statement로 추가 압축할 수 없습니다. 일반적으로 각 문의 Effect와 Resource 요소가 같을 때만 문을 결합할 수 있습니다.

Statement 요소가 하나 이상인 경우

이 오류는 처음에는 이전 섹션에 나온 오류의 변형처럼 보일지도 모릅니다. 하지만 구문으로 보면 다른 유형의 오류입니다. 다음 예제를 보면 중괄호 { } 한 쌍이 최상위 레벨로 정책 객체 하나만 표시하고 있습니다. 하지만 객체에 포함된 Statement 요소는 2개입니다.

SCP는 콜론 왼쪽의 이름(Statement)과 오른쪽의 값으로 구성된 Statement 요소 1개만 포함해야 합니다. 그리고, Statement 요소의 값은 Effect 요소 1개와 Action 요소 1개, 그리고 Resource 요

소 1개가 중괄호 { }로 묶여 구성된 객체가 되어야 합니다. 다음은 예제는 올바르지 않은데, 정책 객체에 Statement 요소 2개가 있기 때문입니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

값 객체는 다수의 값 객체 배열이 될 수 있으므로 이 문제는 다음 예제와 같이 Statement 요소 2개를 객체 배열을 통해 하나의 요소로 결합하여 해결할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

Statement 요소 값이 객체 배열이 되었습니다. 예제의 배열은 두 객체로 구성되며, 각 객체 자체가 정확한 Statement 요소 값으로 인식됩니다. 배열을 구성하는 각 객체는 쉼표로 구분합니다.

정책 문서가 최대 크기를 초과함

SCP 문서의 최대 크기는 5,120자입니다. 이 최대 크기는 공백을 포함하여 모든 문자를 포함합니다. SCP의 크기를 줄이려면 인용 부호 바깥에 있는 공백 문자(예: 공백 및 줄 바꿈)를 모두 제거할 수 있습니다.

HTTP 쿼리 요청을 통한 API 호출

이 단원에는 AWS Organizations용 쿼리 API 사용에 대한 일반적인 정보가 포함되어 있습니다. API 작업 및 오류에 대한 자세한 정보는 AWS Organizations API 참조를 참조하세요.

> **Note**
>
> AWS Organizations 쿼리 API를 직접 호출하는 대신 AWS SDK 중 하나를 사용할 수도 있습니다. AWS SDK는 다양한 프로그래밍 언어 및 플랫폼(Java, Ruby, .NET, iOS, Android 등)을 위한 라이브러리와 샘플 코드로 구성되어 있습니다. SDK를 사용하면 편리하게 AWS Organizations 및 AWS에 프로그래밍 방식으로 액세스할 수 있습니다. 예를 들어 SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. 다운로드 및 설치 방법을 비롯하여 AWS SDK에 대한 자세한 내용은 Amazon Web Services용 도구 페이지를 참조하세요.

AWS Organizations용 쿼리 API를 사용하면 서비스 작업을 호출할 수 있습니다. 쿼리 API 요청은 수행할 작업을 나타내기 위해 `Action` 파라미터를 포함해야 하는 HTTPS 요청입니다. AWS Organizations에서는 모든 작업에 대해 GET과 POST 요청을 지원합니다. 즉, API 사용 시 어떤 작업에는 GET을 사용하고 또 어떤 작업에는 POST를 사용할 필요가 없습니다. 하지만 GET 요청에는 URL 크기 제한이 적용됩니다. 제한은 브라우저에 따라 다르지만, 일반적으로 2,048바이트입니다. 따라서 더 큰 크기가 필요한 쿼리 API 요청의 경우 POST 요청을 사용해야 합니다.

응답은 XML 문서입니다. 응답에 대한 자세한 정보는 AWS Organizations API 참조의 개별 작업 페이지를 참조하세요.

주제

엔드포인트

AWS Organizations에는 미국 동부(버지니아 북부) 리전에서 호스팅되는 글로벌 API 엔드포인트 하나가 있습니다.

