참조 안내서

AWS 어카운트 매니지먼트

AWS 어카운트 매니지먼트: 참조 안내서

Table of Contents

AWS계정 관리 참조 가이드에 오신 것을 환영합니다

AWS 계정AWS서비스 액세스의 기본 부분입니다.

An은 다음과 같은 두 가지 기본 기능을 AWS 계정 제공합니다.

- 컨테이너 — AWS 계정 An은 AWS 고객으로서 생성하는 모든 AWS 리소스의 기본 컨테이너입니다. 예를 들어, 아마존 심플 스토리지 서비스 (Amazon S3) 버킷, 아마존 관계형 데이터베이스 서비스 (아마존 RDS) 데이터베이스, 아마존 Elastic Compute Cloud (Amazon EC2) 인스턴스는 모두 리소스입니다. 모든 리소스는 리소스를 포함하거나 소유한 계정의 계정 ID를 포함하는 Amazon 리소스 이름 (ARN) 으로 고유하게 식별됩니다.
- 보안 경계 — AWS 계정 An은 리소스의 기본 보안 경계이기도 합니다. AWS 계정에서 생성한 리소스는 계정의 자격 증명이 있는 사용자가 사용할 수 있습니다.

  계정에서 만들 수 있는 주요 리소스에는 사용자 및 역할과 같은 ID가 있습니다. ID에는 누군가가 로그인 (인증) 하는 데 사용할 수 있는 자격 증명이 있습니다. AWS 또한 ID에는 사용자가 계정의 리소스로 수행할 수 있는 작업 (권한 부여) 을 지정하는 권한 정책이 있습니다.

  보안 모범 사례로, 사용자가 액세스할 AWS 때 임시 자격 증명을 사용하도록 요구하십시오. 임시 자격 증명을 제공하려면 페더레이션 및 ID 공급자 (예: AWS IAM Identity Center (IAM Identity Center)) 를 사용할 수 있습니다. 회사에서 이미 ID 공급자를 사용하고 있다면 페더레이션과 함께 사용하여 조직 내 리소스에 대한 액세스를 제공하는 방법을 단순화하십시오AWS 계정.

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

주제

여러 기능이 필요합니까?AWS 계정?

AWS 계정기본 보안 경계 역할을 합니다.AWS. 유용한 수준의 격리를 제공하는 리소스 컨테이너 역할을 합니다. 리소스와 사용자를 격리하는 기능은 안전하고 잘 관리되는 환경을 구축하기 위한 핵심 요구 사항입니다.

리소스를 별도의 리소스로 분리AWS 계정클라우드 환경에서 다음 원칙을 지원하는 데 도움이 됩니다.

- 보안 제어— 애플리케이션마다 서로 다른 보안 프로파일을 가질 수 있으며, 이에 따라 다른 제어 정책과 메커니즘이 필요합니다. 예를 들어 감사원과 대화하고 단일 심사를 가리키는 것이 훨씬 쉽습니다.AWS 계정대상 워크로드의 모든 요소를 호스팅하는 경우신용카드 업계 (PCI) 보안 표준.
- 격리— AnAWS 계정보안 보호 단위입니다. 잠재적 위험과 보안 위협은AWS 계정다른 사람에게 영향을 미치지 않습니다. 팀 또는 보안 프로필이 다르기 때문에 보안 요구 사항이 다를 수 있습니다.
- 여러 팀— 팀마다 각기 다른 책임과 자원 요구가 있습니다. 팀을 분리하여 서로 간섭하는 것을 방지할 수 있습니다.AWS 계정.
- 데이터 격리— 팀을 격리하는 것 외에도 데이터 저장소를 계정에 격리하는 것이 중요합니다. 이렇게 하면 해당 데이터 저장소에 액세스하고 관리할 수 있는 사용자 수를 제한할 수 있습니다. 이를 통해 고도의 개인 데이터에 대한 노출을 방지할 수 있으므로유럽연합의 일반 데이터 보호 규정 (GDPR).
- 비즈니스 프로세스— 사업부 또는 제품마다 목적과 프로세스가 완전히 다를 수 있습니다. 여러 사용AWS 계정사업부의 특정 요구 사항을 지원할 수 있습니다.
- 결제— 계정은 결제 수준에서 항목을 분리할 수 있는 유일한 방법입니다. 여러 계정을 사용하면 업무 단위, 직무 팀 또는 개별 사용자 간에 청구 수준에서 항목을 분리할 수 있습니다. 모든 청구서를 단일 지불자에게 통합할 수 있습니다 (AWS Organizations라인 항목을 다음과 같이 구분하는 동안 통합 결제)AWS 계정.
- 할당량 할당–AWS서비스 할당량은 각각에 대해 별도로 적용됩니다.AWS 계정. 워크로드를 다른 워크로드로 분리AWS 계정서로 할당량을 소비하지 못하게 합니다.

이 문서에 설명된 모든 권장 사항 및 절차는AWSWell-Architected. 이 프레임워크는 유연하고 탄력적이며 확장 가능한 클라우드 인프라를 설계하는 데 도움이 됩니다. 소규모로 시작하는 경우에도 프레임워크에서 이 지침을 준수하는 것이 좋습니다. 이렇게 하면 성장에 따라 지속적인 운영에 영향을 주지 않으면서 환경을 안전하게 확장할 수 있습니다.

여러 관리AWS 계정

여러 계정을 추가하기 전에 계정을 관리하기 위한 플랜을 개발해야 합니다. 이를 위해 다음과 같이 하는 것이 좋습니다.AWS Organizations는 무료입니다.AWS모든 것을 관리하는 서비스AWS 계정조직에서

AWS또한 제공AWS Control Tower을 (를) 추가하는 레이어AWS조직으로의 자동화 관리 및 자동으로 다른 조직과 통합AWS다음과 같은 서비스AWS CloudTrail,AWS ConfigAmazon CloudWatchAWS Service Catalog, 그리고 다른 사람. 이러한 서비스는 추가 비용이 발생할 수 있습니다. 자세한 내용은AWS Control Tower요금을 참조하세요.

시작하기: 처음 AWS 사용하시나요?

를 처음 사용하는 경우 첫 번째 단계는 가입하는 AWS 계정 것입니다. AWS 가입하면 입력한 세부 AWS 계정 정보로 계정을 AWS 만들고 계정을 할당합니다. 를 생성한 후 루트 사용자로 로그인하고 루트 사용자에 대한 멀티 팩터 인증 (MFA) 을 활성화하고 사용자에게 관리자 액세스 권한을 할당합니다. AWS 계정

Steps

- 필수 조건
- 1단계: 계정 만들기 AWS 계정
- 2단계: 루트 사용자를 위한 MFA 활성화
- 3단계: 관리자 사용자 생성
- 관련 주제

필수 조건

가입하려면 다음 정보가 필요합니다. AWS 계정

- 계정 이름 — 계정 이름은 청구서와 같은 여러 위치와 Billing and Cost Management 대시보드, 콘솔과 같은 콘솔에 AWS Organizations 표시됩니다.

  쉽게 알아볼 수 있는 계정 이름을 지정할 수 있도록 표준 방식으로 계정 이름을 지정하는 것이 좋습니다. 회사 계정의 경우 조직 - 목적 - 환경 (예: - 감사 AnyCompany- 제품) 과 같은 이름 지정 표준을 사용하는 것이 좋습니다. 개인용 계정의 경우 이름, 성, 목적 (예:) 과 같은 이름 지정 표준을 사용하는 것이 좋습니다. paulo-santos-testaccount

  계정 이름 변경에 대한 자세한 내용은 내 AWS 계정 계정의 이름을 변경하려면 어떻게 해야 하나요? 를 참조하십시오. .
- 주소 — 연락처 주소가 인도인 경우 계정의 사용자 계약은 인도 현지 AWS 판매자인 Amazon Internet Services Private Limited (AISPL) 과 체결합니다. 확인 과정의 일환으로 CVV를 제공해야 합니다. 은행에 따라 일회용 비밀번호를 입력해야 할 수도 있습니다. AISPL은 확인 프로세스의 일환으로 결제 방법에 2 INR을 청구합니다. 확인을 완료한 후 AISPL은 2 INR을 환불합니다.
- 이메일 주소 — 이메일 주소는 루트 사용자의 로그인 이름으로 사용되며 계정 복구에 필요합니다. 이 주소로 전송된 이메일 메시지를 받을 수 있어야 합니다. 특정 작업을 수행하려면 먼저 이 주소로 전송된 이메일에 액세스할 수 있는지 확인해야 합니다.

> **Important**
>
> 이 계정이 기업용 계정인 경우, 직원이 직위를 변경하거나 퇴사하는 AWS 계정 경우에도 회사에서 계속 액세스할 수 있도록 안전한 회사 배포 목록 (예:`it.admins@example.com`) 을 사용하십시오. 이메일 주소를 사용하여 계정의 루트 사용자 자격 증명을 재설정할 수 있으므로 이 배포 목록 또는 주소에 대한 액세스를 보호하십시오.

- 전화번호 - 이 번호를 사용하여 계정 소유권을 확인할 수 있습니다. 이 전화번호로 전화를 받을 수 있어야 합니다.

> **Important**
>
> 이 계정이 기업용 계정인 경우, 직원이 직위를 변경하거나 퇴사하는 AWS 계정 경우에도 회사에서 계속 액세스할 수 있도록 회사 전화번호를 사용하십시오.

1단계: 계정 만들기 AWS 계정

1. 브라우저에서 AWS홈페이지를 엽니다.
2. 만들기를 선택합니다AWS 계정.

> **Note**
>
> AWS최근에 로그인한 경우 로그인을 선택합니다. 새로 만들기 옵션이 보이지 AWS 계정 않으면 먼저 다른 계정으로 로그인을 선택한 다음 새로 만들기를 선택합니다AWS 계정.

3. 계정 정보를 입력한 다음 이메일 주소 확인을 선택합니다. 그러면 지정한 이메일 주소로 확인 코드가 전송됩니다.
4. 확인 코드를 입력한 다음 확인을 선택합니다.
5. 루트 사용자의 강력한 암호를 입력하고 확인한 다음 계속을 선택합니다. AWS암호는 다음 조건을 충족해야 합니다.
   - 최소 8자에서 최대 128자여야 합니다.
   - 대문자, 소문자, 숫자,! 등 다양한 문자 유형 중 최소 세 개를 포함해야 합니다. @ # $% ^ & * () <> [] {} | _+-= 기호.
   - AWS 계정이름 또는 이메일 주소와 동일하지 않아야 합니다.

6. 비즈니스용 또는 개인용을 선택합니다. 이러한 옵션의 차이는 당사가 요청하는 정보입니다. 두 계정 유형 모두 동일한 특징과 기능을 가지고 있습니다.
7. 비즈니스 또는 개인 정보를 입력합니다. 이메일 주소 및 전화번호에 대한 사전 요구 사항 섹션의 권장 사항을 참조하십시오.
8. AWS고객 계약을 읽고 동의하십시오. AWS고객 계약 약관을 읽고 이해했는지 확인하십시오.
9. 계속을 선택합니다. 이제 사용할 준비가 되었음을 확인하는 이메일 메시지를 받게 AWS 계정 됩니다. 가입 시 제공한 이메일 주소와 비밀번호를 사용하여 새 계정에 로그인할 수 있습니다. 하지만 계정 활성화를 마칠 때까지는 AWS 서비스를 이용할 수 없습니다.
10. 결제 방법에 대한 정보를 입력합니다. 청구 목적으로 다른 주소를 사용하려면 새 주소 사용을 선택합니다.
11. 확인 및 계속를 선택합니다.
12. 목록에서 국가 또는 지역 코드를 입력한 다음 몇 분 내에 연락할 수 있는 전화번호를 입력합니다. CAPTCHA 코드를 입력하고 제출하십시오.
13. 자동 시스템에서 연락이 오면 받은 PIN을 입력한 다음 제출하십시오.
14. AWS Support플랜을 선택하세요. 사용 가능한 요금제에 대한 설명은 요금제 AWS Support비교를 참조하십시오.
15. 가입 완료를 선택합니다. 계정이 활성화되고 있음을 나타내는 확인 페이지가 나타납니다.
16. 이메일 및 스팸 폴더에서 계정이 활성화되었음을 확인하는 이메일 메시지를 확인하세요. 활성화에는 보통 몇 분이 걸리지만 때로는 최대 24시간이 걸릴 수도 있습니다.

    활성화 메시지를 받으면 모든 AWS 서비스에 완전히 액세스할 수 있습니다.

> **Note**
>
> 계정 활성화에 문제가 있는 경우 을 참조하십시오the section called “계정 생성 문제”.

2단계: 루트 사용자를 위한 MFA 활성화

루트 사용자를 위해 MFA를 활성화하는 것이 좋습니다. MFA를 사용하면 누군가가 승인 없이 계정에 액세스할 위험을 크게 낮출 수 있습니다.

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

루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS로그인 사용 설명서의 루트 AWS Management Console 사용자로 로그인을 참조하십시오.

2. 루트 사용자를 위해 MFA를 활성화합니다.

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

3단계: 관리자 사용자 생성

루트 사용자가 수행할 수 있는 작업은 제한할 수 없으므로 루트 사용자가 명시적으로 필요하지 않은 작업에는 루트 사용자를 사용하지 않는 것이 좋습니다. 대신 IAM Identity Center의 관리자에게 관리 액세스 권한을 할당하고 해당 관리자로 로그인하여 일상적인 관리 작업을 수행하십시오.

지침은 IAM ID 센터 사용 설명서의 IAM ID 센터 관리 사용자에 대한 AWS 계정 액세스 설정을 참조하십시오.

관련 주제

- 루트 사용자 자격 증명을 보호하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 루트 사용자의 자격 증명 보안을 참조하십시오.
- 루트 사용자가 필요한 작업 목록은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오.

AWS 계정 루트 사용자 사용

> **Important**
>
> AWS 계정에 대한 루트 사용자 보안 인증을 보유한 사람은 누구든지 결제 정보를 포함하여 해당 계정의 모든 리소스에 무제한으로 액세스할 수 있습니다.

AWS 계정을 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 ID로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태

스크를 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 Tasks that require root user credentials를 참조하세요.

일상적인 작업에 루트 사용자를 사용하지 않으려면 에서 관리자 사용자를 설정하는 방법을 알아보십시오AWS IAM Identity Center. 추가 루트 사용자 보안 권장 사항은 해당 지역의 루트 사용자 모범 사례를 참조하십시오 AWS 계정.

루트 사용자 암호를 변경 또는 재설정하고 루트 사용자의 액세스 키 (액세스 키 ID 및 보안 액세스 키)를 생성 또는 삭제할 수 있습니다. 루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS로그인 사용 설명서의 루트 AWS Management Console 사용자로 로그인을 참조하십시오.

당신의 것을 관리하세요AWS 계정

이 섹션에는 관리 방법을 설명하는 항목이 포함되어 있습니다.AWS 계정.

> **Note**
>
> 만약 당신의AWS 계정다음을 사용하여 인도에서 만들어졌습니다.Amazon Internet Services Private Limited(AISPL), 추가 고려 사항이 있습니다. 자세한 정보는 인도 내 계정 관리 단원을 참조하세요.

주제

- 독립형 만들기 AWS 계정
- AWS 계정 식별자 보기
- 루트 사용자의 AWS 계정 이름, 이메일 주소 또는 암호 업데이트
- API 작동 모드 이해
- 업데이트하기AWS 계정연락처 정보
- 보안 챌린지 질문 업데이트
- 어떤 계정을 사용할 수 있는지 AWS 리전 지정하십시오.
- AWS 계정별칭 생성 또는 업데이트
- 청구서 보기AWS 계정
- 인도 내 계정 관리
- 팬 닫기 AWS 계정

독립형 만들기 AWS 계정

이 항목에서는 에서 관리하지 AWS 계정 않는 독립형을 만드는 방법을 설명합니다. AWS Organizations 에서 관리하는 조직에 속하는 계정을 만들려면 AWS Organizations사용 설명서의 조직에 구성원 계정 만들기를 참조하십시오. AWS Organizations

이 지침은 인도 AWS 계정 외부에서 계정을 생성하기 위한 것입니다. 인도에서 계정을 만들려면 을 참조하십시오생성하기AWS 계정AISPL과 함께.

AWS Management Console

AWS 계정 생성

1. Amazon Web Services 홈 페이지를 엽니다.
2. 생성을 선택합니다AWS 계정.

> **Note**
>
> AWS최근에 로그인한 경우 해당 옵션이 없을 수 있습니다. 대신 콘솔에 로그인을 선택하십시오. 그런 다음 새로 만들기가 AWS 계정 여전히 보이지 않으면 먼저 다른 계정으로 로그인을 선택한 다음 새로 만들기를 선택합니다AWS 계정.

3. 계정 정보를 입력한 다음 이메일 주소 확인을 선택합니다. 그러면 지정한 이메일 주소로 확인 코드가 전송됩니다.

> **Important**
>
> 계정 루트 사용자의 중요한 특성 때문에 개인이 아닌 그룹이 액세스할 수 있는 이메일 주소를 사용하는 것이 좋습니다. 이렇게 하면 가입한 사람이 AWS 계정 퇴사하더라도 이메일 주소에 계속 액세스할 AWS 계정 수 있으므로 계속 사용할 수 있습니다.
> 연결된 이메일 주소에 액세스할 수 없는 경우 비밀번호를 분실해도 계정에 대한 액세스 권한을 복구할 수 없습니다. AWS 계정

4. 확인 코드를 입력한 다음 확인을 선택합니다.
5. 루트 사용자의 강력한 암호를 입력하고 확인한 다음 계속을 선택합니다. AWS암호는 다음 조건을 충족해야 합니다.
   - 최소 8자, 최대 128자여야 합니다.
   - 대문자, 소문자, 숫자, 기호(! @ # $ % ^ & * () <> [] {} | _+-=) 중 적어도 세 가지 문자 유형을 혼합하여 포함해야 합니다.
   - AWS 계정 이름 또는 이메일 주소와 동일하지 않아야 합니다.
6. 비즈니스 또는 개인용을 선택합니다. 개인용 계정과 업무용 계정의 특징과 기능은 동일합니다.
7. 회사 또는 개인 정보를 입력합니다.

> **Important**
>
> 비즈니스의 AWS 계정 경우 다음을 입력하는 것이 가장 좋습니다.

- 개인용 전화의 경우 번호가 아닌 회사 전화번호입니다.
- 계정을 사용할 회사 또는 조직의 도메인 이름이 포함된 전자 메일 주소.

계정의 루트 사용자를 개별 이메일 주소 또는 개인 전화번호로 구성하면 계정이 안전하지 않을 수 있습니다.

8. AWS고객 계약을 읽고 동의하십시오. AWS고객 계약 약관을 읽고 이해했는지 확인하십시오.
9. 계속을 선택합니다. 이제 사용할 준비가 되었음을 확인하는 이메일 메시지를 받게 AWS 계정 됩니다. 가입 시 제공한 이메일 주소와 비밀번호를 사용하여 새 계정에 로그인할 수 있습니다. 하지만 계정 활성화를 마칠 때까지는 AWS 서비스를 이용할 수 없습니다.
10. 결제 방법에 대한 정보를 입력한 다음 확인 및 계속을 선택합니다. AWS청구 정보에 다른 청구지 주소를 사용하려면 새 주소 사용을 선택합니다.

    유효한 결제 방법을 추가하기 전까지는 가입 절차를 진행할 수 없습니다.
11. 목록에 있는 국가 또는 지역 코드를 입력한 다음 몇 분 내에 연락할 수 있는 전화번호를 입력합니다.
12. CAPTCHA에 표시된 코드를 입력한 다음 제출하십시오.
13. 자동 시스템에서 연락이 오면 받은 PIN을 입력한 다음 제출하십시오.
14. 사용 가능한 AWS Support 플랜 중 하나를 선택합니다. 사용 가능한 Support 플랜 및 혜택에 대한 설명은 AWS Support플랜 비교를 참조하십시오.
15. 가입 완료를 선택합니다. 계정이 활성화되고 있음을 나타내는 확인 페이지가 나타납니다.
16. 이메일 및 스팸 폴더에서 계정이 활성화되었음을 확인하는 이메일 메시지를 확인하세요. 활성화에는 보통 몇 분이 걸리지만 때로는 최대 24시간이 걸릴 수도 있습니다.

    활성화 메시지를 받으면 모든 AWS 서비스에 완전히 액세스할 수 있습니다.

AWS CLI & SDKs

조직의 관리 계정에 로그인한 상태에서 CreateAccount작업을 AWS Organizations 실행하여 관리되는 조직의 구성원 계정을 만들 수 있습니다.

AWS Command Line Interface(AWS CLI) 또는 AWS API 작업을 사용하여 조직 AWS 계정 외부에서 독립형 계정을 만들 수는 없습니다.

AWS 계정 식별자 보기

AWS 각각에 다음과 같은 고유 식별자를 할당합니다. AWS 계정

AWS 계정 ID

를 고유하게 식별하는 12자리 숫자 (예: 012345678901) 입니다. AWS 계정많은 AWS 리소스는 Amazon 리소스 이름 (ARN) 에 계정 ID를 포함합니다. 계정 ID 부분은 한 계정의 리소스를 다른 계정의 리소스와 구분합니다. AWS Identity and Access Management (IAM) 사용자인 경우 계정 ID 또는 계정 별칭을 AWS Management Console 사용하여 에 로그인할 수 있습니다. 계정 ID는 다른 식별 정보와 마찬가지로 신중하게 사용하고 공유해야 하지만 비밀, 민감한 정보 또는 기밀 정보로 간주되지 않습니다.

표준 사용자 ID

ID의 난독화된 형태인 영숫자 식별자 (예79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be:) AWS 계정 Amazon Simple Storage Service (Amazon S3) 를 사용하여 버킷과 객체에 대한 교차 계정 액세스 권한을 부여하는 AWS 계정 경우를 이 ID를 사용하여 식별할 수 있습니다. 루트 사용자 또는 IAM 사용자의 표준 사용자 ID를 검색할 수 있습니다 AWS 계정 .

이러한 식별자를 보려면 인증을 받아야 합니다 AWS .

> **Warning**
>
> AWS 리소스를 공유하기 위해 AWS 계정 식별자가 필요한 제3자에게 AWS 자격 증명 (암호 및 액세스 키 포함) 을 제공하지 마십시오. 그렇게 하면 귀하와 동일한 액세스 권한을 상대방에게 부여할 수 있습니다. AWS 계정

AWS 계정 신분증 찾기

AWS Management Console 또는 AWS Command Line Interface (AWS CLI) 를 사용하여 AWS 계정 ID를 찾을 수 있습니다. 콘솔에서 계정 ID의 위치는 루트 사용자로 로그인했는지 IAM 사용자로 로그인했는지에 따라 달라집니다. 계정 ID는 루트 사용자로 로그인하든 IAM 사용자로 로그인하든 동일합니다.

루트 사용자로서의 계정 ID 찾기

AWS Management Console

루트 사용자로 로그인했을 때 AWS 계정 ID를 찾으려면

> **최소 권한**
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - 루트 사용자로 로그인하면 IAM 권한이 필요하지 않습니다.

1. 오른쪽 상단의 탐색 표시줄에서 계정 이름 또는 번호를 선택한 다음 보안 자격 증명을 선택합니다.

   > **Tip**
   >
   > 보안 자격 증명 옵션이 보이지 않는 경우 IAM 사용자 대신 IAM 역할을 가진 페더레이션 사용자로 로그인했을 수 있습니다. 이 경우 입력 계정과 그 옆에 있는 계정 ID 번호를 찾아보세요.

2. 계정 세부 정보 섹션에서 계정 번호가 AWS 계정 ID 옆에 표시됩니다.

AWS CLI & SDKs

를 사용하여 AWS 계정 ID를 찾으려면 AWS CLI

> **최소 권한**
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - 루트 사용자로 명령을 실행하면 IAM 권한이 필요하지 않습니다.