모든 서비스의 AWS 엔드포인트 및 리전에 대한 자세한 내용은 의 리전 엔드포인트를 참조하십시오. AWS 일반 참조

HTTPS 필요

쿼리 API는 보안 자격 증명과 같이 민감한 정보를 반환하므로 HTTPS를 이용해 모든 API 요청을 암호화해야 합니다.

AWS Organizations API 요청에 서명

액세스 키 ID와 보안 액세스 키를 사용하여 요청에 서명해야 합니다. AWS Organizations를 사용한 일상적인 작업에는 AWS 계정 루트 사용자 보안 인증 정보를 사용하지 않는 것이 좋습니다. 그 대신 사용자나 역할의 보안 인증 정보를 사용하면 됩니다.

API 요청에 서명하려면 AWS 서명 버전 4를 사용해야 합니다. Signature Version 4 사용에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청에 서명을 참조하세요.

AWS Organizations는 서명 버전 2와 같은 이전 버전은 지원하지 않습니다.

자세한 내용은 다음을 참조하세요.

- AWS 보안 자격 증명 – AWS 액세스를 위해 사용 가능한 자격 증명 유형에 대한 일반 정보를 제공합니다.
- IAM의 보안 모범 사례 - AWS Organizations의 리소스를 비롯해 AWS 리소스를 보호할 수 있도록 IAM 서비스 사용에 대한 제안 사항을 제공합니다.
- IAM의 임시 자격 증명 – 임시 보안 자격 증명을 생성하고 사용하는 방법에 대해 설명합니다.

AWS Organizations에 대한 문서 기록

다음 표에서는 본 AWS Organizations 관련 주요 설명서 업데이트를 설명합니다.

- API 버전: 2016-11-28

변경 사항	설명	날짜
업데이트된 정책 설명	AWS Organizations관리형 정책 설명에 새 `Sid` 요소를 추가했습니다.	2024년 2월 6일
새로운 클로즈 매니지먼트 어카운트 주제	관리 계정을 폐쇄하는 방법을 안내하는 고려 사항 및 세부 단계에 대한 링크를 추가했습니다.	2024년 2월 1일
추가된 모범 사례	IAM 모범 사례에 부합할 수 있도록 유용하고 새로운 정보가 모범 사례 섹션에 추가되었습니다.	2023년 6월 12일
AWSOrganizationsFullAccess 및 AWSOrganizationsReadOnlyAccess 관리형 정책 업데이트	두 관리형 정책 모두 계정의 연락처에 대한 쓰기 또는 읽기 액세스를 허용하도록 업데이트되었습니다.	2022년 10월 21일
AWSOrganizationsFullAccess 관리형 정책이 업데이트되었습니다.	새 조직에 필요한 서비스 연결 역할을 만드는 데 필요한 권한을 추가하여 조직을 만들 수 있도록 관리형 정책이 업데이트되었습니다.	2022년 8월 24일
AWS Organizations 콘솔을 통해 계정을 해지할 수 있는 기능을 제공합니다.	관리 계정의 보안 주체는 AWS Organizations 콘솔을 통해 멤버 계정을 해지하고 IAM 정책을 사용하여 실수로 해지되지	2022년 3월 29일