다음과 같이 get-caller-identity 명령을 실행합니다.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
```

```
123456789012
```

IAM 사용자의 계정 ID를 찾아보세요.

AWS Management Console

IAM 사용자로 로그인했을 때 AWS 계정 ID를 찾으려면

> **최소 권한**
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - `account:GetAccountInformation`

1. 오른쪽 상단의 탐색 표시줄에서 사용자 이름을 선택한 다음 보안 자격 증명을 선택합니다.

   > **Tip**
   >
   > 보안 자격 증명 옵션이 표시되지 않는 경우 IAM 사용자 대신 IAM 역할을 가진 페더레이션 사용자로 로그인했을 수 있습니다. 이 경우 입력 계정과 그 옆에 있는 계정 ID 번호를 찾아보세요.

2. 페이지 상단의 계정 세부 정보에서AWS 계정 ID 옆에 계정 번호가 표시됩니다.

AWS CLI & SDKs

를 사용하여 AWS 계정 ID를 찾으려면 AWS CLI

> **최소 권한**
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - IAM 사용자 또는 역할로 명령을 실행할 때는 다음이 있어야 합니다.
>   - `sts:GetCallerIdentity`

다음과 같이 get-caller-identity 명령을 실행합니다.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

내 표준 사용자 ID를 찾아보세요. AWS 계정

또는 를 AWS 계정 사용하여 사용할 표준 사용자 ID를 찾을 수 있습니다. AWS Management Console AWS CLI의 표준 사용자 AWS 계정 ID는 해당 계정에만 적용됩니다. 루트 사용자, 연동 사용자 또는 AWS 계정 IAM 사용자의 표준 사용자 ID를 검색할 수 있습니다.

루트 사용자 또는 IAM 사용자의 표준 ID를 찾으십시오.

AWS Management Console

콘솔에 루트 사용자 또는 IAM 사용자로 로그인했을 때 계정의 표준 사용자 ID를 찾으려면

> **최소 권한**
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - 루트 사용자로 명령을 실행하면 IAM 권한이 필요하지 않습니다.
> - IAM 사용자로 로그인할 때는 다음이 있어야 합니다.
>   - `account:GetAccountInformation`

1. 루트 사용자 또는 IAM AWS Management Console 사용자로 로그인합니다.
2. 오른쪽 상단의 탐색 표시줄에서 계정 이름 또는 번호를 선택한 다음 보안 자격 증명을 선택합니다.

   > **Tip**
   >
   > 보안 자격 증명 옵션이 표시되지 않는 경우 IAM 사용자 대신 IAM 역할을 가진 페더레이션 사용자로 로그인했을 수 있습니다. 이 경우 입력 계정과 그 옆에 있는 계정 ID 번호를 찾아보세요.

3. 계정 세부 정보 섹션에서 표준 사용자 ID는 표준 사용자 ID 옆에 표시됩니다. 표준 사용자 ID를 사용하여 Amazon S3 액세스 제어 목록 (ACL) 을 구성할 수 있습니다.

AWS CLI & SDKs

다음을 사용하여 표준 사용자 ID를 찾으려면 AWS CLI

AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할에 대해 동일한 AWS CLI API 명령이 작동합니다.

다음과 같이 list-buckets 명령을 사용합니다.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

IAM 역할을 가진 페더레이션 사용자로서 표준 ID를 찾으십시오.

AWS Management Console

IAM 역할을 가진 연동 사용자로 콘솔에 로그인했을 때 계정의 표준 ID를 찾는 방법

> 최소 권한
>
> - Amazon S3 버킷을 나열하고 볼 수 있는 권한이 있어야 합니다.

1. IAM 역할을 가진 연동 AWS Management Console 사용자로 에 로그인합니다.
2. Amazon S3 콘솔에서 버킷 이름을 선택하여 버킷에 대한 세부 정보를 확인합니다.
3. 권한 탭을 선택합니다.
4. 액세스 제어 목록 섹션의 버킷 소유자 아래에 사용자의 AWS 계정 표준 ID가 표시됩니다.

AWS CLI & SDKs

를 사용하여 표준 사용자 ID를 찾으려면 AWS CLI

AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할에 대해 동일한 AWS CLI API 명령이 작동합니다.

다음과 같이 list-buckets 명령을 사용합니다.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

루트 사용자의 AWS 계정 이름, 이메일 주소 또는 암호 업데이트

이름을 편집하거나 루트 사용자의 암호 또는 이메일 주소를 변경하려면 다음 절차의 단계를 수행하십시오. AWS 계정 이 이메일 주소와 암호는 로 로그인할 때 사용하는 자격 AWS 계정 루트 사용자 증명입니다.

> **Note**
>
> 변경 사항이 모든 곳에 적용되려면 최대 4시간이 걸릴 AWS 계정 수 있습니다.

AWS Management Console

AWS 계정이름, 루트 사용자 암호 또는 루트 사용자 이메일 주소를 편집하려면

> **최소 권한**
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - 로 로그인해야 하며AWS 계정 루트 사용자, 로그인하려면 추가 IAM 권한이 필요하지 않습니다. IAM 사용자 또는 역할로는 이 단계를 수행할 수 없습니다.

1. 이메일 AWS 계정 주소와 비밀번호를 사용하여 사용자 계정으로 로그인합니다AWS 계정 루트 사용자. AWS Management Console
2. 콘솔의 오른쪽 상단 모서리 부분에서 계정 이름이나 번호를 선택한 후 계정을 선택합니다.
3. 계정 페이지에서 계정 설정 옆의 편집을 선택합니다. 보안을 위해 재인증하라는 메시지가 표시됩니다.

> **Note**
>
> 편집 옵션이 나타나지 않으면 계정의 루트 사용자로 로그인하지 않은 것일 수 있습니다. IAM 사용자 또는 역할로 로그인한 상태에서는 계정 설정을 수정할 수 없습니다.

4. 계정 설정 업데이트 페이지에서 업데이트하려는 필드 옆의 편집을 선택합니다.

   a. 이름 — 계정 이름 업데이트 페이지의 새 계정 이름에 새 계정 이름을 입력한 다음 변경 내용 저장을 선택합니다.

   > **Note**
   >
   > AWS 계정이름을 수정할 수 없는 경우 작업에 대한 액세스를 `account` 제한하거나 작업을 거부하도록 설정된 SCP (서비스 제어 정책) 가 있는지 확인하십시오. AWS Organizations `iam:UpdateAccountName`

   b. 이메일의 경우 — 이메일 주소 업데이트 페이지에서 새 이메일 주소, 새 이메일 주소 확인, 현재 비밀번호 확인 필드를 입력합니다. 그런 다음 변경 사항 저장을 선택합니다. 에서 새 이메일 주소로 확인 코드가 전송됩니다`no-reply@verify.signin.aws`. 새 이메일 주소 확인 페이지의 인증 코드에서 이메일로 받은 코드를 입력한 다음 변경 사항 저장을 선택합니다.

   > **Note**
   >
   > 확인 코드가 도착하는 데 최대 5분이 걸릴 수 있습니다. 받은 편지함에 이메일이 보이지 않으면 스팸 폴더와 정크 폴더를 확인하세요.

   c. 비밀번호의 경우 — 비밀번호 업데이트 페이지에서 현재 비밀번호, 새 비밀번호, 새 비밀번호 확인 필드를 입력합니다. 그런 다음 변경 사항 저장을 선택합니다. 루트 사용자 암호 설정의 모범 사례를 비롯한 추가 지침은 IAM 사용 설명서의 암호 변경을 참조하십시오. AWS 계정 루트 사용자

5. 변경을 모두 마치고 완료를 선택합니다.

AWS CLI & SDKs

이 작업은 AWS SDK 중 하나의 API 작업에서 또는 AWS CLI에서 지원되지 않습니다. 이 작업은 AWS Management Console을 사용해야만 수행할 수 있습니다.

API 작동 모드 이해

다음과 함께 작동하는 API 작업AWS 계정의 속성은 항상 다음 두 가지 작업 모드 중 하나에서 작동합니다.

- 독립 실행형— 이 모드는 계정의 사용자 또는 역할이 의 계정 속성에 액세스하거나 변경할 때 사용됩니다.동일 계정. 독립형 컨텍스트 모드는 다음과 같은 경우에 자동으로 사용됩니다.하지 않음포함`AccountId`계정 관리 중 하나를 호출할 때 매개 변수AWS CLI또는AWSSDK 작업을 수행합니다.
- Organizations 컨텍스트— 이 모드는 조직의 한 계정에 있는 사용자 또는 역할이 동일한 조직의 다른 멤버 계정에 있는 계정 속성에 액세스하거나 변경할 때 사용됩니다. 다음과 같은 경우 조직 컨텍스트 모드가 자동으로 사용됩니다.해야 할 것포함`AccountId`계정 관리 중 하나를 호출할 때 매개 변수AWS CLI또는AWSSDK 작업을 수행합니다. 조직의 관리 계정 또는 계정 관리를 위해 위임된 관리자 계정에서만 이 모드의 작업을 호출할 수 있습니다.

이AWS CLI과AWSSDK 작업은 독립 실행형 또는 조직 컨텍스트에서 작동할 수 있습니다.

- 만약하지 않음포함`AccountId`매개 변수를 설정하면 작업이 독립 실행형 컨텍스트에서 실행되고 요청에 사용한 계정에 자동으로 요청을 적용합니다. 이는 조직의 구성원인 여부에 관계없이 적용됩니다.
- 다음을 포함하는 경우`AccountId`매개 변수를 설정하면 작업이 Organizations 컨텍스트에서 실행되고 작업이 지정된 조직 계정에서 작동합니다.
  - 작업을 호출하는 계정이 관리 계정이거나 Account Management 서비스의 위임된 관리자 계정인 경우`AccountId`매개 변수를 사용하여 지정된 계정을 업데이트합니다.
  - 대체 연락처 작업 중 하나에 전화를 걸어 해당 계정 번호를`AccountId`매개 변수는 다음으로 지정된 계정입니다.위임된 관리자 계정계정 관리 서비스의 경우 관리 계정을 포함한 다른 모든 계정은`AccessDenied`예외.
- 독립 실행형 모드에서 작업을 실행하는 경우 다음을 포함하는 IAM 정책으로 작업을 실행할 수 있도록 허용되어야 합니다.`Resource`다음 중 하나의 요소`"*"`모든 리소스를 허용하거나독립 실행형 계정에 구문을 사용하는 ARN.
- 조직 모드에서 작업을 실행하는 경우 다음을 포함하는 IAM 정책으로 작업을 실행할 수 있도록 허용되어야 합니다.`Resource`다음 중 하나의 요소`"*"`모든 리소스를 허용하거나조직의 멤버 계정에 대한 구문을 사용하는 ARN.

계정 속성을 업데이트할 수 있는 권한 부여

대부분의 경우와 마찬가지로AWS작업을 수행할 때 계정 속성을 추가, 업데이트 또는 삭제할 수 있는 권한을 부여합니다.AWS 계정를 사용하여IAM 권한 정책. IAM 권한 정책을 IAM 보안 주체 (사용자 또는 역할) 에 연결할 때 보안 주체가 작업의 대상 리소스 또는 작업, 작업의 대상 리소스 또는 작업, 작업의 대상 리소스 또는 작업, 작업의 대상 리소스 또는 작업 대상 리소스 또는 작업

다음은 권한 정책을 만들 때 계정 관리별로 고려해야 할 몇 가지 사항입니다.

의 Amazon 리소스 이름 형식AWS 계정

- 이Amazon 리소스 이름(ARN)... 에 대한AWS 계정다음에 포함시킬 수 있는`resource`정책 설명의 요소는 참조하려는 계정이 독립 실행형 계정인지 또는 조직에 있는 계정인지에 따라 다르게 구성됩니다. 의 이전 단원API 작동 모드 이해.
  - 독립 실행형 계정의 계정 ARN:

    ```
    arn:aws:account::{AccountId}:account
    ```

    독립 실행형 모드에서 계정 속성 작업을 실행할 때 다음을 포함하지 않고 이 형식을 사용해야 합니다.`AccountID`파라미터.
  - 조직의 멤버 계정에 대한 계정 ARN:

    ```
    arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
    ```

    다음을 포함하여 조직 모드에서 계정 속성 작업을 실행할 때 이 형식을 사용해야 합니다.`AccountID`파라미터.

IAM 정책의 컨텍스트 키

계정 관리 서비스는 또한 여러 가지를 제공합니다.계정 관리 서비스별 조건 키사용자가 부여한 권한을 세밀하게 제어할 수 있습니다.

`account:AccountResourceOrgPaths`

컨텍스트 키`account:AccountResourceOrgPaths`조직의 계층 구조를 통해 특정 OU (조직 구성 단위) 에 대한 경로를 지정할 수 있습니다. 해당 OU에 포함된 멤버 계정만 조건과 일치합니다. 다음 예제 스니펫은 지정된 두 OU 중 하나에 있는 계정에만 적용되도록 정책을 제한합니다.

왜냐하면account:AccountResourceOrgPaths은 (는) 다중 값 문자열 유형입니다.ForAnyValue또는ForAllValues다중 값 문자열 연산자. 또한 조건 키의 접두사는 다음과 같습니다.account, 조직에서 OU에 대한 경로를 참조하는 경우에도 마찬가지입니다.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgPaths": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
        ]
    }
}
```

account:AccountResourceOrgTags

컨텍스트 키account:AccountResourceOrgTags조직의 계정에 연결할 수 있는 태그를 참조할 수 있습니다. 태그는 계정의 리소스를 분류하고 레이블을 지정하는 데 사용할 수 있는 키/값 문자열 쌍입니다. 태그 지정에 대한 자세한 내용은Tag Editor의AWS Resource Groups사용 설명서. 속성 기반 액세스 제어 전략의 일부로 태그를 사용하는 방법에 대한 자세한 내용은 단원을 참조하십시오.용 ABAC란 무엇입니까?AWS의IAM 사용 설명서. 다음 예제 스니펫은 키가 있는 태그가 있는 조직의 계정에만 적용되도록 정책을 제한합니다.project및blue또는red.

왜냐하면account:AccountResourceOrgTags은 (는) 다중 값 문자열 유형입니다.ForAnyValue또는ForAllValues다중 값 문자열 연산자. 또한 조건 키의 접두사는 다음과 같습니다.account, 조직의 구성원 계정에 있는 태그를 참조하는 경우에도 마찬가지입니다.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgTags/project": [
            "blue",
            "red"
        ]
    }
}
```

> **Note**
>
> 조직의 계정에만 태그를 첨부할 수 있습니다. 독립 실행형에는 태그를 첨부할 수 없습니다.AWS 계정.

업데이트하기AWS 계정연락처 정보

에 대한 연락처 정보를 저장할 수 있습니다.기본 계정 연락처당신을 위해AWS 계정. 다음에 대한 연락처 정보를 추가하거나 편집할 수도 있습니다.대체 계정 연락처:

- 대금 청구— 대체 청구 연락처는 청구서 사용 가능 여부 알림과 같은 청구 관련 알림을 받게 됩니다.
- 오퍼레이션— 대체 운영 담당자는 운영 관련 알림을 받게 됩니다.
- 보안— 대체 보안 담당자가 보낸 알림을 비롯한 보안 관련 알림을 받게 됩니다.AWS학대 팀.

주제

- 내 대체 연락처를 업데이트하십시오. AWS 계정
- 내 기본 연락처 업데이트 AWS 계정

내 대체 연락처를 업데이트하십시오. AWS 계정

대체 연락처를 사용하면 AWS 해당 계정과 연결된 최대 3명의 대체 연락처에 연락할 수 있습니다. 대체 연락처는 특정 사람일 필요는 없습니다. 결제, 운영, 보안 관련 문제를 관리하는 팀이 있는 경우 대신 이메일 배포 목록을 추가할 수 있습니다. 여기에는 계정의 루트 사용자와 연결된 이메일 주소에 추가됩니다. 기본 계정 연락처는 루트 계정의 이메일로 전송된 모든 이메일 통신을 계속 받게 됩니다.

계정과 관련된 다음 연락처 유형 중 하나만 지정할 수 있습니다.

- 청구 연락처
- 운영 연락처
- 보안 연락처

계정이 독립형인지 아니면 조직의 일부인지에 따라 대체 연락처를 다르게 추가하거나 편집할 수 있습니다.

- 독립형 AWS 계정 — 조직과 관련이 AWS 계정 없는 경우 AWS 관리 콘솔이나 AWS CLI 및 SDK를 통해 대체 연락처를 업데이트할 수 있습니다. 이 작업을 수행하는 방법을 알아보려면 독립형 AWS 계정 대체 연락처 업데이트를 참조하십시오.
- AWS 계정조직 내 — 조직에 속한 구성원 계정의 경우 관리 계정 또는 위임된 관리자 계정의 사용자는 AWS Organizations 콘솔에서 또는 CLI AWS 및 SDK를 통해 프로그래밍 방식으로 조직의 모든 구성원 계정을 중앙에서 업데이트할 수 있습니다. AWS 이 작업을 수행하는 방법을 알아보려면 조직 내 AWS 계정대체 연락처 업데이트를 참조하십시오.

주제

전화번호 및 이메일 주소 요구 사항

계정의 대체 연락처 정보를 업데이트하기 전에 먼저 전화번호와 이메일 주소를 입력할 때 다음 요구 사항을 검토하는 것이 좋습니다.

- 전화번호에는 숫자, 공백 및 다음 문자만 사용할 수 있습니다.+-()”
- 이메일 주소는 최대 254자까지 가능하며 이메일 주소의 로컬 부분에는 표준 영숫자 외에 다음과 같은 특수 문자를 포함할 수 있습니다. "” +=.#|!&-_

독립형 연락처를 위한 대체 연락처 업데이트 AWS 계정

독립형 AWS 계정 연락처를 추가 또는 편집하려면 다음 절차의 단계를 수행하십시오. 아래 AWS Management Console 절차는 항상 독립형 컨텍스트에서만 작동합니다. 를 사용하여 AWS Management Console 오퍼레이션을 호출하는 데 사용한 계정의 대체 연락처만 액세스하거나 변경할 수 있습니다.

AWS Management Console

독립형 연락처를 추가 또는 편집하려면 AWS 계정

> 최소 권한
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - `account:GetAlternateContact`(대체 연락처 세부 정보 보기)
> - `account:PutAlternateContact`(대체 연락처 설정 또는 업데이트하기)
> - `account:DeleteAlternateContact`(대체 연락처 삭제하기)

1. 최소 권한이 있는 IAM 사용자 또는 AWS Management Console역할로 로그인합니다.
2. 창 오른쪽 상단에서 계정 이름을 선택한 다음 계정을 선택합니다.
3. 계정 페이지에서 아래로 스크롤하여 대체 연락처로 이동한 다음 제목 오른쪽에서 편집을 선택합니다.

> **Note**
>
> 편집 옵션이 보이지 않는 경우 계정의 루트 사용자나 위에서 지정한 최소 권한을 가진 사용자로 로그인하지 않은 것일 수 있습니다.

4. 사용 가능한 모든 필드의 값을 변경합니다.

> **Important**
>
> AWS 계정업무용으로는 개인 전화번호 및 이메일 주소 대신 회사 전화번호와 이메일 주소를 입력하는 것이 좋습니다.

5. 모든 내용을 변경한 후 업데이트를 선택합니다.

AWS CLI & SDKs

다음 AWS CLI 명령 또는 해당 AWS SDK에 상응하는 작업을 사용하여 대체 연락처 정보를 검색, 업데이트 또는 삭제할 수 있습니다.

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **참고**
>
> - 구성원 계정을 대상으로 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 계정 서비스에 신뢰할 수 있는 액세스를 활성화해야 합니다.

최소 권한

각 작업에 대해 해당 작업에 해당하는 권한이 있어야 합니다.

- `GetAlternateContact`(대체 연락처 세부 정보 보기)
- `PutAlternateContact`(대체 연락처 설정 또는 업데이트하기)
- `DeleteAlternateContact`(대체 연락처 삭제하기)

이러한 개별 권한을 사용하는 경우 일부 사용자에게는 연락처 정보를 읽을 수 있는 권한만 부여하고 다른 사용자에게는 읽고 쓸 수 있는 권한을 부여할 수 있습니다.

Example

다음 예에서는 발신자 계정에 대한 현재 결제 대체 연락처를 검색합니다.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

다음 예시에서는 발신자 계정에 새 Operations 대체 연락처를 설정합니다.

```
$ aws account put-alternate-contact \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
```

```
    --title="Operations Manager"
```

성공 시 이 명령은 출력을 생성하지 않습니다.

Example

> **Note**
>
> AWS 계정동일하고 동일한 연락처 유형에 대해 여러 PutAlternateContact 작업을 수행하는 경우 첫 번째 작업자가 새 연락처를 추가하고 동일한 연락처 유형과 동일한 AWS 계정 연락처 유형에 대한 모든 후속 통화는 기존 연락처를 업데이트합니다.

Example

다음 예에서는 발신자 계정의 보안 대체 연락처를 삭제합니다.

```
$ aws account delete-alternate-contact \
    --alternate-contact-type=SECURITY
```

성공 시 이 명령은 출력을 생성하지 않습니다.

> **Note**
>
> 같은 연락처를 두 번 이상 삭제하려고 하면 첫 번째 연락처가 자동으로 삭제됩니다. 이후에 시도해도 모두 예외가 발생합니다. ResourceNotFound

조직 AWS 계정 내 모든 사람의 대체 연락처를 업데이트하세요.

조직 AWS 계정 내 임의의 대체 연락처 세부 정보를 추가하거나 편집하려면 다음 절차의 단계를 수행하십시오.

요구 사항

AWS Organizations콘솔에서 대체 연락처를 업데이트하려면 몇 가지 사전 설정을 수행해야 합니다.

- 조직에서 구성원 계정의 설정을 관리하기 위한 모든 기능을 활성화해야 합니다. 이렇게 하면 관리자가 구성원 계정을 제어할 수 있습니다. 이는 조직을 만들 때 기본적으로 설정됩니다. 조직이 통합 결제 전용으로 설정되어 있고 모든 기능을 활성화하려면 조직의 모든 기능 활성화를 참조하십시오.

- AWS계정 관리 서비스에 신뢰할 수 있는 액세스를 활성화해야 합니다. 이를 설정하려면 AWS계정 관리를 위한 신뢰할 수 있는 액세스 활성화를 참조하십시오.

> **Note**
>
> AWS Organizations콘솔에서 AWS 계정 데이터에 액세스할 수 있도록 Account Management API에 액세스할 수 있는 권한을 제공하도록 AWS Organizations 관리형 정책이 `AWSOrganizationsReadOnlyAccess` 또는 `AWSOrganizationsFullAccess` 업데이트되었습니다. 업데이트된 관리형 정책을 보려면 Organizations AWS 관리형 정책 업데이트를 참조하십시오.

AWS Management Console

조직 AWS 계정 내 임의의 대체 연락처를 추가 또는 편집하려면

1. 조직의 관리 계정 자격 증명으로 AWS Organizations콘솔에 로그인합니다.
2. AWS 계정에서 업데이트하려는 계정을 선택합니다.
3. 연락처 정보를 선택하고 대체 연락처에서 연락처 유형 (청구 연락처, 보안 연락처 또는 운영 연락처) 을 찾습니다.
4. 새 연락처를 추가하려면 추가를 선택하고, 기존 연락처를 업데이트하려면 편집을 선택합니다.
5. 사용 가능한 모든 필드의 값을 변경합니다.

   > **Important**
   >
   > AWS 계정업무용으로는 개인 전화번호 및 이메일 주소 대신 회사 전화번호와 이메일 주소를 입력하는 것이 좋습니다.

6. 모든 내용을 변경한 후 업데이트를 선택합니다.

AWS CLI & SDKs

다음 AWS CLI 명령 또는 해당 AWS SDK에 상응하는 작업을 사용하여 대체 연락처 정보를 검색, 업데이트 또는 삭제할 수 있습니다.

- GetAlternateContact

- PutAlternateContact
- DeleteAlternateContact

> **참고**
>
> - 구성원 계정을 대상으로 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 계정 서비스에 신뢰할 수 있는 액세스를 활성화해야 합니다.
> - 오퍼레이션을 호출하는 데 사용하고 있는 조직이 아닌 다른 조직의 계정에는 접근할 수 없습니다.

> **최소 권한**
>
> 각 작업마다 해당 작업에 해당하는 권한이 있어야 합니다.
>
> - `GetAlternateContact`(대체 연락처 세부 정보 보기)
> - `PutAlternateContact`(대체 연락처 설정 또는 업데이트하기)
> - `DeleteAlternateContact`(대체 연락처 삭제하기)
>
> 이러한 개별 권한을 사용하는 경우 일부 사용자에게는 연락처 정보를 읽을 수 있는 권한만 부여하고 다른 사용자에게는 읽고 쓸 수 있는 권한을 부여할 수 있습니다.

Example

다음 예에서는 조직의 발신자 계정에 대한 현재 결제 대체 연락처를 검색합니다. 사용되는 자격 증명은 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING \
    --account-id 123456789012
{
    "AlternateContact": {
```

```
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

다음 예에서는 조직의 지정된 구성원 계정에 대한 운영 대체 연락처를 설정합니다. 사용되는 자격 증명은 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

성공 시 이 명령은 출력을 생성하지 않습니다.

> **Note**
>
> AWS 계정동일하고 동일한 연락처 유형에 대해 여러 `PutAlternateContact` 작업을 수행하는 경우 먼저 새 연락처가 추가되고 동일한 연락처 유형과 동일한 AWS 계정 연락처 유형에 대한 모든 후속 통화는 기존 연락처를 업데이트합니다.

Example

다음 예제에서는 조직의 지정된 구성원 계정에 대한 보안 대체 연락처를 삭제합니다. 사용되는 자격 증명은 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

```
$ aws account delete-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=SECURITY
```

성공 시 이 명령은 출력을 생성하지 않습니다.

Example

> **Note**
>
> 동일한 연락처를 두 번 이상 삭제하려고 하면 첫 번째 연락처가 자동으로 삭제됩니다. 이후에 시도해도 모두 예외가 발생합니다. `ResourceNotFound`

계정: AlternateContactTypes 컨텍스트 키

컨텍스트 키를 `account:AlternateContactTypes` 사용하여 세 가지 결제 유형 중 IAM 정책에서 허용 (또는 거부) 하는 결제 유형을 지정할 수 있습니다. 예를 들어, 다음 예시 IAM 권한 정책은 이 조건 키를 사용하여 연결된 보안 주체가 조직의 특정 계정에 대한 `BILLING` 대체 연락처만 검색할 수 있도록 허용하고 수정은 허용하지 않습니다.

`account:AlternateContactTypes`는 다중 값 문자열 유형이므로 `ForAnyValue`또는 `ForAllValues` 다중 값 문자열 연산자를 사용해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "account:GetAlternateContact",
            "Resource": [
                "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "account:AlternateContactTypes": [
                        "BILLING"
                    ]
                }
            }
        }
    ]
}
```

내 기본 연락처 업데이트 AWS 계정

연락처의 성명, 회사명, 우편 주소, 전화번호, 웹사이트 주소 등 계정과 관련된 기본 연락처 정보를 업데이트할 수 있습니다.