	않도록 멤버 계정을 보호합니다.	
AWS Organizations 콘솔을 사용하여 대체 연락처를 업데이트하도록 공지 사항을 업데이트했습니다.	이제 Organizations는 AWS Organizations 콘솔을 사용하여 조직 내 계정의 대체 연락처를 업데이트하는 기능을 제공합니다. 새로운 기능을 발표하고 지침으로 계정 관리 참조를 제공하십시오.	2022년 2월 8일
Organizations 관리형 정책 업데이트 - 기존 정책에 대한 업데이트	AWS Organizations콘솔을 통해 계정 대체 연락처를 업데이트하거나 보는 데 필요한 계정 API 권한을 허용하도록 AWSOrganizationsFullAccess 및 AWSOrganizationsReadOnlyAccess 관리형 정책을 업데이트했습니다.	2022년 2월 7일
Amazon DevOps Guru와의 조직 통합	Amazon DevOps Guru와 AWS Organizations 통합하여 모든 조직 계정의 애플리케이션 상태를 전체적으로 모니터링하고 통찰력을 얻을 수 있습니다.	2022년 1월 3일
Organizations와 Amazon Detective 통합	Amazon Detective와 AWS Organizations를 통합하여 Detective 동작 그래프가 모든 조직 계정의 활동에 대한 가시성을 제공하게 할 수 있습니다.	2021년 12월 16일

Organizations와 AWS Config의 통합으로 이제 다중 계정 다중 리전 데이터 집계를 지원합니다.	위임된 관리자 계정을 사용하여 조직 내 모든 멤버 계정의 리소스 구성 및 규정 준수 데이터를 집계할 수 있습니다. 자세한 내용은 AWS Config 개발자 안내서에서 다중 계정 다중 리전 데이터 집계를 참조하세요.	2021년 6월 16일
Organizations와 AWS Firewall Manager의 통합에 이제 위임된 관리자에 대한 지원이 포함됩니다.	이제 조직의 멤버 계정을 전체 조직의 Firewall Manager 관리자로 지정할 수 있습니다. 이를 통해 조직의 관리 계정으로부터 권한을 더 잘 분리할 수 있습니다.	2021년 4월 30일
Organizations 백업 정책이 이제 연속 백업을 지원합니다.	AWS Backup 연속 백업 기능을 조직의 백업 정책과 함께 사용할 수 있습니다.	2021년 3월 10일
Organizations와 AWS CloudFormation StackSets 의 통합에 이제 위임된 관리자에 대한 지원이 포함됩니다.	이제 조직의 구성원 계정을 전체 조직의 AWS CloudFormation StackSets 관리자로 지정할 수 있습니다. 이를 통해 조직의 관리 계정으로부터 권한을 더 잘 분리할 수 있습니다.	2021년 2월 18일
전체 기능을 활성화하는 동안 계속해서 계정 초대	AWS가 조직의 모든 기능을 활성화하는 프로세스를 업데이트했습니다. 이제 기존 계정이 초대장에 응답할 때까지 기다리는 동안 조직에 가입할 새 계정을 계속 초대할 수 있습니다.	2021년 2월 3일
AWS Organizations 콘솔 버전 2.0 도입	AWS가 새 버전의 AWS 콘솔을 도입했습니다. 새 작업 수행 방법을 반영하도록 모든 설명서를 업데이트했습니다.	2021년 1월 21일

이제 Organizations에서 AWS Marketplace와의 통합을 지원	이제 AWS Marketplace를 사용하여 조직의 모든 계정에서 소프트웨어 라이선스를 보다 쉽게 공유할 수 있습니다.	2020년 12월 3일
이제 Organizations에서 Amazon S3 Lens와의 통합을 지원	Amazon S3 Lens는 Organizations에서 신뢰할 수 있는 액세스와 위임된 관리자를 지원합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 Storage Lens를 참조하세요.	2020년 11월 18일
교차 계정 백업 복사본	백업 정책을 사용하여 조직의 리소스를 백업할 때 이제 백업 복사본을 조직 내 다른 AWS 계정에 백업할 수 있습니다.	2020년 11월 18일
중국의 AWS 리전에서 이제 AWS Resource Access Manager를 Organizations의 신뢰할 수 있는 서비스로 지원합니다.	이제 중국에서 Organizations와 AWS RAM을(를) 사용할 때 Organizations와 통합된 AWS RAM 기능을 신뢰할 수 있는 서비스로 사용할 수 있습니다.	2020년 11월 18일
이제 Organizations에서 AWS Security Hub와의 통합을 지원	조직의 모든 계정에서 Security Hub를 사용하도록 설정하고, 조직의 멤버 계정 중 하나를 Security Hub에 대한 위임된 관리자 계정으로 지정할 수 있습니다.	2020년 11월 12일
마스터 계정의 이름이 변경됨	AWS Organizations에서 '마스터 계정'을 '관리 계정'이라는 이름으로 변경했습니다. 이름만 변경되었을 뿐 기능은 바뀌지 않았습니다.	2020년 10월 20일