계정이 독립형인지 아니면 조직의 일부인지에 따라 기본 계정 연락처를 다르게 편집합니다.

- 독립형 AWS 계정 — 조직과 AWS 계정 연결되지 않은 경우 AWS 관리 콘솔이나 AWS CLI 및 SDK를 통해 기본 계정 연락처를 업데이트할 수 있습니다. 이 작업을 수행하는 방법을 알아보려면 독립형 기본 AWS 계정 연락처 업데이트를 참조하십시오.
- AWS 계정조직 내 — 조직에 속한 구성원 계정의 경우 관리 계정 또는 위임된 관리자 계정의 사용자는 AWS Organizations 콘솔에서 또는 CLI AWS 및 SDK를 통해 프로그래밍 방식으로 조직의 모든 구성원 계정을 중앙에서 업데이트할 수 있습니다. AWS 이 작업을 수행하는 방법을 알아보려면 조직의 AWS 계정기본 연락처 업데이트를 참조하십시오.

주제

전화번호 및 이메일 주소 요구 사항

계정의 기본 연락처 정보를 업데이트하기 전에 먼저 전화번호와 이메일 주소를 입력할 때 다음 요구 사항을 검토하는 것이 좋습니다.

- 전화번호에는 숫자, 공백 및 다음 문자만 사용할 수 있습니다.+-(")
- 전화번호는 + 및 국가 코드로 시작해야 하며 국가 코드 뒤에 앞에 0이나 추가 공백이 없어야 합니다. 예: +1 (미국/캐나다) 또는 +44 (영국).
- 전화번호에는 지역 번호, 교환 코드 및 지역 번호 사이에 하이픈 - ""이 포함되어야 합니다. 예를 들어 +1 202-555-0179를 예로 들 수 있습니다.

> **Note**
>
> 전화번호를 하이픈 없이 입력하면 루트 사용자의 MFA 디바이스를 재설정할 때 전화번호 확인 프로세스 중에 전화를 받지 못할 수 있습니다. 자세한 내용은 AWS루트 사용자 계정 MFA 디바이스를 재설정하려면 어떻게 해야 합니까? 를 참조하십시오. .

- 보안을 위해 전화번호는 SMS를 수신할 수 있어야 AWS 합니다. 대부분의 전화번호는 SMS를 지원하지 않으므로 수신자 부담 전화번호는 허용되지 않습니다.
- AWS 계정업무용으로는 개인 전화번호 및 이메일 주소 대신 회사 전화번호와 이메일 주소를 입력하는 것이 가장 좋습니다. 계정 루트 사용자를 개인의 이메일 주소 또는 전화번호로 구성하면 해당 개인이 퇴사할 경우 계정을 복구하기 어려울 수 있습니다.

독립형 연락처를 위한 기본 연락처 업데이트 AWS 계정

독립형 AWS 계정 연락처의 기본 연락처 세부 정보를 편집하려면 다음 절차의 단계를 수행하십시오. 아래 AWS Management Console 절차는 항상 독립형 컨텍스트에서만 작동합니다. 를 사용하여 AWS Management Console 오퍼레이션을 호출하는 데 사용한 계정의 기본 연락처 정보만 액세스하거나 변경할 수 있습니다.

AWS Management Console

독립형 연락처를 위한 기본 연락처 편집하기 AWS 계정

> **최소 권한**
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - `account:GetContactInformation`(기본 연락처 세부 정보 보기)
> - `account:PutContactInformation`(기본 연락처 세부 정보 업데이트)

1. 최소 권한이 있는 IAM 사용자 또는 AWS Management Console역할로 로그인합니다.
2. 창 오른쪽 상단에서 계정 이름을 선택한 다음 계정을 선택합니다.
3. 아래로 스크롤하여 연락처 정보 섹션으로 이동한 다음 옆에서 편집을 선택합니다.
4. 사용 가능한 모든 필드의 값을 변경합니다.
5. 모든 내용을 변경한 후 업데이트를 선택합니다.

AWS CLI & SDKs

다음 AWS CLI 명령 또는 AWS SDK에 상응하는 작업을 사용하여 기본 연락처 정보를 검색, 업데이트 또는 삭제할 수 있습니다.

- GetContactInformation
- PutContactInformation

> **참고**
>
> - 구성원 계정을 대상으로 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 계정 서비스에 신뢰할 수 있는 액세스를 활성화해야 합니다.

> **최소 권한**
>
> 각 작업에 대해 해당 작업에 해당하는 권한이 있어야 합니다.
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> 이러한 개별 권한을 사용하는 경우 일부 사용자에게는 연락처 정보를 읽을 수 있는 권한만 부여하고 다른 사용자에게는 읽고 쓸 수 있는 권한을 부여할 수 있습니다.

Example

다음 예에서는 발신자 계정의 현재 기본 연락처 정보를 검색합니다.

```
$ aws account get-contact-information
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
```

```
}
```

Example

다음 예에서는 발신자 계정의 새 기본 연락처 정보를 설정합니다.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
 Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

성공 시 이 명령은 출력을 생성하지 않습니다.

조직 AWS 계정 내 모든 사람의 기본 연락처를 업데이트하세요.

조직 내 어느 AWS 계정 곳에서든 기본 연락처 세부 정보를 편집하려면 다음 절차의 단계를 수행하십시오.

추가 요구 사항

AWS Organizations콘솔에서 기본 연락처를 업데이트하려면 몇 가지 사전 설정을 수행해야 합니다.

- 조직에서 구성원 계정의 설정을 관리하기 위한 모든 기능을 활성화해야 합니다. 이렇게 하면 관리자가 구성원 계정을 제어할 수 있습니다. 이는 조직을 만들 때 기본적으로 설정됩니다. 조직이 통합 결제 전용으로 설정되어 있고 모든 기능을 활성화하려면 조직의 모든 기능 활성화를 참조하십시오.
- AWS계정 관리 서비스에 신뢰할 수 있는 액세스를 활성화해야 합니다. 이를 설정하려면 AWS계정 관리를 위한 신뢰할 수 있는 액세스 활성화를 참조하십시오.

AWS Management Console

조직 AWS 계정 내 모든 구성원의 기본 연락처를 편집하려면

1. 조직의 관리 계정 자격 증명으로 AWS Organizations콘솔에 로그인합니다.
2. AWS 계정에서 업데이트하려는 계정을 선택합니다.
3. 연락처 정보를 선택하고 기본 연락처를 찾아
4. [편집(Edit)]을 선택합니다.
5. 사용 가능한 모든 필드의 값을 변경합니다.

6. 모든 내용을 변경한 후 업데이트를 선택합니다.

AWS CLI & SDKs

다음 AWS CLI 명령 또는 AWS SDK에 상응하는 작업을 사용하여 기본 연락처 정보를 검색, 업데이트 또는 삭제할 수 있습니다.

- GetContactInformation
- PutContactInformation

> **참고**
>
> - 구성원 계정을 대상으로 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 계정 서비스에 신뢰할 수 있는 액세스를 활성화해야 합니다.
> - 오퍼레이션을 호출하는 데 사용하고 있는 조직이 아닌 다른 조직의 계정에는 접근할 수 없습니다.

> **최소 권한**
>
> 각 작업마다 해당 작업에 해당하는 권한이 있어야 합니다.
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> 이러한 개별 권한을 사용하는 경우 일부 사용자에게는 연락처 정보를 읽을 수 있는 권한만 부여하고 다른 사용자에게는 읽고 쓸 수 있는 권한을 부여할 수 있습니다.

Example

다음 예에서는 조직의 지정된 구성원 계정에 대한 현재 기본 연락처 정보를 검색합니다. 사용되는 자격 증명은 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

```
$ aws account get-contact-information --account-id 123456789012
```

```
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

다음 예에서는 조직의 지정된 구성원 계정에 대한 기본 연락처 정보를 설정합니다. 사용되는 자격 증명은 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
 "CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
 "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

성공 시 이 명령은 출력을 생성하지 않습니다.

보안 챌린지 질문 업데이트

보안 챌린지 질문은 이전에 계정 복구 시나리오에서 ID를 확인하는 데 사용했던 확인 방법입니다. 다단계 인증 (MFA) 과 같은 최신 검증 형식보다 안전성이 떨어집니다. 현재 보안 문제 질문이 있는 경우 이를 사용하여 AWS Support 계정 소유자임을 인증할 수 있습니다. AWS 계정

> **Important**
>
> 2024년 1월 5일부터 아직 활성화하여 사용하지 않은 계정에 대한 보안 챌린지 질문이 더 이상 지원되지 않습니다. AWS 이렇게 하면 의 계정 페이지에서 새 보안 챌린지 질문을 추가하는 옵

션이 제거됩니다. AWS Management Console 이미 보안 챌린지 질문을 설정했거나 AWS 조직의 관리 계정에 이미 설정한 경우 계속 사용할 수 있습니다. 2025년 1월 6일 이후에는 나머지 모든 고객에 대한 보안 챌린지 질문을 더 이상 지원하지 않습니다. AWS 대신 MFA를 추가하는 것이 좋습니다. 자세한 내용은 AWS계정의 보안 챌린지 사용 중단 질문을 참조하십시오.

기존 보안 챌린지 질문을 편집하고 답변을 제공하려면 다음 절차의 단계를 수행하십시오.

AWS Management Console

사용자 질문에 대한 보안 챌린지 질문을 편집하려면 AWS 계정

> **최소 권한**
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - `account:GetChallengeQuestions`(보안 챌린지 질문 참조)
> - `account:PutChallangeQuestions`(보안 챌린지 질문 설정 또는 업데이트)

1. 최소 권한이 있는 IAM 사용자 AWS 계정 루트 사용자 또는 역할로 또는 IAM 사용자 또는 역할로 로그인합니다. AWS Management Console
2. 창 오른쪽 상단에서 계정 이름을 선택한 다음 계정을 선택합니다.
3. 아래로 스크롤하여 보안 챌린지 질문 섹션으로 이동한 다음 편집을 선택합니다.

   > **Note**
   >
   > 편집 옵션이 보이지 않으면 계정의 루트 사용자나 위에서 지정한 최소 권한을 가진 사용자로 로그인하지 않은 것일 수 있습니다.

4. 사용 가능한 모든 필드의 값을 변경합니다. 제공된 질문 중 하나를 선택한 다음 적절한 대답을 입력할 수 있습니다.
5. 변경을 완료한 후 업데이트를 선택합니다.

AWS CLI & SDKs

이 작업은 AWS SDK 중 하나의 API 작업에서 또는 AWS CLI에서 지원되지 않습니다. 이 작업은 AWS Management Console을 사용해야만 수행할 수 있습니다.

어떤 계정을 사용할 수 있는지 AWS 리전 지정하십시오.

AWS 리전An은 여러 가용 영역이 있는 전 세계의 물리적 위치입니다. 가용 영역은 하나 이상의 개별 AWS 데이터 센터로 구성되며, 각 데이터 센터는 별도의 시설에 이중화된 전원, 네트워킹 및 연결 기능을 갖추고 있습니다. 즉, 각 AWS 리전 지역은 물리적으로 격리되어 있고 다른 지역과 독립적입니다. 리전에서는 내결함성, 안정성 및 복원성을 지원하고 지연 시간을 줄일 수도 있습니다. 사용 가능한 지역 및 향후 지역 맵은 지역 및 가용 영역을 참조하십시오.

한 지역에서 생성한 리소스는 서비스에서 제공하는 복제 기능을 명시적으로 사용하지 않는 한 다른 지역에는 존재하지 않습니다. AWS 예를 들어, Amazon S3와 Amazon EC2 크로스 리전 복제를 지원합니다. AWS Identity and Access Management (IAM) 과 같은 일부 서비스에는 지역 리소스가 없습니다.

계정을 통해 자신이 사용할 수 있는 리전을 결정합니다.

- An은 요구 사항을 충족하는 위치에서 AWS 리소스를 시작할 수 있도록 여러 지역을 AWS 계정 제공합니다. 예를 들어 유럽 고객에게 더 가까이 다가가거나 법적 요구 사항을 충족하기 위해 유럽에서 Amazon EC2 인스턴스를 시작하고자 할 수 있습니다.
- AWS GovCloud (미국 서부) 계정은 (미국 서부) 지역 및 AWS GovCloud (미국 동부) 지역에 대한 액세스를 제공합니다. AWS GovCloud 자세한 정보는 AWS GovCloud (US)을 참조하세요.
- Amazon AWS (중국) 계정은 베이징 및 닝샤 지역에만 액세스할 수 있습니다. 자세한 내용은 중국 Amazon Web Services를 참조하세요.

지역 이름 및 해당 코드 목록은 AWS 일반 참조 안내서의 지역 엔드포인트를 참조하십시오. 각 지역에서 지원되는 AWS 서비스 목록 (엔드포인트 제외) 은 AWS 지역 서비스 목록을 참조하십시오.

> **Important**
>
> AWS 지연 시간을 줄이려면 글로벌 엔드포인트 대신 지역 AWS Security Token Service (AWS STS) 엔드포인트를 사용할 것을 권장합니다. 지역 AWS STS 엔드포인트의 세션 토큰은 모든 AWS 지역에서 유효합니다. 지역 AWS STS 엔드포인트를 사용하는 경우 변경할 필요가 없습니다. 하지만 글로벌 AWS STS 엔드포인트 (https://sts.amazonaws.com) 의 세션 토큰은 활성화하거나 기본적으로 활성화되어 있다는 점에서만 AWS 리전 유효합니다. 계정에 새 지역을 활성화하려는 경우 지역 엔드포인트의 세션 토큰을 사용하거나 글로벌 AWS STS AWS STS 엔드포인트를 활성화하여 모두에 유효한 세션 토큰을 발행할 수 있습니다. AWS 리전모든 지역에서 유효한 세션 토큰은 더 큽니다. 세션 토큰을 저장하는 경우 이렇게 큰 토큰이 시스템에 영향을 미칠 수 있습니다. AWS STS 엔드포인트가 AWS 지역과 작동하는 방식에 대한 자세한 내용은 AWS STSAWS 지역에서의 관리를 참조하십시오.

주제

지역을 활성화하거나 비활성화하기 전에 고려할 사항

지역을 활성화하거나 비활성화하기 전에 다음 사항을 고려하는 것이 중요합니다.

- 2019년 3월 20일 이전에 도입된 지역은 기본적으로 활성화되어 있으며, AWS 원래는 AWS 리전 기본적으로 모두 새로 활성화되어 있으므로 해당 지역에서 즉시 리소스를 생성하고 관리할 수 있습니다. 기본적으로 활성화된 지역은 활성화하거나 비활성화할 수 없습니다. 현재 지역을 AWS 추가하면 새 지역이 기본적으로 비활성화됩니다. 사용자가 새 지역에서 리소스를 생성하고 관리할 수 있게 하려면 먼저 해당 지역을 활성화해야 합니다. 다음 지역은 기본적으로 비활성화되어 있습니다.

명칭	코드
아프리카(케이프타운)	af-south-1
아시아 태평양(홍콩)	ap-east-1
아시아 태평양(하이데라바드)	ap-south-2
아시아 태평양(자카르타)	ap-southeast-3
아시아 태평양(멜버른)	ap-southeast-4
캐나다 (캘거리)	ca-west-1
유럽(밀라노)	eu-south-1
유럽(스페인)	eu-south-2
유럽(취리히)	eu-central-2
이스라엘(텔아비브)	il-central-1
중동(바레인)	me-south-1

명칭	코드
중동(UAE)	me-central-1

- IAM 권한을 사용하여 지역에 대한 액세스를 제어할 수 있습니다. AWS Identity and Access Management (IAM) 에는 지역을 활성화, 비활성화, 가져오기 및 나열할 수 있는 사용자를 제어할 수 있는 네 가지 권한이 포함되어 있습니다. 자세한 내용은 AWS Billing and Cost Management 사용 설명서의 Billing 및 Cost Management 조치 정책을 참조하십시오. aws:RequestedRegion조건 키를 사용하여 a에 대한 액세스를 AWS 서비스 제어할 수도 AWS 리전있습니다.
- 지역 활성화는 무료입니다. — 지역 활성화에는 요금이 부과되지 않습니다. 새 지역에서 생성한 리소스에 대해서만 요금이 부과됩니다.
- 지역을 비활성화하면 해당 지역의 리소스에 대한 IAM 액세스가 비활성화됩니다. Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스와 같이 AWS 리소스가 여전히 포함되어 있는 지역을 비활성화하면 해당 지역의 리소스에 대한 IAM 액세스 권한을 잃게 됩니다. 예를 들어 비활성화된 지역에 있는 EC2 AWS Management Console 인스턴스의 구성을 보거나 변경하는 데는 를 사용할 수 없습니다.
- 지역을 비활성화해도 활성 리소스에 대한 요금이 계속 부과됩니다. — AWS 리소스가 아직 포함되어 있는 지역을 비활성화하면 해당 리소스 (있는 경우) 에 대한 요금이 계속 표준 요금으로 발생합니다. 예를 들어 Amazon EC2 인스턴스가 있는 리전을 비활성화하여 인스턴스에 액세스할 수 없게 되었더라도 그러한 인스턴스의 요금은 그대로 지불해야 합니다.
- 지역을 비활성화해도 항상 즉시 표시되는 것은 아닙니다. 지역을 비활성화한 후 서비스와 콘솔이 일시적으로 표시될 수 있습니다. 지역 비활성화가 적용되는 데 몇 분에서 몇 시간이 걸릴 수 있습니다.
- 지역을 활성화하는 데 몇 분에서 몇 시간이 걸리는 경우도 있습니다. — 지역을 활성화하면 IAM 리소스를 지역에 배포하는 등 해당 지역에서 계정을 준비하기 위한 작업이 AWS 수행됩니다. 이 프로세스는 대부분의 계정에서 몇 분 정도 걸리지만 때로는 몇 시간이 걸릴 수도 있습니다. 이 프로세스가 완료될 때까지는 해당 리전을 사용할 수 없습니다.
- 조직은 조직 전체에서 지정된 시간에 50개의 region-opt 요청을 열 수 있습니다. — 관리 계정은 언제든지 AWS 조직에 대한 완료 대기 중인 50개의 공개 요청을 가질 수 있습니다. 요청 1번은 계정 하나에 대해 특정 지역 하나를 활성화하거나 비활성화하는 것과 같습니다.
- 단일 계정에서 언제든지 6개의 region-opt 요청을 진행할 수 있습니다. 즉, 요청 1개는 계정 하나에 대해 특정 지역 하나를 활성화 또는 비활성화하는 것과 같습니다.
- Amazon EventBridge 통합 — 고객은 에서 지역 선택 상태 업데이트 알림을 구독할 수 있습니다. EventBridge 각 상태 변경에 대한 EventBridge 알림이 생성되어 고객이 워크플로를 자동화할 수 있습니다.

- 명시적 지역-옵트 아웃 상태 — 옵트인 영역 활성화/비활성화의 비동기 특성으로 인해 region-opt 요청에는 네 가지 잠재적 상태가 있습니다.
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  또는 상태일 때는 옵트인 또는 옵트아웃을 취소할 수 없습니다. `ENABLING` `DISABLING` 그렇지 `ConflictException` 않으면 a가 삭제됩니다. 완료된 (활성화/비활성화) region-opt 요청은 주요 기본 서비스의 프로비저닝에 따라 달라집니다. AWS 일부 AWS 서비스는 현재 상태임에도 불구하고 즉시 사용할 수 없는 경우가 있을 수 있습니다. `ENABLED`
- 완전 통합 AWS Organizations — 관리 계정은 해당 조직의 모든 구성원 계정을 수정하거나 region-opt를 읽을 수 있습니다. AWS 회원 계정은 해당 지역 상태도 읽고 쓸 수 있습니다.

독립형 계정의 지역 활성화 또는 비활성화

액세스 AWS 계정 권한이 있는 지역을 업데이트하려면 다음 절차의 단계를 수행하십시오. 아래 AWS Management Console 절차는 항상 독립형 컨텍스트에서만 작동합니다. 를 사용하여 AWS Management Console 오퍼레이션을 호출하는 데 사용한 계정에서 사용 가능한 지역만 보거나 업데이트할 수 있습니다.

AWS Management Console

독립형 지역을 활성화하거나 비활성화하려면 AWS 계정

> 최소 권한
>
> 다음 절차의 단계를 수행하려면 IAM 사용자 또는 역할에 다음 권한이 있어야 합니다.
>
> - `account:ListRegions`(목록 AWS 리전 및 해당 사용자의 현재 활성화 또는 비활성화 여부를 확인하는 데 필요함).
> - `account:EnableRegion`
> - `account:DisableRegion`

1. 에 AWS Management Console AWS 계정 루트 사용자 로그인하거나 최소 권한이 있는 IAM 사용자 또는 역할로 로그인합니다.

2. 창 오른쪽 상단에서 계정 이름을 선택한 다음 계정을 선택합니다.
3. 계정 페이지에서 아래로 스크롤하여 섹션으로 이동합니다 AWS 리전.

> **Note**
>
> 이 정보에 대한 액세스를 승인하라는 메시지가 표시될 수 있습니다. AWS 계정과 연결된 이메일 주소 및 기본 연락처 전화번호로 요청을 보냅니다. 요청에서 링크를 선택하여 브라우저에서 열고 액세스를 승인합니다.

4. 계정의 사용자가 해당 지역의 리소스를 생성하고 액세스할 수 있도록 할지 여부에 따라 작업 열의 각 AWS 리전 옵션 옆에서 활성화 또는 비활성화를 선택합니다.
5. 메시지가 표시되면 선택을 확인합니다.
6. 모든 변경을 완료한 후 업데이트를 선택합니다.

AWS CLI & SDKs

다음 AWS CLI 명령어 또는 AWS SDK에 상응하는 작업을 사용하여 지역 선택 상태를 활성화, 비활성화, 읽기 및 나열할 수 있습니다.

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **최소 권한**
>
> 다음 단계를 수행하려면 해당 작업에 매핑되는 권한이 있어야 합니다.
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

이러한 개별 권한을 사용하는 경우 일부 사용자에게는 지역 선택 정보를 읽을 수 있는 권한만 부여하고 다른 사용자에게는 읽기 및 쓰기 권한을 모두 부여할 수 있습니다.

다음 예에서는 조직의 지정된 구성원 계정에 대해 지역을 활성화합니다. 사용되는 자격 증명은 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

동일한 명령을 사용하여 지역을 비활성화한 다음 다음으로 바꿀 수도 있다는 점에 `enable-region` 유의하세요`disable-region`.