새로운 모범 사례 단원 및 주제	AWS Organizations의 모범 사례에 대한 새로운 단원을 추가했습니다. 새 단원에는 관리 계정/멤버 계정 루트 사용자 및 암호 관리에 대한 모범 사례를 설명하는 주제가 포함되었습니다.	2020년 10월 6일
새로운 모범 사례 단원과 처음 두 페이지 추가됨	AWS Organizations의 모범 사례를 설명하는 주제를 위한 새로운 단원이 생겼습니다. 이 업데이트에는 조직의 관리 계정의 모범 사례에 대한 주제와, 멤버 계정의 모범 사례에 대한 주제가 포함되었습니다.	2020년 10월 2일
Organizations 백업 정책이 이제 Windows EC2 인스턴스에서 VSS(Volume Shadow Copy Service)를 사용한 애플리케이션 일관성 보장 백업을 지원합니다.	백업 정책에서 새로운 `advanced_backup_settings "` 섹션이 지원됩니다. 새로운 이 섹션의 첫 번째 항목은 `WindowsVSS` 라는 `ec2` 설정이며, 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 AWS Backup 개발자 안내서의 VSS 지원 Windows 백업 생성을 참조하세요.	2020년 9월 24일
조직은 태그 기반 액세스 제어를 지원합니다 tag-on-create .	Organizations 리소스를 만들 때 태그를 해당 리소스에 추가할 수 있습니다. 태그 정책을 사용하여 Organizations 리소스에 대한 태그 사용을 표준화할 수 있습니다. 태그 키 및 값을 지정한 리소스로만 액세스를 제한하는 IAM 정책을 사용할 수 있습니다.	2020년 9월 15일

AWS Health를 신뢰할 수 있는 서비스로 추가했습니다.	조직 내 계정 전반의 AWS Health 이벤트를 집계할 수 있습니다.	2020년 8월 4일
인공 지능(AI) 서비스 옵트아웃 정책	AI 서비스 옵트아웃 정책을 사용하여 AWS AI 서비스가 AWS AI 서비스 및 기술의 개발 및 지속적인 개선을 위해 해당 서비스에서 처리하는 고객 콘텐츠(AI 콘텐츠)를 저장하고 사용할 수 있는지 여부를 제어할 수 있습니다.	2020년 7월 8일
백업 정책 및 AWS Backup와의 통합이 추가되었습니다.	백업 정책을 사용하여 조직 내 모든 계정에서 백업 정책을 만들고 적용할 수 있습니다.	2020년 6월 24일
IAM Access Analyzer의 위임된 관리를 지원합니다.	조직의 액세스 분석기에 대한 관리 액세스를 지정된 멤버 계정에 위임할 수 있습니다.	2020년 3월 30일
AWS CloudFormation과 통합 StackSets	서비스 관리형 스택 세트를 생성하여 AWS Organizations에서 관리되는 계정에 스택 인스턴스를 배포할 수 있습니다.	2020년 2월 11일
Compute Optimizer와의 통합	Compute Optimizer가 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2020년 2월 4일
태그 정책	태그 정책을 사용하여 조직의 계정에 있는 리소스 전체에서 태그를 표준화할 수 있습니다.	2019년 11월 26일
Systems Manager와의 통합	Systems Manager Explorer에서 조직의 모든 AWS 계정 계정 간에 작업 데이터를 동기화할 수 있습니다.	2019년 11월 26일