```
aws account enable-region --region-name af-south-1
```

성공 시 이 명령은 출력을 생성하지 않습니다.

작업은 비동기식입니다. 다음 명령을 사용하면 요청의 최신 상태를 볼 수 있습니다.

```
aws account get-region-opt-status --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

조직의 지역을 활성화하거나 비활성화합니다.

회원 계정에 대해 활성화된 지역을 업데이트하려면 다음 절차의 단계를 수행하십시오. AWS Organizations

> **Note**
>
> AWS Organizations 콘솔에서 AWS 계정 데이터에 액세스할 수 있도록 Account Management API에 액세스할 수 있는 권한을 제공하도록 AWS Organizations 관리형 정책이 `AWSOrganizationsReadOnlyAccess` 또는 `AWSOrganizationsFullAccess` 업데이트되었습니다. 업데이트된 관리형 정책을 보려면 Organizations AWS 관리 정책 업데이트를 참조하십시오.

> **Note**
>
> 구성원 계정과 함께 사용할 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 먼저 다음을 수행해야 합니다.
>
> - 조직의 모든 기능을 활성화하여 구성원 계정의 설정을 관리할 수 있습니다. 이렇게 하면 관리자가 구성원 계정을 제어할 수 있습니다. 이는 조직을 만들 때 기본적으로 설정됩니다. 조

직이 통합 결제 전용으로 설정되어 있고 모든 기능을 활성화하려면 조직의 모든 기능 활성화를 참조하십시오.

- AWS 계정 관리 서비스에 신뢰할 수 있는 액세스를 활성화하세요. 이를 설정하려면 을 참조하십시오AWS계정 관리를 위한 신뢰할 수 있는 액세스 활성화.

AWS Management Console

조직 내 지역을 활성화 또는 비활성화하려면

1. 조직의 관리 계정 자격 증명으로 AWS Organizations 콘솔에 로그인합니다.
2. AWS 계정페이지에서 업데이트하려는 계정을 선택합니다.
3. 계정 설정 탭을 선택합니다.
4. 지역에서 활성화하거나 비활성화하려는 지역을 선택합니다.
5. 작업을 선택한 다음 활성화 또는 비활성화 옵션을 선택합니다.
6. 활성화 옵션을 선택한 경우 표시된 텍스트를 검토한 다음 지역 활성화를 선택합니다.
7. 비활성화 옵션을 선택한 경우 표시된 텍스트를 검토하고 비활성화를 입력하여 확인한 다음 지역 비활성화를 선택합니다.

AWS CLI & SDKs

다음 AWS CLI 명령어 또는 AWS SDK에 상응하는 작업을 사용하여 기관 구성원 계정의 지역 선택 상태를 활성화, 비활성화, 읽기 및 나열할 수 있습니다.

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

최소 권한

다음 단계를 수행하려면 해당 작업에 매핑되는 권한이 있어야 합니다.

- `account:EnableRegion`
- `account:DisableRegion`

- account:GetRegionOptStatus
- account:ListRegions

이러한 개별 권한을 사용하는 경우 일부 사용자에게는 지역 선택 정보를 읽을 수 있는 권한만 부여하고 다른 사용자에게는 읽기 및 쓰기 권한을 모두 부여할 수 있습니다.

다음 예에서는 조직의 지정된 구성원 계정에 대해 지역을 활성화합니다. 사용되는 자격 증명은 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

동일한 명령을 사용하여 지역을 비활성화한 다음 다음으로 바꿀 수도 있다는 점에 enable-region 유의하세요disable-region.

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

성공 시 이 명령은 출력을 생성하지 않습니다.

> **Note**
>
> 조직은 한 번에 최대 20개의 지역 요청만 할 수 있습니다. 그렇지 않으면 a를 받게 TooManyRequestsException 됩니다.

작업은 비동기식입니다. 다음 명령을 사용하면 요청의 최신 상태를 볼 수 있습니다.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

AWS 계정별칭 생성 또는 업데이트

IAM 사용자의 URL에 AWS 계정 ID 대신 회사 이름 (또는 다른 easy-to-remember 식별자) 을 포함하려는 경우 계정 별칭을 생성할 수 있습니다.

계정 별칭을 생성하거나 업데이트하는 방법을 알아보려면 IAM 사용 설명서의 AWS 계정별칭 생성, 삭제 및 등재를 참조하십시오.

청구서 보기AWS 계정

청구 관련 절차 및 사용자 관련 작업의 경우AWS 계정에서 다음 주제를 참조하십시오.AWS Billing and Cost Management사용 설명서:

- 청구서 결제에 사용되는 통화 변경
- 사업자 등록 번호 업데이트 및 삭제
- 세금 설정 상속 활성화

인도 내 계정 관리

새로 가입하는 경우AWS 계정연락처 주소로 인도를 선택하십시오. 사용자 계약서는 다음과 같습니다.Amazon Internet Services Private Limited(AISPL), 현지인AWS인도의 셀러.AISPL에서 청구를 관리하며, 청구서 총액이 미국 달러 (USD) 대신 인도 루피 (INR) 로 표시됩니다. AISPL을 통해 계정 생성을 마치면 연락처 정보에서 국가를 변경할 수 없습니다.

기존에 있는 경우AWS 계정인도 주소인 경우 귀하의 계정은 다음 중AWS또는 AISPL (계좌 개설 시기에 따라 다름) 계정에 다음 계정이 있는지 알아보려면AWSAISPL에 대해서는 을 참조하십시오.Determining which company your account is with. 기존 AWS 고객인 경우 AWS 계정을 계속해서 사용할 수 있습니다. 둘 다 선택할 수도 있습니다AWS 계정및 AISPL 계정 (동일한 계정으로 통합할 수는 없지만)AWS조직. 관리에 대한 자세한 내용은AWS 계정, 참조당신의 것을 관리하세요AWS 계정.

AISPL 계정을 사용하는 경우 이 항목의 절차에 따라 계정을 관리하십시오. 이 항목에서는 AISPL 계정에 가입하고, AISPL 계정에 대한 정보를 편집하고, 영구 계정 번호 (PAN) 를 추가 또는 편집하는 방법에 대해 설명합니다.

가입 중 신용 카드 확인 절차의 일환으로 AISPL에서 신용 카드에 2 INR을 부과합니다. 확인을 완료한 후 AISPL은 2 INR을 환불합니다. 확인 프로세스의 한 부분으로 AISPL은 신용 카드 2INR을 부과합니다.

주제

- 계정이 어느 회사에 속해 있는지 확인하세요.
- 생성하기AWS 계정AISPL과 함께
- AISPL 계정 관리

계정이 어느 회사에 속해 있는지 확인하세요.

AWS 서비스는 AWS 및 AISPL 모두에서 제공합니다. 이 절차를 통해 사용할 계정에 대한 판매자를 확인하세요.

AWS Management Console

회사가 어떤 계정을 사용하는지 확인하려면

> 최소 권한
>
> 다음 단계를 수행하려면 최소한 다음과 같은 IAM 권한이 있어야 합니다.
>
> - 이 절차에는 특별한 권한이 필요하지 않습니다.

1. 열기AWS Management Console...에서AWS Management Console.
2. 페이지 하단의 페이지 바닥글에서 저작권 고지를 확인하세요. 저작권이 Amazon Web Services에 있는 경우, 귀하의 계정은 AWS의 계정입니다. 저작권이 Amazon Internet Services Private Ltd에 있는 경우, 귀하의 계정은 AISPL의 계정입니다.

AWS CLI & SDKs

이 작업은 에서 지원되지 않습니다.AWS CLI또는 다음 중 하나에서 API 작업을 통해AWSSDK. 이 작업은 를 통해서만 수행할 수 있습니다.AWS Management Console.

생성하기AWS 계정AISPL과 함께

AISPL은 다음과 같은 현지 판매자입니다.AWS인도에서. 자신의 연락처 주소가 인도에 있는 경우, 다음 절차를 사용해 AISPL 계정에 가입합니다.

AWS Management Console

AISPL 계정에 가입하려면

> 최소 권한
>
> 다음 단계를 수행하려면 최소한 다음과 같은 IAM 권한이 있어야 합니다.

- 이 작업은 시작하기 전에 발생하기 때문입니다.AWS 계정, 이 작업에는 다음이 필요하지 않습니다.AWS사용 권한.

1. 열기AWS Management Console, 그런 다음 선택콘솔에 로그인.
2. ... 에로그인페이지에서 사용할 이메일 주소를 입력합니다.
3. 이메일 주소에서 I am a new user를 선택한 후 Sign in using our secure server를 선택합니다.
4. 각 로그인 자격 증명 필드에 정보를 입력한 다음 선택하십시오.계정 생성.
5. 각 연락처 정보 필드에 정보를 입력합니다.
6. 계약을 읽고 약관 확인란을 선택한 다음 Create Account and Continue를 다시 선택합니다.
7. Payment Information 페이지에서 사용할 지불 방법을 입력합니다.
8. 아래PAN 정보, 선택아니오영구 계좌 번호 (PAN) 가 없거나 나중에 추가하려는 경우. PAN이 있고 지금 추가하려는 경우 다음을 선택하십시오.예, 그리고팬필드에 PAN을 입력합니다.
9. Verify Card and Continue를 선택합니다. 확인 과정의 일환으로 CVV를 제공해야 합니다. 확인 절차의 일환으로 AISPL에서 카드에 2 INR을 부과합니다. 확인을 완료한 후 AISPL은 2 INR을 환불합니다.
10. ... 에 대한전화번호 입력, 전화번호를 입력하세요. 내선 전화가 있는 경우내선 번호, 휴대폰 내선 번호를 입력하세요.
11. Call Me Now를 선택합니다. 잠시 후에 4자리 PIN이 화면상에 표시됩니다.
12. AISPL의 자동 호출을 수락합니다. 휴대폰 키패드에서 화면에 표시된 4자리 핀을 입력합니다.
13. 자동 호출을 통해 연락처 번호를 확인하고 나면 Continue to Select Your Support Plan를 선택합니다.
14. Support Plan 페이지에서 지원 계획을 선택한 다음 Continue를 다시 선택합니다. 결제 방법이 확인되고 계정이 활성화되면 계정 활성화를 확인하는 이메일 메시지를 받게 됩니다.

AWS CLI & SDKs

이 작업은 에서 지원되지 않습니다.AWS CLI또는 다음 중 하나에서 API 작업을 통해AWSSDK. 이 작업은 를 통해서만 수행할 수 있습니다.AWS Management Console.

AISPL 계정 관리

다음 작업을 제외하고 계정 관리 절차는 인도 외부에서 만든 계정과 동일합니다. 당신의 것을 관리하세요AWS 계정을 참조하세요.

사용AWS Management Console다음 작업을 수행하려면:

- 영구 계정 번호 (PAN) 추가 또는 편집
- 여러 영구 계정 번호 (PAN) 편집
- 여러 상품 및 용역세 번호 (GST) 편집
- 세금계산서 보기

팬 닫기 AWS 계정

더 이상 필요하지 않은 경우 이 섹션의 지침에 따라 언제든지 닫을 수 있습니다. AWS 계정계정을 폐쇄한 후에는 계정을 폐쇄한 날로부터 90일 이내에 다시 개설할 수 있습니다. 계정을 폐쇄한 날부터 계정이 AWS 영구적으로 폐쇄되는 시점 사이의 기간을 해지 후 기간이라고 합니다.

계정을 폐쇄하기 전에 알아두어야 할 사항

계정을 AWS 계정폐쇄하기 전에 다음 사항을 고려해야 합니다.

- 계정을 폐쇄하면 이 계정에 대한 AWS 고객 계약 해지 통지가 됩니다.
- 계정을 폐쇄하기 AWS 계정 전에 내 리소스를 삭제할 필요는 없습니다. 하지만 보관하려는 모든 리소스나 데이터를 백업하는 것이 좋습니다. 특정 리소스를 백업하는 방법에 대한 지침은 해당 서비스의 해당 AWS 설명서를 참조하십시오.
- 폐쇄 후 기간 동안 계정을 다시 개설할 수 있습니다. 계정을 다시 열면 계정에 남아 있던 서비스에 대한 요금이 다시 청구됩니다. 또한 모든 미결제 청구서와 미결제 예약 인스턴스 및 Savings Plans에 대한 책임은 귀하에게 있습니다.
- 계정 폐쇄 전에 사용한 서비스에 대한 모든 미결제 수수료 및 요금은 귀하가 부담합니다. 계정 폐쇄 후 다음 달에 AWS 청구서를 받게 됩니다. 예를 들어 1월 15일에 계정을 폐쇄한 경우 1월 1일부터 1월 15일까지 발생한 사용에 대한 청구서를 2월 초에 받게 됩니다. 계정을 폐쇄한 후에도 만료될 때까지 예약 인스턴스 및 Savings Plans에 대한 청구서를 계속 받게 됩니다.
- 이전에 계정에서 사용할 수 있었던 AWS 서비스를 더 이상 이용할 수 없게 됩니다. 그러나 해지 후 기간 AWS 계정 동안에는 로그인하고 폐쇄된 계정에 액세스하여 과거 청구 정보를 보거나 계정 설정에 액세스하거나 연락할 수만 있습니다. AWS Support

- 계정 폐쇄 당시 등록된 이메일 주소를 다른 사람의 기본 이메일로 사용할 수 없습니다. AWS 계정 AWS 계정동일한 이메일 주소를 다른 AWS 계정이메일 주소로 사용하려는 경우 종료 전에 이메일 주소를 업데이트하는 것이 좋습니다. 이메일 주소 업데이트에 루트 사용자의 AWS 계정 이름, 이메일 주소 또는 암호 업데이트 대한 지침은 을 참조하십시오.
- 루트 사용자에 대해 멀티 팩터 인증 (MFA) 을 활성화하거나 IAM 사용자에게 MFA 디바이스를 구성한 경우, AWS 계정 계정을 폐쇄해도 MFA는 자동으로 제거되지 않습니다. 폐쇄 후 90일 동안 MFA를 켜둔 상태로 두기로 선택한 경우, 해당 기간 동안 계정에 액세스해야 하는 경우에 대비해 종료 후 기간이 만료될 때까지 MFA 디바이스를 활성 상태로 유지하십시오. 참고: 계정이 영구 폐쇄된 후에는 하드웨어 TOTP 토큰 디바이스를 다른 사용자와 연결할 수 없습니다. 나중에 다른 사용자와 함께 하드웨어 TOTP 토큰을 사용하려는 경우 계정을 폐쇄하기 전에 하드웨어 MFA 디바이스를 비활성화할 수 있습니다. IAM 사용자를 위한 MFA 디바이스는 계정 관리자가 삭제해야 합니다.

회원 계정에 대한 추가 고려 사항

- 구성원 계정을 폐쇄하면 해당 계정은 폐쇄 후 기간이 경과할 때까지 조직에서 제거되지 않습니다. 해지 후 기간 동안에는 해지된 멤버 계정이 여전히 조직의 계정 할당량 계산에 반영됩니다. 계정이 할당량에 포함되지 않도록 하려면 계정을 폐쇄하기 전에 조직에서 구성원 계정 제거를 참조하십시오.
- 30일의 기간 동안 멤버 계정 중 10%를 해지할 수 있습니다. 이 할당량의 기간은 달력상의 월을 기준으로 하지 않으며, 계정을 해지하는 시점에 시작됩니다. 최초 계정 해지 후 30일간은 10% 계정 해지 한도를 초과할 수 없습니다. 계정 중 10% 가 1000개를 초과하더라도 최소 계정 폐쇄는 10개이고 최대 계정 폐쇄는 1000개입니다. 조직 할당량에 대한 자세한 내용은 할당량을 참조하십시오. AWS Organizations
- AWS Control Tower를 사용하는 경우 계정을 폐쇄하기 전에 회원 계정을 관리 해제해야 합니다. AWS Control Tower 사용 설명서에서 멤버 계정 관리 해제를 참조하세요.

서비스별 고려사항

- AWS Marketplace 계정 폐쇄 시 구독은 자동으로 취소되지 않습니다. 구독이 있는 경우 먼저 구독에 포함된 소프트웨어의 모든 인스턴스를 종료하십시오. 그런 다음 AWS Marketplace 콘솔의 구독 관리 페이지로 이동하여 구독을 취소하십시오.
- Route 53에 등록된 도메인은 자동으로 삭제되지 않습니다. 구독을 종료하기 전에 다음 네 가지 옵션을 사용할 수 있습니다 AWS 계정.
  - 자동 갱신을 비활성화할 수 있으며 등록 기간이 만료되면 도메인이 자동으로 삭제됩니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 도메인 자동 갱신 활성화 또는 비활성화를 참조하세요.

- 도메인을 다른 AWS 계정으로 이전할 수 있습니다. 자세한 내용은 도메인을 다른 AWS 계정으로 이전하기를 참조하세요.
- 도메인을 다른 도메인 등록 대행자로 이전할 수 있습니다. 자세한 내용은 Route 53로부터 다른 등록 대행자로 도메인 이전하기를 참조하세요.
- 이미 계정을 폐쇄한 경우, 케이스를 열어 도메인 이전에 AWS Support대한 도움을 요청할 수 있습니다.

계정 해지 방법

다음 절차를 AWS 계정 사용하여 계정을 폐쇄할 수 있습니다. 폐쇄하려는 계정 유형 [독립 실행형, 구성원, 관리 계정 및 AWS GovCloud (US)] 에 따라 각 탭에 제공되는 지침이 다르다는 점에 유의하십시오.

계정을 폐쇄하는 과정에서 문제가 발생하는 경우 을 참조하십시오AWS 계정 폐쇄 관련 문제 해결.

Standalone account

독립형 계정은 소속되지 않은 개별적으로 관리되는 계정입니다. AWS Organizations

계정 페이지에서 독립형 계정을 폐쇄하려면

1. AWS 계정 폐쇄하려는 계정의 루트 AWS Management Console 사용자로 로그인합니다. IAM 사용자 또는 역할로 로그인한 상태에서는 계정을 폐쇄할 수 없습니다.
2. 오른쪽 상단의 탐색 표시줄에서 계정 이름 또는 번호를 선택한 다음 계정을 선택합니다.
3. 계정 페이지에서 페이지 하단으로 스크롤하여 계정 닫기 섹션으로 이동합니다. 계정 폐쇄 절차를 읽고 이해했는지 확인하세요.
4. 계정 해지 버튼을 선택하여 계정 폐쇄 프로세스를 시작합니다.
5. 몇 분 내에 계정이 폐쇄되었다는 확인 이메일을 받게 됩니다.

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

Member account

멤버 계정은 AWS 계정 해당 계정의 일부입니다 AWS Organizations.

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 독립형 계정 탭의 단계를 따라야 합니다.
4. 모든 필수 계정 해지 문을 승인하려면 각 확인란을 선택합니다.
5. 멤버 계정 ID를 입력한 다음 계정 폐쇄를 선택합니다.

계정 페이지에서 회원 계정을 폐쇄하려면

필요에 따라 의 계정 페이지에서 AWS 멤버 계정을 직접 폐쇄할 수 AWS Management Console있습니다. step-by-step지침을 보려면 독립형 계정 탭의 지침을 따르세요.

AWS CLI 및 SDK를 사용하여 멤버 계정을 폐쇄하려면

AWS CLI 및 SDK를 사용하여 구성원 계정을 폐쇄하는 방법에 대한 지침은 사용 AWS Organizations 설명서의 조직 내 구성원 계정 폐쇄를 참조하십시오.

Management account

관리 계정은 상위 또는 루트 계정 역할을 AWS 계정 하는 계정입니다. AWS Organizations

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

계정 페이지에서 관리 계정을 폐쇄하려면

1. 폐쇄하려는 관리 계정의 루트 AWS Management Console 사용자로 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 이동하기 전에 회원 계정 탭에 제공된 계정 폐쇄 지침을 따라야 합니다.

3. 오른쪽 상단의 탐색 막대에서 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.

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

AWS GovCloud (US) account

AWS GovCloud (US) 계정은 청구 및 결제 AWS 계정 목적으로 항상 단일 표준에 연결됩니다.

AWS GovCloud (US) 계정을 폐쇄하려면

계정에 연결된 계정이 AWS 계정 있는 경우 AWS GovCloud (US) 계정을 폐쇄하기 전에 표준 계정을 폐쇄해야 합니다. AWS GovCloud (US) 데이터를 백업하고 의도하지 않은 AWS GovCloud (US) 청구를 방지하는 방법을 비롯한 자세한 내용은 AWS GovCloud (US) 사용 설명서의 AWS GovCloud (US) 계정 해지를 참조하십시오.

계정 해지 후 예상되는 사항

계정을 폐쇄하는 즉시 다음과 같은 상황이 발생합니다.

- 루트 사용자의 이메일 주소로 계정 폐쇄를 확인하는 이메일이 발송됩니다. 몇 시간 내에 이 이메일을 받지 못하면 을 참조하십시오AWS 계정 폐쇄 관련 문제 해결.
- 회원 계정을 폐쇄하면 AWS Organizations 콘솔에서 해당 계정 이름 옆에 SUSPENDED 레이블이 표시됩니다.
- 다른 계정에 AWS 계정 내 서비스에 액세스할 수 있는 권한을 부여한 경우 해당 계정에서 이루어진 모든 액세스 요청은 계정 폐쇄 후 실패해야 합니다. 계정을 다시 열면 필요한 권한을 부여한 경우 다른 사람이 계정의 AWS 서비스 및 리소스에 다시 액세스할 AWS 계정 수 있습니다. AWS 계정

폐쇄 후 기간

해지 후 기간이란 계정을 폐쇄한 날부터 계정을 AWS 영구적으로 폐쇄하는 시점까지의 기간을 말합니다. AWS 계정폐쇄 후 기간은 90일입니다. 폐쇄 후 기간에는 계정을 다시 개설해야만 콘텐츠와 AWS 서비스에 액세스할 수 있습니다. 폐쇄 후 기간이 지나면 계정이 AWS 영구적으로 폐쇄되며 더 이상 AWS 계정계정을 다시 열 수 없습니다. AWS 또한 계정의 모든 콘텐츠와 리소스도 삭제됩니다. 계정이 영구 폐쇄된 후에는 해당 AWS 계정 ID를 다시 사용할 수 없습니다.

계정 재개설 AWS 계정

계정은 90일 후에 영구적으로 폐쇄되며, 그 이후에는 계정을 다시 열 수 없으며 계정에 남아 있는 콘텐츠가 AWS 삭제됩니다. 계정이 영구 폐쇄되기 전에 계정을 다시 개설하려면 (1) 가능한 한 AWS Support빨리 연락해야 하며, (2) 계정 폐쇄일로부터 60일 이내에 청구서에 명시된 필수 정보 제공을 포함하여 미결제 잔액 전액을 당사에 수령해야 합니다.

조직 내 AWS 계정 관리 사용

AWS Organizations그룹으로 관리하는 AWS 계정 데 사용할 수 있는 AWS 서비스입니다. 이는 계정의 모든 청구서를 그룹화하여 한 명의 지불자가 처리하는 통합 청구와 같은 기능을 제공합니다. 또한 정책 기반 제어를 사용하여 조직의 보안을 중앙에서 관리할 수 있습니다. AWS Organizations에 대한 자세한 내용은 사용 설명서AWS Organizations를 참조하세요.

트러스트된 액세스

계정을 그룹으로 관리하는 AWS Organizations 데 사용하는 경우 조직에 대한 대부분의 관리 작업은 조직의 관리 계정으로만 수행할 수 있습니다. 기본적으로 여기에는 조직 자체 관리와 관련된 작업만 포함됩니다. 조직과 해당 AWS 서비스 간에 신뢰할 수 있는 액세스를 허용하여 이 추가 기능을 다른 서비스로 확장할 수 있습니다. 신뢰할 수 있는 액세스는 지정된 AWS 서비스에 조직 및 포함된 계정에 대한 정보에 액세스할 수 있는 권한을 부여합니다. 계정 관리에 신뢰할 수 있는 액세스를 활성화하면 계정 관리 서비스에서 조직 및 해당 관리 계정에 기관의 모든 구성원 계정에 대한 기본 연락처 또는 대체 연락처 정보와 같은 메타데이터에 액세스할 수 있는 권한을 부여합니다.

자세한 정보는 AWS계정 관리를 위한 신뢰할 수 있는 액세스 활성화을 참조하세요.

위임된 관리자

신뢰할 수 있는 액세스를 활성화한 후 구성원 계정 중 하나를 계정 관리를 위한 AWS위임된 관리자 계정으로 지정하도록 선택할 수도 있습니다. 이렇게 하면 위임된 관리자 계정은 이전에 관리 계정만 수행할 수 있었던 것과 동일한 Account Management 메타데이터 관리 작업을 조직의 구성원 계정에 대해 수행할 수 있습니다. 위임된 관리자 계정은 계정 관리 서비스의 관리 작업에만 액세스할 수 있습니다. 위임된 관리자 계정에는 관리 계정에 있는 조직에 대한 모든 관리 액세스 권한이 없습니다.

자세한 정보는 에 대해 위임된 관리자 계정 활성화AWS계정 관리을 참조하세요.

서비스 제어 정책

에서 관리하는 조직에 속해 AWS Organizations 있는 경우 해당 기관의 관리자는 구성원 계정의 보안 주체가 수행할 수 있는 작업을 제한할 수 있는 서비스 제어 정책 (SCP) 을 적용할 수 있습니다. AWS 계정 SCP는 권한을 부여하지 않습니다. 대신 회원 계정에서 사용할 수 있는 권한을 제한하는 필터입니다. 구성원 계정의 사용자 또는 역할 (주체) 은 해당 계정에 적용되는 SCP가 허용하는 것과 보안 주체에 연결된 IAM 권한 정책이 교차하는 작업만 수행할 수 있습니다. 예를 들어, SCP를 사용하여 계정의 보안 주체가 자신의 계정의 대체 연락처를 수정하는 것을 방지할 수 있습니다.

에 적용되는 SCP의 예는 AWS 계정 을 참조하십시오를 사용하여 액세스 제한AWS Organizations서비스 제어 정책.

AWS계정 관리를 위한 신뢰할 수 있는 액세스 활성화

AWS계정 관리에 대한 신뢰할 수 있는 액세스를 활성화하면 관리 계정 관리자가 에서 각 구성원 계정과 관련된 정보 및 메타데이터 (예: 기본 연락처 또는 대체 연락처 세부 정보) 를 수정할 수 있습니다. AWS Organizations 자세한 내용은 AWS계정 관리 및 AWS OrganizationsAWS Organizations 사용 설명서를 참조하십시오. 신뢰할 수 있는 액세스의 작동 방식에 대한 일반 정보는 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하십시오.

신뢰할 수 있는 액세스가 활성화되면 이를 지원하는 계정 관리 API 작업에서 `accountID` 파라미터를 사용할 수 있습니다. 관리 계정의 자격 증명을 사용하여 작업을 호출하거나 조직의 위임된 관리자 계정을 활성화한 경우에만 이 매개 변수를 성공적으로 사용할 수 있습니다. 자세한 정보는 에 대해 위임된 관리자 계정 활성화AWS계정 관리을 참조하세요.

다음 절차를 사용하여 조직의 계정 관리에 대한 신뢰할 수 있는 액세스를 활성화하십시오.

> 최소 권한
>
> 이러한 작업을 수행하려면 다음 요구 사항을 충족해야 합니다.
>
> - 이 작업은 조직의 관리 계정에서만 수행할 수 있습니다.
> - 조직의 모든 기능을 활성화해야 합니다.

AWS Management Console

AWS계정 관리에 신뢰할 수 있는 액세스를 활성화하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인(권장되지 않음)해야 합니다.
2. 탐색 창에서 [서비스] 를 선택합니다.
3. 서비스 목록에서 AWS계정 관리를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS계정 관리에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 enable을 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.

AWS CLI & SDKs

AWS계정 관리에 신뢰할 수 있는 액세스를 활성화하려면

다음 명령을 실행한 후 조직 관리 계정의 자격 증명을 사용하여 `--accountId` 매개 변수를 사용하여 조직의 구성원 계정을 참조하는 Account Management API 작업을 호출할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 예에서는 발신 계정 조직의 AWS 계정 관리에 대한 신뢰할 수 있는 액세스를 활성화합니다.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  성공 시 이 명령은 출력을 생성하지 않습니다.

에 대해 위임된 관리자 계정 활성화AWS계정 관리

위임된 관리자 계정은AWS조직의 다른 멤버 계정의 계정 관리 API 작업입니다. 조직의 구성원 계정을 위임된 관리자 계정으로 지정하려면 다음 절차를 따르십시오.

> 최소 권한
>
> 이러한 작업을 수행하려면 다음 요구 사항을 충족해야 합니다.
>
> - 이 작업은 조직의 관리 계정에서만 수행할 수 있습니다.
> - 조직의 모든 기능을 활성화해야 합니다.
> - 해야 할 사항조직의 계정 관리에 대한 신뢰할 수 있는 액세스 사용.

조직에 위임된 관리자 계정을 지정하면 해당 계정의 사용자 및 역할이AWS CLI과AWSSDK 작업`account`선택 사항을 지원하여 Organizations 모드에서 작동할 수 있는 네임스페이스`AccountId`파라미터.

AWS Management Console

이 작업은 에서 지원되지 않습니다.AWS계정 관리 콘솔을 엽니다. 이 작업은 을 사용해야만 수행할 수 있습니다.AWS CLI또는 다음 중 하나의 API 작업AWSSDK.

AWS CLI & SDKs

계정 관리 서비스에 위임된 관리자 계정을 등록하려면

다음 명령을 사용하여 계정 관리 서비스에 대해 위임된 관리자를 활성화할 수 있습니다.

다음 서비스 보안 주체를 지정해야 합니다.

```
account.amazonaws.com
```

- AWS CLI:등록 위임된 관리자

  다음 예제에서는 조직의 구성원 계정을 계정 관리 서비스에 대한 위임된 관리자로 등록합니다.

  ```
  $ aws organizations register-delegated-administrator \
      --account-id 123456789012 \
      --service-principal account.amazonaws.com
  ```

  이 명령은 성공 시 출력을 생성하지 않습니다.

  이 명령을 실행한 후 계정 123456789012의 자격 증명을 사용하여 계정 관리를 호출할 수 있습니다.AWS CLI및 다음을 사용하는 SDK API 작업`--account-id`조직의 멤버 계정을 참조하는 매개 변수입니다.

를 사용하여 액세스 제한AWS Organizations서비스 제어 정책

이 주제에서는 서비스 제어 정책 (SCP) 을 사용하여 조직의 계정에 있는 사용자와 역할이 수행할 수 있는 작업을 제한하는 방법을 보여 주는 예제를 제공합니다. 서비스 제어 정책에 대한 자세한 내용은 의 다음 주제를 참조하십시오.AWS Organizations사용 설명서:

- SCP 생성
- OU 및 계정에 SCP 연결
- SCP 전략
- SCP 정책 구문

Example 예제 1: 계정이 자신의 대체 연락처를 수정하지 못하도록 방지

다음 예제에서는`PutAlternateContact`과`DeleteAlternateContact`의 멤버 계정에서 API 작업을 호출하지 못함독립 실행형 계정. 이렇게 하면 영향을 받는 계정의 보안 주체가 자신의 대체 연락처를 변경할 수 없습니다.

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

```
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "arn:aws:account::*:account" ]
        }
    ]
}
```

Example 예제 2: 구성원 계정이 조직의 다른 구성원 계정에 대한 대체 연락처를 수정하지 못하도록 합니다.

다음 예제에서는Resource요소를 “*”로 지정합니다. 이는 두 요소 모두에 적용됨을 의미합니다.독립형 모드 요청 및 조직 모드 요청. 즉, SCP가 적용되는 경우 계정 관리에 대해 위임된 관리자 계정조차도 조직의 모든 계정에 대한 대체 연락처를 변경할 수 없습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "*" ]
        }
    ]
}
```

Example 예제 3: OU의 구성원 계정이 자체 대체 연락처를 수정하지 못하도록 방지

다음 예제 SCP에는 계정의 조직 경로를 두 OU 목록과 비교하는 조건이 포함되어 있습니다. 이렇게 하면 지정된 OU의 계정에 있는 보안 주체가 자신의 대체 연락처를 수정하지 못하도록 차단됩니다.

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

```
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": "account:PutAlternateContact",
            "Resource": [
                "arn:aws:account::*:account"
            ],
            "Condition": {
                "ForAnyValue:StringLike": {
                    "account:AccountResourceOrgPath": [
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/",
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
                    ]
                }
            }
    ]
}
```

의 보안AWS계정 관리

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 매우 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 귀하의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안 – AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. 또한, AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램의 일환으로 보안 효과를 정기적으로 테스트하고 검증합니다. 계정 관리에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 단원을 참조하십시오.AWS 서비스규정 준수 프로그램별 범위.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스로 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 사용 시 책임 공유 모델을 적용하는 방법을 이해하는 데 도움이 됩니다.AWS계정 관리. 계정 관리를 구성하여 보안 및 규정 준수 목적에 맞게 를 구성하는 방법을 보여줍니다. 또한 다른 사용 방법을 배웁니다.AWS계정 관리 리소스를 모니터링하고 보호하는 데 도움이 되는 서비스입니다.

주제

- AWS계정 관리에서의 데이터 보호
- AWS PrivateLink...에 대한AWS계정 관리
- AWS계정 관리를 위한 Identity 및 Access Management
- AWS에 대한 관리형 정책AWS계정 관리
- AWS계정 관리를 위한 규정 준수 검증
- 의 복원성AWS계정 관리
- AWS Account Management의 인프라 보안

AWS계정 관리에서의 데이터 보호

AWS공동 책임 모델 AWS 계정 관리의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS은(는) 모든 AWS 클라우드을(를) 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스의 보안

구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정 보안 인증 정보를 보호하고 AWS IAM Identity Center 또는 AWS Identity and Access Management(IAM)을 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이러한 방식에는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- AWS CloudTrail(으)로 API 및 사용자 활동 로깅을 설정합니다.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용합니다.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 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.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔AWS CLI, API 또는 AWS 서비스 AWS SDK를 사용하여 계정 관리 또는 기타 작업을 수행하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

AWS PrivateLink...에 대한AWS계정 관리

Amazon Virtual Private Cloud (Amazon VPC) 를 사용하여 호스트하는 경우AWS리소스에 액세스할 수 있습니다.AWS공용 인터넷을 통과할 필요 없이 VPC 내에서 계정 관리 서비스입니다.

Amazon VPC 시작할 수 있습니다.AWS사용자 지정 가상 네트워크의 리소스 VPC를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC에 대한 자세한 내용은 를 참조하십시오.Amazon VPC User Guide.

Amazon VPC 계정 관리에 연결하려면 먼저인터페이스 VPC 엔드포인트를 사용하면 VPC를 다른 VPC 연결할 수 있습니다.AWS서비스. 이 엔드포인트를 이용하면 인터넷 게이트웨이나 NAT(네트워크 주소

변환) 인스턴스 또는 VPN 연결 없이도 안정적이고 확장 가능하게 연결됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.

엔드포인트 만들기

를 생성할 수 있습니다.AWSVPC 계정 관리 엔드포인트AWS Management Console,AWS Command Line Interface(AWS CLI), aAWSSDKAWS계정 관리 API 또는AWS CloudFormation.

Amazon VPC 콘솔 또는 AWS CLI를 사용한 엔드포인트 생성 및 구성에 대한 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

> **Note**
>
> 엔드포인트를 생성할 때 VPC 연결할 서비스로 계정 관리를 지정해야 합니다. 이 형식을 사용합니다.
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> 표시된 대로 문자열을 정확하게 사용해야 합니다.`us-east-1`리전. 글로벌 서비스로서 계정 관리는 해당 서비스에서만 호스팅됩니다.AWS리전.

AWS CloudFormation을 사용하여 엔드포인트를 생성하고 구성하는 방법에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS::EC2::VPCEndpoint 리소스를 참조하세요.

Amazon VPC 엔드포인트 정책

Amazon VPC 엔드포인트를 생성할 때 엔드포인트 정책을 연결하여 이 서비스 엔드포인트를 통해 수행할 수 있는 작업을 제어할 수 있습니다. 여러 엔드포인트 정책을 연결하여 복잡한 IAM 규칙을 생성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- Amazon Virtual Private Cloud 엔드포인트 정책 관리
- VPC 엔드포인트로 서비스에 대한 액세스 제어의AWS PrivateLink안내서.

Amazon Virtual Private Cloud 엔드포인트 정책 관리

계정 관리를 위한 Amazon VPC 엔드포인트 정책을 생성하여 다음을 지정할 수 있습니다.

- 태스크를 수행할 수 있는 보안 주체.

- 보안 주체가 수행할 수 있는 작업입니다.
- 작업을 수행할 수 있는 리소스

다음 예에서는 계정 123456789012에서 Alice라는 IAM 사용자 한 명이 대체 연락처 정보를 검색하고 변경할 수 있도록 허용하는 Amazon VPC 엔드포인트 정책을 보여 줍니다.AWS 계정모든 IAM 사용자가 모든 계정의 대체 연락처 정보를 삭제할 수 있는 권한을 거부합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "account:GetAlternateContact",
                "account:PutAlternateContact"
            ],
            "Resource": "arn:aws::iam:*:account,
            "Effect": "Allow",
            "Principal": {
              "AWS": "arn:aws::iam:123456789012:user/Alice"
            }
        },
        {
            "Action": "account:DeleteAlternateContact",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "arn:aws::iam:*:root"
        }
    ]
}
```

에 속하는 계정에 액세스 권한을 부여하려는 경우AWS조직을 조직의 구성원 계정 중 하나에 있는 보안 주체로 이동한 다음Resourceelement는 다음 형식을 사용해야 합니다.

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

엔드포인트 정책 생성에 대한 자세한 내용은 단원을 참조하십시오.VPC 엔드포인트로 서비스에 대한 액세스 제어의AWS PrivateLink안내서.

AWS계정 관리를 위한 Identity 및 Access Management

AWS Identity and Access Management(IAM)은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 지원하는 AWS 서비스입니다. IAM 관리자는 계정 관리 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 관리합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

고객

계정 관리에서 수행하는 작업에 따라 사용 방식 AWS Identity and Access Management (IAM) 이 다릅니다.

서비스 사용자 - 계정 관리 서비스를 사용하여 업무를 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 계정 관리 기능을 사용하여 업무를 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. 계정 관리의 기능에 액세스할 수 없는 경우 을 참조하십시오AWS계정 관리 ID 및 액세스 문제 해결.

서비스 관리자 — 회사에서 계정 관리 리소스를 담당하는 경우 계정 관리에 대한 전체 액세스 권한이 있을 것입니다. 서비스 사용자가 액세스해야 하는 계정 관리 기능 및 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사에서 계정 관리와 함께 IAM을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오AWS계정 관리가 IAM과 함께 작동하는 방식.

IAM 관리자 — IAM 관리자라면 계정 관리에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 계정 관리 ID 기반 정책의 예를 보려면 을 참조하십시오. 계정 관리를 위한 ID 기반 정책 예제 AWS

보안 인증 정보를 통한 인증

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

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

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

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

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS는 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

AWS 계정을 생성할 때는 해당 계정의 모든 AWS 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 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

페더레이션 ID

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 사용자가 자격 증명 공급자와의 페더레이션을 통해 임시 보안 인증을 사용하여 AWS 서비스에 액세스하도록 요구하는 것입니다.

연동 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리의 사용자 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서

비스에 액세스하는 모든 사용자입니다. 페더레이션 보안 인증 정보는 AWS 계정에 액세스할 때 역할을 수임하고 역할은 임시 보안 인증 정보를 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 AWS 계정및 애플리케이션에서 사용하기 위해 고유한 자격 증명 소스의 사용자 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가지고 있는 AWS 계정내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

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

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 보안 인증을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가지고 있는 AWS 계정계정 내 ID입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할 전환하여 AWS Management Console에서 IAM 역할을 임시로 수임할 수 있습니다. AWS CLI 또는 AWSAPI 태스크를 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 자격 증명에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이

부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 Creating a role for a third-party Identity Provider(서드 파티 자격 증명 공급자의 역할 만들기) 부분을 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 보안 인증 정보에서 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연결합니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center사용 설명서의 권한 세트를 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스: IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스를 사용하면 역할을(프록시로 사용하는 대신) 리소스에 정책을 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.
- 교차 서비스 액세스 - 일부 AWS 서비스는 다른 AWS 서비스의 기능을 사용합니다. 예를 들어 서비스에서 직접적으로 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 보안 주체의 권한과 요청하는 AWS 서비스를 함께 사용하여 다운스트림 서비스에 대한 요청을 수행합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하십시오.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
  - 서비스 연결 역할 - 서비스 연결 역할은 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon EC2에서 실행 중인 애플리케이션 – IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI또는 AWSAPI 요청을 수행하는 애플리케이션의 임시 보안 인증 정보를 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS역할을 할당하고 해당 역할을 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서

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

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 AWSID 또는 리소스에 연결하여 AWS내 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 해당 권한을 정의하는 AWS의 객체입니다. AWS는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청을 보낼 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되는지 또는 거부되는지를 결정합니다. 대부분의 정책은 AWS에 JSON 설명서로서 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

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

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

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

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 AWS 계정에 속한 다수의 사용자, 그룹 및 역할에 독립적으로 추가할 수 있는 정책입니다. 관리형 정책에는 AWS관리형 정책과 고객 관리형 정책이 포함되어 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 AWS 서비스가 포함될 수 있습니다.

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

액세스 제어 목록(ACL)

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

Amazon S3, AWS WAF및 Amazon VPC는 ACL을 지원하는 대표적인 서비스입니다. ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 참조하십시오.

기타 정책 유형

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

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 ID 기반 정책 및 해당 권한 경계의 교집합입니다. `Principal`필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.
- 서비스 제어 정책(SCP) – SCP는 AWS Organizations에서 조직 또는 조직 단위(OU)에 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations은 기업이 소유하는 여러 개의 AWS 계정를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 AWS 계정 루트 사용자을 비롯하여 멤버 계정의 엔터티에 대한 권한을 제한합니다. 조직 및 SCP에 대한 자세한 정보는 AWS Organizations사용 설명서의 SCP 작동 방식을 참조하세요.

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

여러 정책 유형

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

AWS계정 관리가 IAM과 함께 작동하는 방식

IAM을 사용하여 계정 관리에 대한 액세스를 관리하기 전에 계정 관리에 사용할 수 있는 IAM 기능에 대해 알아보세요.

계정 관리와 함께 사용할 수 있는 IAM 기능 AWS

IAM 특성	계정 관리 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
보안 주체 권한	예

IAM 특성	계정 관리 지원
서비스 역할	아니요
서비스 연결 역할	아니오

계정 관리 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는 AWS 서비스를 참조하십시오.

계정 관리를 위한 ID 기반 정책

ID 기반 정책 지원	예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조 섹션을 참조하십시오.

계정 관리를 위한 ID 기반 정책 예제

계정 관리 ID 기반 정책의 예를 보려면 을 참조하십시오. 계정 관리를 위한 ID 기반 정책 예제 AWS

계정 관리 내의 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다.

리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 AWS 서비스이(가) 포함될 수 있습니다.

교차 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념합니다. 보안 주체와 리소스가 서로 다른 AWS 계정에 있는 경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체(사용자 또는 역할)에도 리소스 액세스 권한을 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 ID 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이 섹션을 참조하십시오.

계정 관리를 위한 정책 조치

정책 작업 지원	예

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

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

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

계정 관리 작업 목록을 보려면 서비스 권한 부여 참조의 AWS Account Management에서 정의한 작업을 참조하십시오.

계정 관리의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
account
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "account:action1",
      "account:action2"
```

```
        ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, AWS 계정 의 대체 연락처와 함께 작동하는 모든 작업을 지정하려면 다음 작업을 포함하십시오.

```
"Action": "account:*AlternateContact"
```

계정 관리 ID 기반 정책의 예를 보려면 을 참조하십시오. 계정 관리를 위한 ID 기반 정책 예제 AWS

계정 관리를 위한 정책 리소스

정책 리소스 지원	예

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

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

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

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

계정 관리 서비스는 정책을 필터링하고 이러한 유형의 리소스를 구분할 수 있도록 IAM 정책 Resources 요소에서 다음과 같은 특정 리소스 유형을 지원합니다. AWS 계정

- account

  이 resource 유형은 서비스에서 관리하는 조직의 구성원 계정이 AWS 계정 아닌 독립형 계정과만 일치합니다AWS Organizations.
- accountInOrganization

  이 resource 유형은 AWS Organizations 서비스에서 관리하는 조직의 구성원 계정에만 AWS 계정 일치합니다.

계정 관리 리소스 유형 및 해당 ARN 목록을 보려면 서비스 권한 부여 참조의 AWS Account Management에서 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 AWS계정 관리에서 정의한 작업을 참조하십시오.

계정 관리 ID 기반 정책의 예를 보려면 을 참조하십시오. 계정 관리를 위한 ID 기반 정책 예제 AWS

계정 관리를 위한 정책 조건 키

서비스별 정책 조건 키 지원	예

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

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

한 문에서 여러 `Condition`요소를 지정하거나 단일 `Condition`요소에서 여러 키를 지정하는 경우 AWS는 논리적 `AND`태스크를 사용하여 평가합니다. 단일 조건 키의 여러 값을 지정하는 경우 AWS는 논리적 `OR`태스크를 사용하여 조건을 평가합니다. 명령문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

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

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

계정 관리 서비스는 IAM 정책을 세밀하게 필터링하는 데 사용할 수 있는 다음과 같은 조건 키를 지원합니다.

- 계정: TargetRegion

  이 조건 키는 AWS지역 코드 목록으로 구성된 인수를 사용합니다. 정책을 필터링하여 지정된 지역에 적용되는 작업에만 영향을 줄 수 있습니다.
- 계정: AlternateContactTypes

  이 조건 키는 대체 연락처 유형 목록을 사용합니다.

- 청구
- OPERATIONS
- SECURITY

이 키를 사용하면 지정된 대체 연락처 유형을 대상으로 하는 작업으로만 요청을 필터링할 수 있습니다.

- 계정: AccountResourceOrgPaths

  이 조건 키는 ARN 목록과 조직의 계정을 나타내는 와일드카드로 구성된 인수를 사용합니다. 정책을 필터링하여 일치하는 ARN이 있는 계정을 대상으로 하는 작업에만 영향을 미치도록 할 수 있습니다. 예를 들어 다음 ARN은 지정된 조직 및 지정된 OU (조직 구성 단위) 의 계정과만 일치합니다.

```
arn:aws:account::111111111111:ou/o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
```

- 계정: AccountResourceOrgTags

  이 조건 키는 태그 키 및 값 목록으로 구성된 인수를 사용합니다. 정책을 필터링하여 조직의 구성원이고 지정된 태그 키와 값으로 태그가 지정된 계정에만 영향을 미치도록 할 수 있습니다.

계정 관리 조건 키 목록을 보려면 서비스 권한 부여 참조의 AWS 계정 관리를 위한 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 AWS계정 관리에서 정의한 작업을 참조하십시오.

계정 관리 ID 기반 정책의 예를 보려면 을 참조하십시오. 계정 관리를 위한 ID 기반 정책 예제 AWS

계정 관리의 액세스 제어 목록

ACL 지원	아니요

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

계정 관리를 통한 속성 기반 액세스 제어

ABAC 지원(정책의 태그)	예

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

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

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

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

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

계정 관리를 통한 임시 자격 증명 사용

임시 보안 인증 지원	예

일부 AWS 서비스는 임시 보안 인증 정보를 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 작동하는 AWS 서비스를 비롯한 추가 정보는 IAM 사용 설명서의 IAM으로 작업하는 AWS 서비스를 참조하세요.

사용자 이름과 암호를 제외한 다른 방법을 사용하여 AWS Management Console에 로그인하면 임시 보안 인증 정보를 사용하는 것입니다. 예를 들어 회사의 Single Sign-On(SSO) 링크를 사용하여 AWS에 액세스하면 해당 프로세스에서 자동으로 임시 보안 인증 정보를 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증 정보를 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWSAPI를 사용하여 임시 보안 인증 정보를 수동으로 만들 수 있습니다 그런 다음 이러한 임시 보안 인증 정보를 사용하여 AWS에 액세스할 수 있습니다. AWS에서는 장기 액세스 키를 사용하는 대신 임시 보안 인증 정보를 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명을 참조하십시오.

계정 관리를 위한 크로스 서비스 사용자 권한

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 보안 주체의 권한과 요청하는 AWS 서비스를 함께 사용하여 다운스트림 서비스에 대한 요청을 수행합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

계정 관리를 위한 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

계정 관리를 위한 서비스 연결 역할

서비스 연결 역할 지원	아니오

서비스 연결 역할은 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는 AWS서비스 단원을 참조하세요. 서비스 연결 역할 열에서 `Yes`이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

계정 관리를 위한 ID 기반 정책 예제 AWS

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

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

각 리소스 유형의 ARN 형식을 포함하여 Account Management에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS 계정 관리를 위한 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례
- 내 계정 페이지 사용 AWS Management Console
- 계정 페이지에 대한 읽기 전용 액세스 권한 제공 AWS Management Console
- 계정 페이지에 대한 전체 액세스 권한 제공 AWS Management Console

정책 모범 사례

ID 기반 정책은 누군가가 사용자 계정에서 Account Management 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS관리형 정책을 사용합니다. 관리형 정책은 AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWSmanaged policies(관리형 정책) 또는 AWSmanaged policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한: 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 특정 AWS 서비스(예: AWS CloudFormation)을(를) 통해 사용되는 경우에만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 IAM 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하십시오.

- 다중 인증(MFA) 필요 – AWS 계정계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

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

내 계정 페이지 사용 AWS Management Console

에서 계정 페이지에 액세스하려면 최소 권한 집합이 있어야 합니다. AWS Management Console 이러한 권한을 통해 자신의 세부 정보를 나열하고 볼 수 있어야 AWS 계정 합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(IAM 사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

사용자와 역할이 Account Management 콘솔을 사용할 수 있도록 하려면 엔티티에 `AWSAccountManagementReadOnlyAccess` 또는 `AWSAccountManagementFullAccess` AWS 관리형 정책을 연결하도록 선택할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신 대부분의 경우 수행하려는 API 작업과 일치하는 작업에만 액세스를 허용하도록 선택할 수 있습니다.

계정 페이지에 대한 읽기 전용 액세스 권한 제공 AWS Management Console

다음 예시에서는 IAM 사용자에게 의 계정 페이지에 대한 AWS 계정 읽기 전용 액세스 권한을 부여하려고 합니다. AWS Management Console 이 정책이 연결된 사용자는 아무 것도 변경할 수 없습니다.

이 `account:GetAccountInformation` 작업을 통해 계정 페이지에 있는 대부분의 설정을 볼 수 있는 액세스 권한이 부여됩니다. 하지만 현재 활성화된 AWS 지역을 보려면 `account:ListRegions` 작업도 포함해야 합니다.

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

```
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

계정 페이지에 대한 전체 액세스 권한 제공 AWS Management Console

다음 예시에서는 IAM 사용자에게 의 계정 페이지에 대한 AWS 계정 전체 액세스 권한을 부여하려고 합니다AWS Management Console. 이 정책이 연결된 사용자는 계정 설정을 변경할 수 있습니다.

이 예제 정책은 이전 예제 정책을 기반으로 사용 가능한 각 쓰기 권한 (제외 CloseAccount) 을 추가하여 사용자가 `account:EnableRegion` 및 `account:DisableRegion` 권한을 포함하여 계정에 대한 대부분의 설정을 변경할 수 있도록 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutChallengeQuestions",
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

계정 관리를 위한 ID 기반 정책 (IAM 정책) 사용 AWS

AWS 계정 및 IAM 사용자에 관한 전체 논의는 IAM 사용 설명서의 IAM이란 무엇입니까?를 참조하세요.

고객 관리형 정책을 업데이트하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 고객 관리형 정책 편집(콘솔)을 참조하세요.

AWS계정 관리 조치 정책

이 표에는 계정 설정에 대한 액세스 권한을 부여하는 권한이 요약되어 있습니다. 이러한 권한을 사용하는 정책의 예는 AWS계정 관리 정책 예를 참조하십시오.

> **Note**
>
> 의 계정 페이지에서 IAM 사용자에게 특정 계정 설정에 대한 쓰기 액세스 권한을 부여하려면 해당 설정을 수정하는 데 사용할 권한 (또는 권한) 외에도 해당 권한을 허용해야 합니다. AWS Management Console `GetAccountInformation`

권한 이름	액세스 레벨	설명
`account:ListRegions`	목록	사용 가능한 지역을 나열할 권한을 부여합니다.
`account:GetAccountInformation`	읽기	계정의 계정 정보를 검색할 권한을 부여합니다.
`account:GetAlternateContact`	읽기	계정의 대체 연락처를 검색할 권한을 부여합니다.
`account:GetChallengeQuestions`	읽기	계정에 대한 챌린지 질문을 검색할 수 있는 권한을 부여합니다.
`account:GetContactInformation`	읽기	계정의 기본 연락처 정보를 검색할 권한을 부여합니다.
`account:GetRegionOptStatus`	읽기	지역의 옵트인 상태를 얻을 수 있는 권한을 부여합니다.
`account:CloseAccount`	쓰기	계정을 폐쇄할 권한을 부여합니다.

권한 이름	액세스 레벨	설명
		Note 이 권한은 콘솔에만 해당합니다. 이 권한으로 이용할 수 있는 API 액세스는 없습니다.
account:DeleteAlternateContact	쓰기	계정의 대체 연락처를 삭제할 권한을 부여합니다.
account:DisableRegion	쓰기	지역 사용을 비활성화할 권한을 부여합니다.
account:EnableRegion	쓰기	지역을 사용할 수 있는 권한을 부여합니다.
account:PutAlternateContact	쓰기	계정의 대체 연락처를 수정할 권한을 부여합니다.
account:PutChallengeQuestions	쓰기	계정의 챌린지 질문을 수정할 수 있는 권한을 부여합니다. Note 이 권한은 콘솔에만 해당합니다. 이 권한으로 이용할 수 있는 API 액세스는 없습니다.
account:PutContactInformation	쓰기	계정의 기본 연락처 정보를 업데이트할 권한을 부여합니다.

AWS계정 관리 ID 및 액세스 문제 해결

다음 정보를 사용하면 계정 관리 및 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

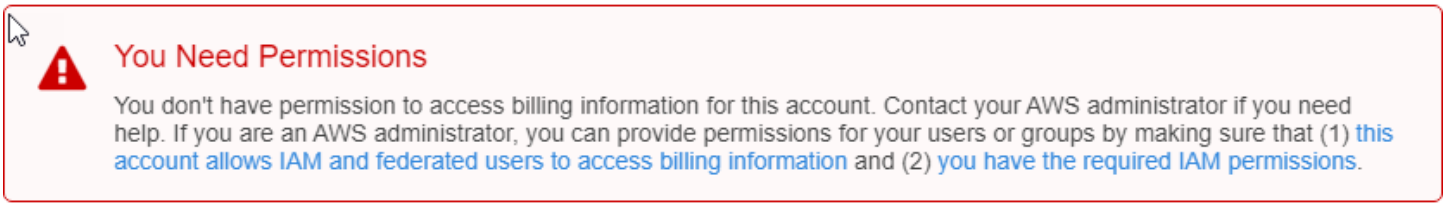
주제

- 계정 페이지에서 작업을 수행할 권한이 없습니다.
- iam:PassRole을 수행할 권한이 없음
- 외부 사용자가 내 계정 세부 정보에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

계정 페이지에서 작업을 수행할 권한이 없습니다.

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

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 의 계정 페이지에서 자신의 AWS 계정 세부 정보를 보려고 AWS Management Console 하지만 `account:GetAccountInformation` 권한이 없는 경우 발생합니다.



이 경우 Mateo는 *`my-example-widget`* 작업을 사용하여 `account:`*`GetWidget`* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

`iam:PassRole`을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 발생하는 경우 `iam:PassRole` Account Management에 역할을 넘길 수 있도록 정책을 업데이트해야 합니다.

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

다음 예제 오류는 이라는 IAM 사용자가 콘솔을 사용하여 Account Management에서 작업을 `marymajor` 수행하려고 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

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

도움이 필요한 경우 AWS관리자에게 문의하세요. 관리자는 로그인 보안 인증을 제공한 사용자입니다.

외부 사용자가 내 계정 세부 정보에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

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

자세히 알아보려면 다음을 참조하십시오.

- 계정 관리가 이러한 기능을 지원하는지 알아보려면 을 참조하십시오AWS계정 관리가 IAM과 함께 작동하는 방식.
- 소유하고 있는 AWS 계정의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공을 참조하십시오.
- 리소스에 대한 액세스 권한을 서드 파티 AWS 계정에게 제공하는 방법을 알아보려면 IAM 사용 설명서의 서드 파티가 소유한 AWS 계정에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하십시오.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.

AWS에 대한 관리형 정책AWS계정 관리

AWS계정 관리는 현재 두 가지를 제공합니다.AWS사용할 수 있는 관리형 정책:

- AWS 관리형 정책: AWSAccountManagementReadOnlyAccess
- AWS 관리형 정책: AWSAccountManagementFullAccess
- 계정 관리 업데이트AWS관리형 정책

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

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

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

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSAccountManagementReadOnlyAccess

`AWSAccountManagementReadOnlyAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 다음을 보기만 할 수 있는 읽기 전용 권한을 제공합니다.

- 귀하에 대한 메타데이터AWS 계정
- 더AWS 리전에 대해 활성화 또는 비활성화된AWS 계정(계정의 지역 상태는 다음을 통해서만 볼 수 있습니다.AWS콘솔)

이 작업은 다음 중 하나를 실행할 수 있는 권한을 부여하여 수행됩니다.`Get*`또는`List*`오퍼레이션. 계정 메타데이터를 수정하거나 활성화 또는 비활성화하는 기능은 제공하지 않습니다.AWS 리전계정을 위해.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `account`— 보안 주체가 다음에 대한 메타데이터 정보를 검색할 수 있습니다.AWS 계정. 또한 교장이 다음 사항을 나열할 수 있습니다.AWS 리전해당 계정에 대해 활성화되어 있는AWS Management Console.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSAccountManagementFullAccess

AWSAccountManagementFullAccess 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 다음을 보거나 수정할 수 있는 전체 관리자 액세스를 제공합니다.

- 귀하에 대한 메타데이터AWS 계정
- 더AWS 리전에 대해 활성화 또는 비활성화된AWS 계정(계정을 통해서만 상태를 보거나 계정의 지역을 활성화 또는 비활성화할 수 있습니다.AWS콘솔)

이는 모든 것을 실행할 수 있는 권한을 부여하여 수행됩니다.account오퍼레이션.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- account— 주체가 다음에 대한 메타데이터 정보를 보거나 수정할 수 있습니다.AWS 계정. 또한 교장이 다음 사항을 나열할 수 있습니다.AWS 리전계정에 대해 활성화되어 있고 해당 계정에서 활성화 또는 비활성화됩니다.AWS Management Console.

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

```
        }
    ]
}
```

계정 관리 업데이트AWS관리형 정책

업데이트에 대한 세부 정보 보기AWS이 서비스에서 이러한 변경 사항을 추적하기 시작한 이후로 계정 관리에 대한 정책이 관리되었습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 계정 관리 문서 기록 페이지의 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AWS신규 버전과 함께 계정 관리 출시AWS정책 관리 및 변경 추적 시작	계정 관리는 처음에 다음과 같이 시작되었습니다.AWS관리형 정책: • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	2021년 9월 30일

AWS계정 관리를 위한 규정 준수 검증

타사 감사자는 여러 규정 준수 프로그램의 AWS 계정 일부로 귀사에서 실행할 수 있는 AWS 서비스의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램의 범위에 속하는 AWS 서비스 목록은 규정 준수 프로그램별 범위에서 규정 준수 AWS 서비스 프로그램별 참조하십시오AWS 서비스. 일반적인 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact사용 설명서의 보고서 AWS ArtifactAWS Artifact 다운로드에서 참조하십시오.

서비스를 사용할 때의 규정 준수 AWS 계정 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 결정됩니다. AWS규정 준수에 도움이 되는 다음과 같은 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 – 이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔 기본 AWS 환경을 배포하기 위한 단계를 제공합니다.

- Amazon Web Services에서 HIPAA 보안 및 규정 준수 기술 백서 설계 - 이 백서는 기업에서 AWS를 사용하여 HIPAA를 준수하는 애플리케이션을 만드는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스에 HIPAA 자격이 있는 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하세요.

- AWS 규정 준수 리소스 - 고객 조직이 속한 산업 및 위치에 적용될 수 있는 워크북 및 가이드 콜렉션입니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 – AWS Config 서비스는 내부 사례, 산업 지침 및 규제에 대한 리소스 구성의 준수 상태를 평가합니다.
- AWS Security Hub - 이 AWS 서비스는 보안 산업 표준 및 모범 사례 규정 준수 여부를 확인하는 데 도움이 되도록 AWS 내 보안 상태를 종합적으로 보여줍니다.
- AWS Audit Manager - 이 AWS 서비스는 AWS 사용을 지속해서 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 간소화할 수 있도록 지원합니다.

의 복원성AWS계정 관리

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

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

AWS Account Management의 인프라 보안

관리 서비스로서 사용자 AWS 계정 내에서 실행되는 AWS 서비스는 AWS 글로벌 네트워크 보안에 의해 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.

AWS게시된 API 호출을 사용하여 네트워크를 통해 계정 설정에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS계정 관리 모니터링

모니터링은 AWS 계정 관리 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS계정 관리를 관찰하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail사용자가 또는 사용자를 대신하여 수행한 API 호출 및 관련 이벤트를 캡처 (기록) AWS 계정 하고 지정한 Amazon Simple Storage Service (Amazon S3) 버킷에 로그 파일을 씁니다. 이를 통해 어떤 사용자와 계정이 전화를 걸었는지AWS, 어떤 소스 IP 주소에서 전화를 걸었는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 사용 설명서AWS CloudTrail를 참조하세요.
- Amazon은 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에 자동으로 대응하여 AWS 서비스를 EventBridge 더욱 자동화합니다. AWS서비스의 이벤트는 거의 EventBridge 실시간으로 전송됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하십시오.

로깅AWS을 사용하여 계정 관리 API 호출AWS CloudTrail

이AWS계정 관리 API는 다음과 통합됩니다.AWS CloudTrail, 사용자, 역할 또는 해당 사용자가 수행한 작업의 기록을 제공하는 서비스AWS계정 관리 작업을 호출하는 서비스입니다. CloudTrail은 모든 계정 관리 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 계정 관리 작업에 대한 모든 호출이 포함됩니다. 추적을 생성하면 계정 관리 작업을 위한 이벤트를 비롯하여 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 배포하도록 설정할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록(Event history)에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 계정 관리 작업을 호출한 사람 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 계정 관리 정보

CloudTrail 켜져 있습니다.AWS 계정계정을 생성할 때입니다. 계정 관리 작업에서 활동이 발생하면 CloudTrail은 해당 활동을 다른 사용자와 함께 CloudTrail 이벤트 로그에 기록합니다.AWS의 서비스 이벤트이벤트 기록. 에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다.AWS 계정. 자세한 정보는 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

에 이벤트를 지속적으로 기록하려면AWS 계정은 계정 관리 작업을 위한 이벤트를 비롯하여 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 추적을 생성할 때AWS Management Console트레일은 모두에게 적용됩니다.AWS 리전. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. CloudTrail 로그에 수집된 이벤트 데이터를 좀 더 분석하고 작업하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

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

AWS CloudTrail에 있는 모든 계정 관리 API 작업을 기록합니다.API 참조이 설명서의 단원을 참조하십시오. 예를 들어, `CreateAccount`, `DeleteAlternateContact` 및 `PutAlternateContact` 작업에 대한 호출은 CloudTrail 로그 파일의 항목을 생성합니다.

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

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

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

계정 관리 로그 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

예제 1: 다음은 호출에 대한 CloudTrail 로그 항목을 보여주는 예입니다.`GetAlternateContact`현재 검색 작업`OPERATIONS`계정에 대한 대체 연락처 작업에 의해 반환되는 값은 기록된 정보에 포함되지 않습니다.

Example 예 1


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

예제 2: 다음은 호출에 대한 CloudTrail 로그 항목을 보여주는 예입니다.PutAlternateContact새 작업을 추가하려면BILLING계정에 대한 대체 연락처


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
```

```
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

예제 3: 다음은 호출에 대한 CloudTrail 로그 항목을 보여주는 예입니다.DeleteAlternateContact현재를 삭제하는 작업OPERATIONS대체 연락처.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
```

```
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

를 사용하여 계정 관리 이벤트 모니터링 EventBridge

Amazon은 EventBridge 이전에 CloudWatch Events라고 불렸으며 특정 이벤트를 모니터링하고 다른 이벤트를 사용하는 대상 작업을 시작할 수 있도록 도와줍니다. AWS 서비스 의 AWS 서비스 이벤트가 거의 EventBridge 실시간으로 전송됩니다.

를 사용하여 EventBridge 수신 이벤트와 일치하는 규칙을 만들고 이를 처리 대상으로 라우팅할 수 있습니다.

자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 시작하기를 참조하십시오.

계정 관리 이벤트

다음 예는 계정 관리 이벤트를 보여줍니다. 이벤트는 최선의 작업을 기반으로 생성됩니다.

현재 계정 관리에는 지역 및 API 호출을 활성화 및 비활성화하는 것과 관련된 이벤트만 사용할 수 있습니다. CloudTrail

이벤트 유형

- 지역 활성화 및 비활성화 이벤트

지역 활성화 및 비활성화 이벤트

콘솔 또는 API에서 계정의 지역을 활성화하거나 비활성화하면 비동기 작업이 시작됩니다. 초기 요청은 대상 계정에 CloudTrail 이벤트로 기록됩니다. 또한 활성화 또는 비활성화 프로세스가 시작되면 EventBridge 이벤트가 통화 계정으로 전송되고, 두 프로세스가 모두 완료되면 다시 이벤트가 통화 계정으로 전송됩니다.

다음 예제 이벤트는 on이 `ap-east-1` Region `2020-09-30` `ENABLED` for account임을 나타내는 요청이 전송되는 방식을 보여줍니다`123456789012`.

```
{
```

```
   "version":"0",
   "id":"11112222-3333-4444-5555-666677778888",
   "detail-type":"Region Opt-In Status Change",
   "source":"aws.account",
   "account":"123456789012",
   "time":"2020-09-30T06:51:08Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:account::123456789012:account"
   ],
   "detail":{
      "accountId":"123456789012",
      "regionName":"ap-east-1",
      "status":"ENABLED"
   }
}
```

GetRegionOptStatus및 ListRegions API에서 반환된 상태와 일치하는 네 가지 상태가 있을 수 있습니다.

- ENABLED— 지정된 지역에 대해 지역이 성공적으로 활성화되었습니다. accountId
- ENABLING— accountId 지정된 지역에 대해 지역을 활성화하는 중입니다.
- DISABLED— accountId 지정된 지역에 대해 지역이 성공적으로 비활성화되었습니다.
- DISABLING— 해당 지역은 accountId 지정된 기간 동안 비활성화되는 중입니다.

다음 샘플 이벤트 패턴은 모든 지역 이벤트를 캡처하는 규칙을 생성합니다.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ]
}
```

다음 샘플 이벤트 패턴은 DISABLED 지역 이벤트만 ENABLED 캡처하는 규칙을 만듭니다.

```
{
   "source":[
```

```
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ],
   "detail":{
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

API 참조

계정 관리에서의 API 작업 (account) 네임스페이스를 사용하면 다음을 수정할 수 있습니다.AWS 계정.

모든AWS 계정계정과 연결된 최대 세 개의 대체 연락처에 대한 정보를 포함하여 계정에 대한 정보가 포함된 메타데이터를 지원합니다. 여기에는 연결된 이메일 주소에 추가됩니다.루트 사용자계좌의. 계정과 연결된 다음 연락처 유형 중 하나만 지정할 수 있습니다.

- 청구 연락처
- 운영 연락처
- 보안 연락처

기본적으로 이 가이드에서 설명하는 API 작업은 작업을 호출하는 계정에 직접 적용됩니다. 더신원을 확인합니다작업을 호출하는 계정에는 일반적으로 IAM 역할 또는 IAM 사용자이며 API 작업을 호출하려면 IAM 정책에 의해 적용된 권한이 있어야 합니다. 또는 의 ID에서 이러한 API 작업을 호출할 수 있습니다.AWS Organizations관리 계정 및 모든 계정 ID 번호 지정AWS 계정그 사람은 조직의 일원입니다.

API 버전

이 버전의 계정 API 레퍼런스는 계정 관리 API 버전 2021-02-01을 문서화합니다.

> **Note**
>
> API를 직접 사용하는 대신 다음 중 하나를 사용할 수 있습니다.AWSSDK는 다양한 프로그래밍 언어 및 플랫폼 (Java, Ruby, .NET, iOS, Android 등) 을 위한 라이브러리와 샘플 코드로 구성됩니다. SDK는 프로그래밍 방식으로 액세스할 수 있는 편리한 방법을 제공합니다.AWS조직. 예를 들어 SDK는 요청에 암호화 방식으로 서명하고, 오류를 관리하고, 요청을 자동으로 재시도합니다. AWS SDK 다운로드 및 설치 방법을 비롯한 자세한 내용은 Amazon Web Services용 도구를 참조하세요.

를 사용하는 것이 좋습니다.AWS계정 관리 서비스에 프로그래밍 방식의 API 호출을 하기 위한 SDK 하지만 계정 관리 쿼리 API를 사용하여 계정 관리 웹 서비스를 직접 호출할 수도 있습니다. 계정 관리 쿼리 API에 대한 자세한 내용은 을 참조하십시오.HTTP 쿼리 요청을 통한 API 호출계정 관리 사용 설명서에서 조직에서는 모든 작업에 대해 GET 및 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. 따라서 더 큰 크기가 필요한 작업의 경우 POST 요청을 사용하십시오.

요청에 서명하기

HTTP 요청을 다음 주소로 보내는 경우AWS, 다음과 같이 요청서에 서명해야 합니다.AWS누가 보냈는지 확인할 수 있습니다. 귀하는 귀하의 요청에 서명합니다AWS액세스 키는 액세스 키 ID와 보안 액세스 키로 구성됩니다. 루트 계정에는 액세스 키를 만들지 않는 것이 좋습니다. 루트 계정의 액세스 키가 있는 사람은 누구나 계정 내 모든 리소스에 제한 없이 액세스할 수 있습니다. 대신 관리자 권한이 있는 IAM 사용자를 위한 액세스 키를 생성하십시오. 다른 옵션으로 다음을 사용하십시오.AWS보안 토큰 서비스는 임시 보안 자격 증명을 생성하고 해당 자격 증명을 사용하여 요청에 서명합니다.

요청에 서명하려면 서명 버전 4를 사용하는 것이 좋습니다. 서명 버전 2를 사용하는 기존 애플리케이션이 있는 경우 서명 버전 4를 사용하도록 업데이트하지 않아도 됩니다. 그러나 일부 작업에는 이제 서명 버전 4가 필요합니다. 버전 4가 필요한 작업에 대한 설명서에는 이 요구 사항이 나와 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS API 요청에 서명을 참조하세요.

사용할 때AWS명령줄 인터페이스 (AWSCLI) 또는 다음 중 하나AWS요청을 보낼 SDKAWS, 이러한 도구는 도구를 구성할 때 지정한 액세스 키를 사용하여 요청에 자동으로 서명합니다.

계정 관리에 대한 지원 및 피드백

우리는 여러분의 의견을 환영합니다. 다음 주소로 의견 보내기feedback-awsaccounts@amazon.com또는 다음 주소로 피드백 및 질문을 게시하십시오.계정 관리 지원 포럼. AWS 지원 포럼에 대한 자세한 내용은 포럼 도움말을 참조하십시오.

예제 제시 방법

계정 관리에서 요청에 대한 응답으로 반환한 JSON은 줄 바꿈이나 공백 형식 지정 없이 하나의 긴 문자열로 반환됩니다. 이 안내서의 예에는 가독성을 높이기 위해 줄 바꿈과 공백이 모두 표시되어 있습니다. 예제 입력 매개 변수로 인해 화면 밖으로 확장되는 긴 문자열이 생성되는 경우 가독성을 높이기 위해 줄 바꿈을 삽입합니다. 입력은 항상 단일 JSON 텍스트 문자열로 제출해야 합니다.

API 요청 기록

계정 관리 지원CloudTrail, 기록하는 서비스AWS사용자를 위한 API 호출AWS 계정로그 파일을 Amazon S3 버킷으로 전송합니다. 에서 수집한 정보를 사용하여CloudTrail에서 Account Management에 어떤 요청이 성공적으로 이루어졌는지, 누가 요청했는지, 언제 요청했는지 등을 확인할 수 있습니다. 계정 관리 및 지원에 대한 자세한 내용은CloudTrail, 참조로깅AWS을 사용하여 계정 관리 API 호출 AWS CloudTrail. 에 대해 자세히 알아보려면CloudTrail이 기능을 켜고 로그 파일을 찾는 방법을 포함하여 다음을 참조하십시오.AWS CloudTrail사용자 가이드.

작업

다음 작업이 지원됩니다.

- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAlternateContact
- GetContactInformation
- GetRegionOptStatus
- ListRegions
- PutAlternateContact
- PutContactInformation

DeleteAlternateContact

에서 지정된 대체 연락처를 삭제합니다. AWS 계정

대체 연락처 작업을 사용하는 방법에 대한 자세한 내용은 대체 연락처 액세스 또는 업데이트를 참조하십시오.

> **Note**
>
> 에서 관리하는 담당자의 대체 연락처 정보를 업데이트하려면 먼저 AWS 계정 AWS Account Management와 Organizations 간의 통합을 활성화해야 합니다. AWS Organizations 자세한 내용은 AWS계정 관리를 위한 신뢰할 수 있는 액세스 활성화를 참조하십시오.

요청 구문

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식의 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 수정하려는 AWS 계정의 12자리 계정 ID 번호를 지정합니다.

이 매개 변수를 지정하지 않으면 작업 호출에 사용된 ID의 AWS 계정이 기본값으로 사용됩니다.

이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 하고, 지정된 계정 ID는 동일한 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어

있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 고유한 계정을 지정할 수 없습니다`AccountId`. 관리 계정은 매개 변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다. `AccountId`

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 말고 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 작업을 호출하십시오.

유형: String

패턴: `^\d{12}$`

필수 여부: 아니요

AlternateContactType

삭제할 대체 연락처를 지정합니다.

유형: String

유효한 값: `BILLING | OPERATIONS | SECURITY`

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

응답 요소

작업이 성공하면 서비스가 비어있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

내부 오류로 인해 작업이 실패했습니다AWS. 나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스를 지정했기 때문에 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

작업이 너무 자주 호출되고 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

예제

예 1

다음 예에서는 작업을 호출하는 데 사용되는 자격 증명을 가진 계정의 보안 대체 연락처를 삭제합니다.

예제 요청

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AlternateContactType": "SECURITY" }
```

샘플 응답

```
HTTP/1.1 200 OK
```

```
Content-Type: application/json
```

예 2

다음 예제에서는 조직의 지정된 구성원 계정에 대한 청구 대체 연락처를 삭제합니다. 조직의 관리 계정 또는 계정 관리 서비스의 위임된 관리자 계정의 자격 증명을 사용해야 합니다.

예제 요청

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "BILLING" }
```

샘플 응답

```
HTTP/1.1 200 OK
Content-Type: application/json
```

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요:

- AWS 명령줄 인터페이스
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWSV3용 SDK JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisableRegion

계정의 특정 지역을 비활성화 (옵트아웃) 합니다.

> **Note**
>
> 지역을 비활성화하면 해당 지역에 있는 모든 리소스에 대한 모든 IAM 액세스 권한이 제거됩니다.

Request Syntax

```
POST /disableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 AWS 계정 수정하려는 12자리 계정 ID 번호를 지정합니다. 이 매개 변수를 지정하지 않으면 작업을 호출하는 데 사용되는 ID가 기본값으로 사용됩니다. AWS 계정 이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 합니다. 또한 지정된 계정 ID는 같은 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId` 계정을 지정할 수 없습니다. `AccountId`매개변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다.

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 마세요. 대신 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 오퍼레이션을 호출하세요.

유형: String

패턴: `^\d{12}$`

필수 여부: 아니요

RegionName

지정된 지역 이름 (예:) 의 지역 코드를 지정합니다. `af-south-1` 지역을 비활성화하면 계정에서 해당 지역을 비활성화하는 작업 (예: 지역의 IAM 리소스 삭제) 을 AWS 수행합니다. 이 프로세스는 대부분의 계정에서 몇 분이 걸리지만 몇 시간이 걸릴 수도 있습니다. 비활성화 프로세스가 완전히 완료될 때까지는 지역을 활성화할 수 없습니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50입니다.

필수 항목 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 반송합니다.

Errors

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

ConflictException

리소스의 현재 상태가 충돌하여 요청을 처리할 수 없습니다. 예를 들어, 현재 비활성화되어 있는 (DISABLING 상태인) 지역을 활성화하려고 하면 이런 상황이 발생합니다.

HTTP Status Code: 409

InternalServerException

내부 오류로 인해 작업이 실패했습니다. AWS나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

TooManyRequestsException

너무 자주 호출되어 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP Status Code: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDK 중 하나에서 이 API를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS Java V2용 SDK
- AWS V3용 SDK JavaScript
- AWS PHP V3용 SDK

- AWS Python용 SDK
- AWS 루비 V3용 SDK

EnableRegion

계정에 대해 특정 지역을 활성화 (옵트인) 합니다.

요청 구문

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식의 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 AWS 계정 수정하려는 12자리 계정 ID 번호를 지정합니다. 이 매개 변수를 지정하지 않으면 작업을 호출하는 데 사용되는 ID가 기본값으로 사용됩니다. AWS 계정 이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 합니다. 또한 지정된 계정 ID는 같은 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 자체 AccountId 계정을 지정할 수 없습니다. AccountId매개변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다.

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 마세요. 대신 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 오퍼레이션을 호출하세요.

유형: String

패턴: ^\d{12}$

필수 여부: 아니요

RegionName

지정된 지역 이름 (예:) 의 지역 코드를 지정합니다. af-south-1 리전을 활성화하면 AWS에서 해당 리전의 계정을 준비하는 작업(예: IAM 리소스를 해당 리전으로 배포)을 수행합니다. 이 프로세스는 대부분의 계정에서 몇 분 정도 걸리지만 몇 시간이 걸릴 수 있습니다. 이 프로세스가 완료될 때까지는 해당 리전을 사용할 수 없습니다. 또한 활성화 프로세스가 완전히 완료될 때까지는 지역을 비활성화할 수 없습니다.

유형: String

길이 제약: 최소 길이 1. 최대 길이 50.

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

응답 요소

작업이 성공하면 서비스가 비어있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

ConflictException

리소스의 현재 상태가 충돌하여 요청을 처리할 수 없습니다. 예를 들어, 현재 비활성화되어 있는 (DISABLING 상태인) 지역을 활성화하려고 하면 이런 상황이 발생합니다.

HTTP 상태 코드: 409

InternalServerException

내부 오류로 인해 작업이 실패했습니다. AWS 나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

TooManyRequestsException

너무 자주 호출되어 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요:

- AWS 명령줄 인터페이스
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWSV3용 JavaScript SDK
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAlternateContact

에 첨부된 지정된 대체 연락처를 검색합니다. AWS 계정

대체 연락처 작업을 사용하는 방법에 대한 자세한 내용은 대체 연락처 액세스 또는 업데이트를 참조하십시오.

> **Note**
>
> 에서 관리하는 담당자의 대체 연락처 정보를 업데이트하려면 먼저 AWS 계정 AWS Account Management와 Organizations 간의 통합을 활성화해야 합니다. AWS Organizations 자세한 내용은 AWS계정 관리를 위한 신뢰할 수 있는 액세스 활성화를 참조하십시오.

요청 구문

```
POST /getAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식의 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 수정하려는 AWS 계정의 12자리 계정 ID 번호를 지정합니다.

이 매개 변수를 지정하지 않으면 작업 호출에 사용된 ID의 AWS 계정이 기본값으로 사용됩니다.

이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 하고, 지정된 계정 ID는 동일한 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어

있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 고유한 계정을 지정할 수 없습니다`AccountId`. 관리 계정은 매개 변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다. `AccountId`

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 말고 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 작업을 호출하십시오.

유형: String

패턴: `^\d{12}$`

필수 여부: 아니요

AlternateContactType

검색하려는 대체 연락처를 지정합니다.

유형: String

유효한 값: `BILLING | OPERATIONS | SECURITY`

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "AlternateContact": {
      "AlternateContactType": "string",
      "EmailAddress": "string",
      "Name": "string",
      "PhoneNumber": "string",
      "Title": "string"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AlternateContact

지정된 대체 연락처에 대한 세부 정보가 포함된 구조입니다.

유형: AlternateContact 객체

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

내부 오류 때문에 작업이 실패했습니다AWS. 나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스를 지정했기 때문에 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

작업이 너무 자주 호출되고 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

예제

예 1

다음 예에서는 작업을 호출하는 데 사용되는 자격 증명을 가진 계정의 보안 대체 연락처를 검색합니다.

예제 요청

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AlternateContactType": "SECURITY" }
```

샘플 응답

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Security"
    }
}
```

예 2

다음 예에서는 조직의 지정된 구성원 계정에 대한 작업 대체 연락처를 검색합니다. 조직의 관리 계정 또는 계정 관리 서비스의 위임된 관리자 계정의 자격 증명을 사용해야 합니다.

예제 요청

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "Operations" }
```

샘플 응답

```
HTTP/1.1 200 OK
```

```
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Operations"
    }
}
```

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요:

- AWS 명령줄 인터페이스
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWSV3용 SDK JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetContactInformation

의 기본 연락처 정보를 검색합니다. AWS 계정

기본 연락처 작업을 사용하는 방법에 대한 자세한 내용은 기본 및 대체 연락처 정보 업데이트를 참조하십시오.

요청 구문

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식의 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 AWS 계정 수정하려는 12자리 계정 ID 번호를 지정합니다. 이 매개변수를 지정하지 않으면 작업 호출에 AWS 계정 사용되는 ID가 기본값으로 사용됩니다. 이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 합니다. 또한 지정된 계정 ID는 같은 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 자체 AccountId 계정을 지정할 수 없습니다. AccountId매개변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다.

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 마세요. 대신 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 오퍼레이션을 호출하세요.

유형: String

패턴: ^\d{12}$

필수 여부: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ContactInformation

와 관련된 기본 연락처 정보의 세부 정보가 들어 AWS 계정 있습니다.

유형: ContactInformation 객체

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

내부 오류 때문에 작업이 실패했습니다AWS. 나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스를 지정했기 때문에 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

작업이 너무 자주 호출되고 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요:

- AWS 명령줄 인터페이스
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWSV3용 JavaScript SDK
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRegionOptStatus

특정 지역의 옵트인 상태를 검색합니다.

요청 구문

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식의 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 AWS 계정 수정하려는 12자리 계정 ID 번호를 지정합니다. 이 매개 변수를 지정하지 않으면 작업을 호출하는 데 사용되는 ID가 기본값으로 사용됩니다. AWS 계정 이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 합니다. 또한 지정된 계정 ID는 같은 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId` 계정을 지정할 수 없습니다. `AccountId`매개변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다.

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 마세요. 대신 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 오퍼레이션을 호출하세요.

유형: String

패턴: ^\d{12}$

필수 여부: 아니요

RegionName

지정된 지역 이름 (예:) 의 지역 코드를 지정합니다. af-south-1 이 함수는 이 매개변수에 전달한 모든 지역의 상태를 반환합니다.

유형: String

길이 제약: 최소 길이 1. 최대 길이 50.

필수 여부: 예

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "RegionName": "string",
   "RegionOptStatus": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

RegionName

전달된 지역 코드입니다.

유형: String

길이 제약: 최소 길이 1. 최대 길이 50.

RegionOptStatus

지역이 겪을 수 있는 잠재적 상태 중 하나입니다 (활성화, 활성화, 비활성화, 비활성화, Enabled_By_Default).

유형: String

유효한 값: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

내부 오류로 인해 작업이 실패했습니다AWS. 나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

TooManyRequestsException

너무 자주 호출되어 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요:

- AWS 명령줄 인터페이스
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWSV3용 JavaScript SDK

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRegions

해당 계정의 모든 지역과 해당 지역의 옵트인 상태를 나열합니다. 선택적으로 이 목록을 매개변수로 필터링할 수 있습니다. `region-opt-status-contains`

요청 구문

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "MaxResults": number,
   "NextToken": "string",
   "RegionOptStatusContains": [ "string" ]
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식의 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 AWS 계정 수정하려는 12자리 계정 ID 번호를 지정합니다. 이 매개변수를 지정하지 않으면 작업을 호출하는 데 사용되는 ID가 기본값으로 사용됩니다. AWS 계정 이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 합니다. 또한 지정된 계정 ID는 같은 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId` 계정을 지정할 수 없습니다. `AccountId`매개변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다.

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 마세요. 대신 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 오퍼레이션을 호출하세요.

유형: String

패턴: `^\d{12}$`

필수 여부: 아니요

MaxResults

명령 출력에서 반환할 총 항목 수입니다. 사용 가능한 총 항목 수가 지정된 값보다 많으면 명령 출력에 `NextToken` a가 제공됩니다. 페이지 매김을 재개하려면 후속 명령의 `starting-token` 인수에 `NextToken` 값을 제공합니다. AWSCLI 외부에서 직접 `NextToken` 응답 요소를 사용하지 마십시오. 사용 예는 AWS명령줄 인터페이스 사용 설명서의 페이지 매김을 참조하십시오.

유형: 정수

유효한 범위: 최소값 1. 최대값 50.

필수 여부: 아니요

NextToken

페이지 매김을 시작할 위치를 지정하는 데 사용되는 토큰입니다. 이전에 잘린 `NextToken` 응답에서 가져온 것입니다. 사용 예는 AWS명령줄 인터페이스 사용 설명서의 페이지 매김을 참조하십시오.

유형: String

길이 제약: 최소 길이 0. 최대 길이는 1,000입니다.

필수 여부: 아니요

RegionOptStatusContains

특정 계정의 지역 목록을 필터링하는 데 사용할 지역 상태 목록 (활성화, 활성화, 비활성화, 비활성화, Enabled_BY_Default). 예를 들어 ENABLING 값을 전달하면 지역 상태가 ENABLEING인 지역 목록만 반환됩니다.

유형: 문자열 배열

유효한 값: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

필수 여부: 아니요

응답 구문

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Regions": [
      {
         "RegionName": "string",
         "RegionOptStatus": "string"
      }
   ]
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환할 데이터가 더 있는 경우 해당 데이터가 채워집니다. 의 `next-token` `list-regions` 요청 매개변수로 전달되어야 합니다.

유형: String

Regions

이 목록은 해당 계정의 지역 목록이며, 필터링된 매개변수가 사용된 경우 `filter` 매개변수에 설정된 필터 기준과 일치하는 지역 목록입니다.

유형: Region 객체 배열

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

내부 오류로 인해 작업이 실패했습니다AWS. 나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

TooManyRequestsException

너무 자주 호출되어 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요:

- AWS 명령줄 인터페이스
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWSV3용 JavaScript SDK
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutAlternateContact

에 첨부된 지정된 대체 연락처를 수정합니다. AWS 계정

대체 연락처 작업을 사용하는 방법에 대한 자세한 내용은 대체 연락처 액세스 또는 업데이트를 참조하십시오.

> **Note**
>
> 에서 관리하는 담당자의 대체 연락처 정보를 업데이트하려면 먼저 AWS 계정 AWS Account Management와 Organizations 간의 통합을 활성화해야 합니다. AWS Organizations 자세한 내용은 AWS계정 관리를 위한 신뢰할 수 있는 액세스 활성화를 참조하십시오.

요청 구문

```
POST /putAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string",
   "EmailAddress": "string",
   "Name": "string",
   "PhoneNumber": "string",
   "Title": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식의 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 수정하려는 AWS 계정의 12자리 계정 ID 번호를 지정합니다.

이 매개 변수를 지정하지 않으면 작업 호출에 사용된 ID의 AWS 계정이 기본값으로 사용됩니다.

이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 하고, 지정된 계정 ID는 동일한 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 고유한 계정을 지정할 수 없습니다`AccountId`. 관리 계정은 매개 변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다. `AccountId`

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 말고 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 작업을 호출하십시오.

유형: String

패턴: `^\d{12}$`

필수 여부: 아니요

AlternateContactType

만들거나 업데이트하려는 대체 연락처를 지정합니다.

유형: String

유효한 값: `BILLING | OPERATIONS | SECURITY`

필수 여부: 예

EmailAddress

대체 연락처의 이메일 주소를 지정합니다.

유형: String

길이 제약: 최소 길이 1. 최대 길이는 64입니다.

패턴: `^[\s]*[\w+=.#!&-]+@[\w.-]+\.[\w]+[\s]*$`

필수 항목 여부: 예

Name

대체 연락처의 이름을 지정합니다.

유형: String

길이 제약: 최소 길이 1. 최대 길이는 64입니다.

필수 여부: 예

PhoneNumber

대체 연락처의 전화 번호를 지정합니다.

유형: String

길이 제약: 최소 길이 1. 최대 길이는 25입니다.

패턴: ^[\s0-9()+-]+$

필수 항목 여부: 예

Title

대체 연락처의 제목을 지정합니다.

유형: String

길이 제약: 최소 길이 1. 최대 길이 50.

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

응답 요소

작업이 성공하면 서비스가 비어있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

내부 오류로 인해 작업이 실패했습니다AWS. 나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

TooManyRequestsException

너무 자주 호출되어 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

예제

예 1

다음 예에서는 작업을 호출하는 데 사용되는 자격 증명을 가진 계정의 결제 대체 연락처를 설정합니다.

예제 요청

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

샘플 응답

```
HTTP/1.1 200 OK
Content-Type: application/json
```

예 2

다음 예에서는 조직의 지정된 구성원 계정에 대해 청구 대체 연락처를 설정하거나 덮어씁니다. 조직의 관리 계정 또는 계정 관리 서비스의 위임된 관리자 계정의 자격 증명을 사용해야 합니다.

예제 요청

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AccountId": "123456789012",
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

샘플 응답

```
HTTP/1.1 200 OK
Content-Type: application/json
```

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요:

- AWS 명령줄 인터페이스
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWSV3용 SDK JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutContactInformation

의 기본 연락처 정보를 AWS 계정 업데이트합니다.

기본 연락처 작업을 사용하는 방법에 대한 자세한 내용은 기본 및 대체 연락처 정보 업데이트를 참조하십시오.

요청 구문

```
POST /putContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식의 다음 데이터를 받습니다.

AccountId

이 작업을 통해 액세스하거나 AWS 계정 수정하려는 12자리 계정 ID 번호를 지정합니다. 이 매개 변수를 지정하지 않으면 작업 호출에 AWS 계정 사용되는 ID가 기본값으로 사용됩니다. 이 매개 변수를 사용하려면 호출자가 조직의 관리 계정에 있는 ID 또는 위임된 관리자 계정이어야 합니다. 또

한 지정된 계정 ID는 같은 조직의 구성원 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하고, 조직에 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정을 할당해야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId` 계정을 지정할 수 없습니다. `AccountId`매개변수를 포함하지 않고 독립형 컨텍스트에서 작업을 호출해야 합니다.

조직의 구성원이 아닌 계정에서 이 작업을 호출하려면 이 매개 변수를 지정하지 마세요. 대신 연락처를 검색하거나 수정하려는 계정의 ID를 사용하여 오퍼레이션을 호출하세요.

유형: String

패턴: `^\d{12}$`

필수 여부: 아니요

ContactInformation

와 관련된 기본 연락처 정보의 세부 정보가 들어 AWS 계정 있습니다.

유형: ContactInformation 객체

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

응답 요소

작업이 성공하면 서비스가 비어있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에서 공통적으로 발생하는 오류에 대한 자세한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

발신 ID에 필요한 최소 권한이 없어서 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

내부 오류 때문에 작업이 실패했습니다AWS. 나중에 작업을 다시 시도하세요.

HTTP 상태 코드: 500

TooManyRequestsException

너무 자주 호출되어 스로틀 한도를 초과하여 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 매개 변수 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요:

- AWS 명령줄 인터페이스
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWSV3용 JavaScript SDK
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

기타 관련 작업AWS서비스

다음은 와 관련된 작업입니다.AWS Account Management하지만 의 일부입니다.AWS Organizations네임스페이스:

- CreateAccount

- 크레아티고브클라우드계정
- DescribeAccount

CreateAccount

이CreateAccountAPI 작업은 에 의해 관리되는 조직의 컨텍스트에서만 사용할 수 있습니다.AWS Organizations서비스. API 작업은 해당 서비스의 네임스페이스에 정의됩니다.

자세한 내용은 단원을 참조하십시오.CreateAccount의AWS OrganizationsAPI 참조.

크레아티고브클라우드계정

이CreateGovCloudAccountAPI 작업은 에서 관리하는 조직의 컨텍스트에서만 사용할 수 있습니다.AWS Organizations서비스. API 작업은 해당 서비스의 네임스페이스에 정의됩니다.

자세한 내용은 단원을 참조하십시오.크레아티고브클라우드계정의AWS OrganizationsAPI 참조.

DescribeAccount

이DescribeAccountAPI 작업은 에 의해 관리되는 조직의 컨텍스트에서만 사용할 수 있습니다.AWS Organizations서비스. API 작업은 해당 서비스의 네임스페이스에 정의됩니다.

자세한 내용은 단원을 참조하십시오.DescribeAccount의AWS OrganizationsAPI 참조.

데이터 유형

다음 데이터 유형이 지원됩니다.

- AlternateContact
- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

계정과 연결된 대체 연락처의 세부 정보가 포함된 구조입니다AWS.

목차

AlternateContactType

대체 연락처 유형.

유형: String

유효한 값: `BILLING | OPERATIONS | SECURITY`

필수 항목 여부: 아니요

EmailAddress

이 대체 연락처와 연결된 이메일 주소입니다.

유형: String

길이 제약: 최소 길이는 1입니다. 최대 길이는 64입니다.

패턴: `^[\s]*[\w+=.#!&-]+@[\w.-]+\.[\w]+[\s]*$`

필수 항목 여부: 아니요

Name

이 대체 연락처와 관련된 이름.

유형: String

길이 제약: 최소 길이는 1입니다. 최대 길이는 64입니다.

필수 항목 여부: 아니요

PhoneNumber

이 대체 연락처와 연결된 전화번호입니다.

유형: String

길이 제약: 최소 길이는 1입니다. 최대 길이 25입니다.

패턴: ^[\s0-9()+-]+$

필수 항목 여부: 아니요

Title

이 대체 연락처와 관련된 제목입니다.

유형: String

길이 제약: 최소 길이는 1입니다. 최대 길이 50.

필수 항목 여부: 아니요

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요.

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ContactInformation

와 관련된 기본 연락처 정보의 세부 정보가 들어 AWS 계정 있습니다.

내용

AddressLine1

기본 연락처 주소의 첫 번째 줄.

유형: 문자열

길이 제약: 최소 길이 1자. 최대 길이는 60개입니다.

필수 항목 여부: 예

City

기본 연락처 주소의 도시.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 예

CountryCode

기본 연락처 주소의 ISO-3166 2자리 국가 코드입니다.

유형: 문자열

길이 제약: 고정 길이 2.

필수 항목 여부: 예

FullName

기본 연락처 주소의 전체 이름.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 예

PhoneNumber

기본 연락처 정보의 전화번호. 번호가 확인되고 일부 국가에서는 활성화 여부를 확인합니다.

유형: 문자열

길이 제약: 최소 길이 1자. 최대 길이 20자.

패턴: ^[+][\s0-9()-]+$

필수 항목 여부: 예

PostalCode

기본 연락처 주소의 우편번호.

유형: 문자열

길이 제약: 최소 길이 1자. 최대 길이는 20입니다.

필수 항목 여부: 예

AddressLine2

기본 연락처 주소의 두 번째 줄 (있는 경우).

유형: 문자열

길이 제약: 최소 길이 1자. 최대 길이는 60입니다.

필수 항목 여부: 아니요

AddressLine3

기본 연락처 주소의 세 번째 줄 (있는 경우).

유형: 문자열

길이 제약: 최소 길이 1자. 최대 길이는 60개입니다.

필수 항목 여부: 아니요

CompanyName

기본 연락처 정보와 관련된 회사 이름 (있는 경우).

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 아니요

DistrictOrCounty

주 연락처 주소의 지역 또는 카운티 (있는 경우).

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 아니요

StateOrRegion

기본 연락처 주소의 주 또는 지역. 우편 주소가 미국 내에 있는 경우 이 필드의 값은 2자리 주 코드 (예:NJ) 또는 전체 주 이름 (예:) 일 수 있습니다. `New Jersey` 이 필드는 다음 국가에서 필수입니다:US, CAGB,DE, JPIN, 및BR.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 아니요

WebsiteUrl

기본 연락처 정보와 관련된 웹 사이트의 URL (있는 경우).

유형: 문자열

길이 제약: 최소 길이 1자. 최대 길이 256자.

필수 항목 여부: 아니요

참고

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요.

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWS SDK for Ruby V3

Region

이는 이름과 옵트인 상태로 구성된 지정된 계정의 지역을 나타내는 구조입니다.

내용

RegionName

특정 지역의 지역 코드 (예:). `us-east-1`

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 아니요

RegionOptStatus

지역이 겪을 수 있는 잠재적 상태 중 하나입니다 (활성화, 활성화, 비활성화, 비활성화, Enabled_By_Default).

타입: 문자열

유효 값: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

필수 여부: 아니요

참고

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 설명은 다음을 참조하세요.

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ValidationExceptionField

입력이 지정된 필드에서AWS 서비스에서 지정한 제약 조건을 충족하지 못했습니다.

목차

message

유효성 검사 예외에 대한 메시지입니다.

유형: String

필수 항목 여부: 예

name

잘못된 항목이 감지된 필드 이름입니다.

유형: String

필수 항목 여부: 예

참고 항목

이 API를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요.

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

공통 파라미터

다음 목록에는 모든 작업이 쿼리 문자열을 사용하여 Signature Version 4 요청에 서명하는 데 사용하는 파라미터가 포함되어 있습니다. 작업별 파라미터는 그 작업에 대한 항목에 나열되어 있습니다. 서명 버전 4에 대한 자세한 내용은 IAM 사용 설명서의AWS API 요청 서명을 참조하십시오.

Action

수행할 작업입니다.

유형: 문자열

필수 항목 여부: 예

Version

요청이 작성되는 API 버전으로 YYYY-MM-DD 형식으로 표시됩니다.

유형: 문자열

필수 항목 여부: 예

X-Amz-Algorithm

요청 서명을 생성하는 데 사용된 해시 알고리즘입니다.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

유효한 값: `AWS4-HMAC-SHA256`

필수 항목 여부: 조건부

X-Amz-Credential

자격 증명 범위 값이며 액세스 키, 날짜, 대상으로 하는 리전, 요청하는 서비스 및 종료 문자열("aws4_request")이 포함된 문자열입니다. 값은 다음 형식으로 표시됩니다. access_key/YYYYMMDD/region/service/aws4_request.

자세한 내용은 IAM 사용 설명서의 서명된AWS API 요청 생성을 참조하십시오.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Date

서명을 만드는 데 사용되는 날짜입니다. 형식은 ISO 8601 기본 형식(YYYYMMDD'T'HHMMSS'Z') 이어야 합니다. 예를 들어 다음 날짜 시간은 유효한 X-Amz-Date 값: `20120325T120000Z`.

조건: X-Amz-Date는 모든 요청에서 옵션이지만 서명 요청에 사용되는 날짜보다 우선할 때 사용됩니다. 날짜 헤더가 ISO 8601 기본 형식으로 지정된 경우 X-Amz-Date가 필요하지 않습니다. X-Amz-Date를 사용하는 경우 항상 Date 헤더의 값을 재정의합니다. 자세한 내용은 IAM 사용 설명서의AWS API 요청 서명 요소를 참조하십시오.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Security-Token

toAWS Security Token Service (AWS STS) 에 대한 호출을 통해 받은 임시 보안 토큰입니다. 의 임시 보안 인증 정보를 지원하는 서비스 목록은 IAM 사용 설명서 의 IAM와 함께AWS 서비스 작동하는 서비스 에서 확인할 수 있습니다.AWS STS

조건: 의 임시 보안 인증 정보를 사용하는 경우AWS STS, 보안 토큰을 포함해야 합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Signature

서명할 문자열과 파생된 서명 키에서 계산된 16진수로 인코딩된 서명을 지정합니다.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-SignedHeaders

표준 요청의 일부로 포함된 모든 HTTP 헤더를 지정합니다. 서명된 헤더 지정에 대한 자세한 내용은 IAM 사용 설명서의 서명된AWS API 요청 생성을 참조하십시오.

조건: HTTP 권한 부여 헤더 대신 쿼리 문자열에 인증 정보를 포함하는 경우 이 파라미터를 지정합니다.

유형: 문자열

필수 항목 여부: 조건부

일반적인 오류

이 단원에는 모든 AWS 서비스의 API 작업에 대한 일반 오류가 나와 있습니다. 이 서비스의 API 작업에 대한 오류는 해당 API 작업 항목을 참조하십시오.

AccessDeniedException

이 작업을 수행할 수 있는 충분한 액세스 권한이 없습니다.

HTTP 상태 코드: 400

IncompleteSignature

요청 서명이 AWS 표준을 준수하지 않습니다.

HTTP 상태 코드: 400

InternalFailure

알 수 없는 오류, 예외 또는 장애 때문에 요청 처리가 실패했습니다.

HTTP 상태 코드: 500

InvalidAction

요청된 동작 또는 작업이 유효하지 않습니다. 작업을 올바로 입력했는지 확인합니다.

HTTP 상태 코드: 400

InvalidClientTokenId

제공된 X.509 인증서 또는 AWS 액세스 키 ID가 AWS의 레코드에 존재하지 않습니다.

HTTP 상태 코드: 403

NotAuthorized

이 작업을 수행하려면 권한이 있어야 합니다.

HTTP 상태 코드: 400

OptInRequired

AWS 액세스 키 ID는 서비스에 대한 구독이 필요합니다.

HTTP 상태 코드: 403

RequestExpired

요청이 요청상의 날짜 스탬프로부터 15분 이상, 또는 요청 만료 날짜(예: 미리 서명된 URL)로부터 15분 이상 경과한 후 서비스에 도달했거나, 요청상의 날짜 스탬프가 15분 이상 미래입니다.

HTTP 상태 코드: 400

ServiceUnavailable

서버의 일시적 장애로 인해 요청이 실패하였습니다.

HTTP 상태 코드: 503

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

ValidationError

입력이 AWS 서비스에서 지정한 제약에 충족되지 않습니다.

HTTP 상태 코드: 400

HTTP 쿼리 요청을 통한 API 호출

이 섹션에는 다음에 대한 Query API 사용에 대한 일반 정보가 포함되어 있습니다.AWS계정 관리. API 작업 및 오류에 대한 자세한 정보는 API 참조를 참조하십시오.

> **Note**
>
> 에 직접 전화를 거는 대신AWS계정 관리 쿼리 API, 다음 중 하나를 사용할 수 있습니다.AWSSDK. AWS SDK는 다양한 프로그래밍 언어 및 플랫폼(Java, Ruby, .NET, iOS, Android 등)을 위한 라이브러리와 샘플 코드로 구성되어 있습니다. SDK는 프로그래밍 방식으로 액세스할 수 있는 편리한 방법을 제공합니다.AWS계정 관리 및AWS. 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.

에 대한 쿼리 API 사용AWS계정 관리, 서비스 작업을 호출할 수 있습니다. 쿼리 API 요청은 다음을 포함해야 하는 HTTPS 요청입니다.`Action`수행할 작업을 나타내는 매개 변수입니다.AWS 계정 관리 지

원GET과POST모든 작업에 대한 요청 즉, API를 사용할 필요가 없습니다.GET일부 행동 및POST다른 사람들을 위해. 그러나GET요청에는 URL 크기 제한이 적용됩니다. 이 제한은 브라우저에 따라 다르지만 일반적인 제한은 2,048바이트입니다. 따라서 더 큰 크기가 필요한 Query API 요청의 경우 다음을 사용해야 합니다.POST의뢰.

응답은 XML 문서입니다. 응답에 대한 자세한 내용은 API 참조의 개별 작업 페이지를 참조하십시오.

주제

- 엔드포인트
- HTTPS 필요
- 서명AWS계정 관리 API 요청

엔드포인트

AWS계정 관리에는 미국 동부 (버지니아 북부) 에서 호스팅되는 단일 글로벌 API 엔드포인트가 있습니다.AWS 리전.

에 대한 자세한 내용은AWS모든 서비스의 엔드포인트 및 지역, 참조리전 및 엔드포인트에서AWS 일반 참조.

HTTPS 필요

Query API는 보안 자격 증명과 같은 민감한 정보를 반환할 수 있으므로 HTTPS를 사용하여 모든 API 요청을 암호화해야 합니다.

서명AWS계정 관리 API 요청

액세스 키 ID와 보안 액세스 키를 사용하여 요청에 서명해야 합니다. 사용하지 않는 것이 좋습니다 AWS일상적인 작업을 위한 루트 계정 자격 증명AWS계정 관리. 에 대한 자격 증명을 사용할 수 있습니다.AWS Identity and Access Management(IAM) 사용자 또는 IAM 역할과 함께 사용하는 임시 자격 증명

API 요청에 서명하려면 AWS 서명 버전 4를 사용해야 합니다. Signature Version 4 사용에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청에 서명을 참조하세요.

자세한 내용은 다음을 참조하세요.

- AWS 보안 자격 증명 – AWS 액세스를 위해 사용 가능한 자격 증명 유형에 대한 일반 정보를 제공합니다.

- IAM의 보안 모범 사례— 보안을 지원하는 IAM 서비스 사용에 대한 제안을 제공합니다.AWS리소스(다음 리소스 포함)AWS계정 관리.
- IAM의 임시 자격 증명 – 임시 보안 자격 증명을 생성하고 사용하는 방법에 대해 설명합니다.

AWS Account Management에 대한 할당량

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 달리 명시되지 않는 한, 각 할당량은 AWS 리전 개인별로 다릅니다.

각 AWS 계정 계정에는 계정 관리와 관련된 다음과 같은 할당량이 있습니다.

리소스	Quota
한 명의 대체 연락처 수 AWS 계정	3 -BILLING,SECURITY, 에 대해 각각 하나씩 OPERATIONS
계정당 동시 지역-옵트 요청 수	6
조직당 동시 지역-옵트 요청 수	20
계정당 DeleteAlternateContact 요청 비율	초당 1개, 초당 6개로 버스트
계정당 DisableRegion 요청 비율	초당 1개, 버스트는 초당 1개로 증가
계정당 EnableRegion 요청 비율	초당 1개, 버스트는 초당 1개로 증가
계정당 GetAlternateContact 요청 비율	초당 10개, 버스트는 초당 15개로 증가
계정당 GetContactInformation 요청 비율	초당 10개, 버스트는 초당 15개로 증가
계정당 GetRegionOptStatus 요청 비율	초당 5개, 버스트는 초당 5개로 증가
계정당 ListRegions 요청 비율	초당 5개, 버스트는 초당 5개로 증가
계정당 PutAlternateContact 요청 비율	초당 5개, 버스트는 초당 8개로
계정당 PutContactInformation 요청 비율	초당 5개, 버스트는 초당 8개로

문제 해결 AWS 계정

다음 항목의 정보를 사용하여 관련 문제를 진단하고 해결하십시오AWS 계정. 루트 사용자에 대한 도움이 필요하면 IAM 사용 설명서의 루트 사용자 관련 문제 해결을 참조하십시오. 로그인 프로세스에 대한 도움이 필요하면 로그인 사용 AWS 계정설명서의 AWS로그인 문제 해결을 참조하십시오.

주제 문제 해결

- AWS 계정생성 관련 문제 해결
- AWS 계정 폐쇄 관련 문제 해결
- 다른 문제 해결AWS 계정

AWS 계정생성 관련 문제 해결

여기의 정보를 사용하면 AWS 계정 생성과 관련된 문제를 해결하는 데 도움이 됩니다. 새 계정을 만든 후 로그인하는 데 문제가 발생하는 경우 로그인 가이드의 AWS 계정AWS로그인 문제 해결을 참조하십시오.

문제

- AWS에서 새 계정을 확인하라는 전화가 오지 않음
- 전화로 AWS 계정 인증을 시도할 때 "최대 실패 횟수" 관련 오류 발생
- 24시간 후에도 계정이 활성화되지 않음

AWS에서 새 계정을 확인하라는 전화가 오지 않음

계정을 AWS 계정 만들 때 SMS 메시지나 음성 통화를 받을 수 있는 전화번호를 입력해야 합니다. 전화번호 검증에 사용할 방법을 지정합니다.

메시지나 전화를 받지 못한 경우 다음을 확인합니다.

- 가입 과정에서 올바른 전화번호를 입력하고 올바른 국가 코드를 선택했습니다.
- 휴대폰을 사용하는 경우 SMS 메시지나 전화를 받을 수 있는 셀룰러 신호가 있는지 확인하세요.
- 결제 방법으로 입력한 정보가 정확합니다.

신원 확인 절차를 완료하라는 SMS나 전화를 받지 못한 경우 AWS 계정 수동으로 활성화하는 데 도움이 될 AWS Support 수 있습니다. 다음 단계를 사용합니다.

1. AWS 계정 정보에 입력한 전화번호로 연락할 수 있는지 확인합니다.
2. AWS Support 콘솔을 열고 사례 생성을 선택합니다.
   a. 계정 및 결제 지원을 선택합니다.
   b. 유형에서 계정을 선택합니다.
   c. 카테고리에서 활성화를 선택합니다.
   d. 사례 설명 섹션에 연락을 받을 수 있는 날짜 및 시간을 입력합니다.
   e. 연락처 옵션 섹션에서 연락 방법으로 채팅을 선택합니다.
   f. 제출을 선택합니다.

> **Note**
>
> 아직 AWS 계정 활성화되지 AWS Support 않았더라도 케이스를 생성할 수 있습니다.

전화로 AWS 계정 인증을 시도할 때 "최대 실패 횟수" 관련 오류 발생

AWS Support가 계정을 수동으로 활성화하는 데 도움이 될 수 있습니다. 다음 단계를 따릅니다.

1. 계정을 만들 때 지정한 이메일 주소와 암호를 입력하여 AWS 계정에 로그인합니다.
2. AWS Support 콘솔을 열고 사례 생성을 선택합니다.
3. 계정 및 결제 지원을 선택합니다.
4. 유형에서 계정을 선택합니다.
5. 카테고리에서 활성화를 선택합니다.
6. 사례 설명 섹션에 연락을 받을 수 있는 날짜 및 시간을 입력합니다.
7. 연락처 옵션 섹션에서 연락 방법으로 채팅을 선택합니다.
8. 제출을 선택합니다.

AWS Support에서 사용자에게 연락하여 AWS 계정의 수동 활성화를 시도합니다.

24시간 후에도 계정이 활성화되지 않음

경우에 따라 계정 활성화가 지연될 수 있습니다. 프로세스가 24시간 이상 소요되는 경우 다음을 확인합니다.

- 계정 활성화 프로세스를 완료합니다.

필요한 정보를 모두 추가하기 전에 가입 프로세스 창을 닫았다면 등록 페이지를 엽니다. 기존 AWS 계정 계정에 로그인을 선택하고, 계정으로 선택한 이메일 주소 및 비밀번호를 사용하여 로그인합니다.

- 결제 방법과 관련된 정보를 확인합니다.

  AWS Billing and Cost Management 콘솔에서 결제 방법에 오류가 있는지 확인합니다.

- 금융 기관에 문의합니다.

  금융 기관에서 AWS가 요청한 승인을 거부하는 경우가 있습니다. 결제 방법과 관련된 기관에 연락하여 AWS의 승인 요청을 승인해 달라고 요청합니다. AWS는 금융 기관에서 승인 요청을 승인하는 즉시 승인 요청을 취소하므로, 승인 요청 비용이 청구되지 않습니다. 금융 기관의 명세서에는 승인 요청이 여전히 소액 수수료(보통 1USD)로 표시될 수 있습니다.

- 이메일 및 스팸 폴더에서 추가 정보 요청을 확인합니다.
- 다른 브라우저를 사용해 보세요.
- AWS Support에 문의하세요.

  AWS Support에 문의하여 도움을 받으세요. 시도한 문제 해결 단계를 모두 알려주세요.

> **Note**
>
> AWS에 응답 시 신용카드 번호와 같은 민감한 정보를 제공하지 마세요.

AWS 계정 폐쇄 관련 문제 해결

아래 정보를 사용하여 계정 폐쇄 과정에서 발견되는 일반적인 문제를 진단하고 해결하세요. 계정 폐쇄 프로세스에 대한 일반 정보는 을 참조하십시오팬 닫기 AWS 계정.

주제

- 계정을 삭제하거나 취소하는 방법을 모르겠어요
- 계정 페이지에 계정 해지 버튼이 보이지 않습니다.
- 계정을 폐쇄했지만 확인 이메일을 아직 받지 못했습니다.
- 계정을 폐쇄하려고 할 때 ConstraintViolationException "" 오류 메시지가 나타납니다.
- 회원 계정을 폐쇄하려고 할 때 “CLOSE_ACCOUNT_QUOTA_EXCEDED”라는 오류 메시지가 나타납니다.

- 관리 계정을 폐쇄하기 전에 AWS 조직을 삭제해야 하나요?

계정을 삭제하거나 취소하는 방법을 모르겠어요

계정을 폐쇄하려면 에 나와 있는 지침을 따르세요팬 닫기 AWS 계정.

계정 페이지에 계정 해지 버튼이 보이지 않습니다.

루트 사용자로 로그인하지 않은 경우 계정 페이지에 계정 해지 버튼이 표시되지 않습니다. 계정을 폐쇄하려면 루트 AWS Management Console 사용자로 로그인해야 합니다. 로그인할 수 없는 경우 루트 사용자 관련 문제 해결을 참조하십시오.

계정을 폐쇄했지만 확인 이메일을 아직 받지 못했습니다.

이 확인 이메일은 의 루트 사용자 이메일 주소로만 AWS 계정발송됩니다. 몇 시간 내에 이 이메일을 받지 못하면 루트 AWS Management Console 사용자로 로그인하여 계정이 폐쇄되었는지 확인할 수 있습니다. 계정이 성공적으로 폐쇄되면 계정이 폐쇄되었음을 알리는 메시지가 표시됩니다. 폐쇄한 계정이 멤버 계정인 경우 SUSPENDED AWS Organizations 콘솔에서 폐쇄한 계정에 라벨이 표시되어 있는지 확인하여 성공적으로 폐쇄되었는지 확인할 수 있습니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 멤버 계정 해지를 참조하세요.

관리 계정을 폐쇄하려고 하는데 계정 폐쇄에 대한 확인 이메일을 받지 못했다면 조직에 활성 회원 계정이 있을 가능성이 큽니다. 조직에 활성 회원 계정이 없는 경우에만 관리 계정을 폐쇄할 수 있습니다. 조직에 활성 구성원 계정이 남아 있지 않은지 확인하려면 AWS Organizations 콘솔로 이동하여 계정 이름 Suspended 옆에 모든 구성원 계정이 표시되는지 확인하세요. 그런 다음 관리 계정을 폐쇄할 수 있습니다.

계정을 폐쇄하려고 할 때 ConstraintViolationException "" 오류 메시지가 나타납니다.

AWS Organizations 콘솔을 사용하여 관리 계정을 폐쇄하려고 하는데 이는 불가능합니다. 관리 계정을 폐쇄하려면 관리 계정의 루트 AWS Management Console 사용자로 로그인하고 계정 페이지에서 관리 계정을 닫아야 합니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 관리 계정 폐쇄를 참조하십시오.

회원 계정을 폐쇄하려고 할 때 “CLOSE_ACCOUNT_QUOTA_EXCEDED”라는 오류 메시지가 나타납니다.

30일의 기간 동안 멤버 계정 중 10%를 해지할 수 있습니다. 이 할당량의 기간은 달력상의 월을 기준으로 하지 않으며, 계정을 해지하는 시점에 시작됩니다. 최초 계정 해지 후 30일간은 10% 계정 해지 한도를 초과할 수 없습니다. 계정이 10% 를 초과하더라도 최소 계정 폐쇄는 10개이고 최대 계정 폐쇄는 1000개입니다. Organizations 할당량에 대한 자세한 내용은 사용 설명서의 할당량을 참조하십시오 AWS Organizations.AWS Organizations

관리 계정을 폐쇄하기 전에 AWS 조직을 삭제해야 하나요?

아니요. 관리 계정을 폐쇄하기 전에 AWS 조직을 삭제할 필요는 없습니다. 하지만 조직에 활성 구성원 계정이 없는 경우에만 관리 계정을 폐쇄할 수 있습니다. 조직에 활성 구성원 계정이 남아 있지 않은지 확인하려면 AWS Organizations 콘솔로 이동하여 계정 이름 Suspended 옆에 모든 구성원 계정이 표시되는지 확인하세요. 그런 다음 관리 계정을 폐쇄할 수 있습니다.

다른 문제 해결AWS 계정

여기에 있는 정보를 사용하여 관련 문제를 해결할 수 있습니다.AWS 계정.

문제

- 내 신용카드를 변경해야 함AWS 계정
- 사기성 신고해야 함AWS 계정활동
- 닫아야 함AWS 계정

내 신용카드를 변경해야 함AWS 계정

내 신용카드를 변경하려면AWS 계정로그인할 수 있어야 합니다.AWS사용자가 계정 소유자임을 증명해야 하는 보호 기능을 갖추고 있습니다. 지침은 단원을 참조하십시오.신용 카드 결제 방법 관리의AWS Billing사용 설명서.

사기성 신고해야 함AWS 계정활동

귀하의 부정 행위가 의심되는 경우AWS 계정보고서를 만들고 싶습니다.악용을 신고하려면 어떻게 해야 함AWS자원.

Amazon.com에서 구매한 상품에 문제가 있는 경우 단원을 참조하십시오.아마존 고객 서비스.

닫아야 함AWS 계정

닫기 관련 문제 해결에 도움이 필요하면AWS 계정참조팬 닫기 AWS 계정.

계정 관리 사용 설명서의 문서 기록

다음 표에는 AWS 계정 관리에 대한 설명서 릴리스가 설명되어 있습니다.

변경 사항	설명	날짜
계정 닫기 주제 다시 작성	회원 및 관리 계정을 폐쇄하는 방법에 대한 단계 추가를 포함하여 전체 계정 닫기 주제를 완전히 개편했습니다.	2024년 2월 1일
새 보안 챌린지 질문 추가에 대한 지원 종료	계정 페이지에서 새 챌린지 질문을 추가하는 옵션이 제거되었다는 점을 참고하여 새 콘텐츠를 추가했습니다.	2024년 1월 5일
`aws-portal` 네임스페이스 지원 종료	AWS Identity and Access Management이전에 계정을 관리하는 데 사용되었던 (IAM) 작업 (예:, `aws-portal:ModifyAccount` `aws-portal:