aws: PrincipalOrgPaths	새 전역 조건 키는 요청을 하는 IAM 사용자, IAM 역할 또는 AWS 계정 루트 사용자의 AWS Organizations 경로를 확인합니다.	2019년 11월 20일
AWS Config 규칙과 통합	AWS Config API 작업을 사용하여 조직의 모든 AWS 계정에 걸쳐 AWS Config 규칙을 관리할 수 있습니다.	2019년 7월 8일
신뢰할 수 있는 액세스를 위한 새로운 서비스	Service Quotas가 사용자 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2019년 6월 24일
AWS Control Tower와 통합	AWS Control Tower가 사용자 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2019년 6월 24일
AWS Identity and Access Management과 통합	IAM은 조직의 엔터티(조직 루트, OU 및 계정)에 대해 마지막으로 액세스한 데이터를 서비스에 제공합니다. 이 데이터를 사용하여 필요한 AWS 서비스로만 액세스를 제한할 수 있습니다.	2019년 6월 20일
계정 태그 지정	조직의 계정에 태그를 지정 및 지정 취소하여 조직의 계정에 지정된 태그를 볼 수 있습니다.	2019년 6월 6일
서비스 제어 정책(SCP)의 리소스, 조건 및 NotAction 요소	이제 SCP에서 리소스, 조건 및 NotAction 요소를 지정하여 조직 또는 조직 단위(OU)의 계정 전체에서 액세스를 거부할 수 있습니다.	2019년 3월 25일

신뢰할 수 있는 액세스를 위한 새로운 서비스	AWS License Manager 및 Service Catalog가 사용자 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2018년 12월 21일
신뢰할 수 있는 액세스를 위한 새로운 서비스	AWS CloudTrail 및 AWS RAM가 사용자 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2018년 12월 4일
신뢰할 수 있는 액세스를 위한 새로운 서비스	AWS Directory Service가 사용자 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2018년 9월 25일
이메일 주소 확인	기존 계정을 조직에 초대하려면 먼저 관리 계정과 연결된 이메일 주소의 소유자임을 입증해야 합니다.	2018년 9월 20일
CreateAccount 알림	`CreateAccount` 알림은 관리 계정의 CloudTrail 로그에 게시됩니다.	2018년 6월 28일
신뢰할 수 있는 액세스를 위한 새로운 서비스	AWS Artifact가 사용자 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2018년 6월 20일
신뢰할 수 있는 액세스를 위한 새로운 서비스	AWS Config 및 AWS Firewall Manager가 사용자 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2018년 4월 18일

신뢰할 수 있는 서비스 액세스	이제는 사용자의 조직 내 계정으로 작업할 수 있는 일부 AWS 서비스에 대한 액세스를 활성화 또는 비활성화할 수 있습니다. IAM Identity Center는 일차적으로 지원되는 신뢰할 수 있는 서비스입니다.	2018년 3월 29일
계정 제거가 이제는 셀프 서비스	이제 AWS Support에 연락하지 않아도 AWS Organizations에서 생성했던 계정을 제거할 수 있습니다.	2017년 12월 19일
새로운 서비스 AWS IAM Identity Center에 대해 추가된 지원	이제 AWS Organizations에서 AWS IAM Identity Center(IAM Identity Center)과의 통합을 지원합니다.	2017년 12월 7일
AWS가 모든 조직 계정에 서비스 연결 역할 추가	서비스 연결 역할(`AWSServiceRoleForOrganizations`)이 조직의 모든 계정에 추가되어 AWS Organizations과 기타 AWS 서비스 사이의 통합이 가능합니다.	2017년 10월 11일
이제 생성된 계정 제거 가능	고객은 이제 AWS Support의 도움을 통해 조직에서 생성된 계정을 제거할 수 있습니다.	2017년 6월 15일
서비스 시작	새로운 서비스 시작과 함께 제공된 AWS Organizations 설명서의 최초 버전입니다.	2017년 2월 17일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하세요.

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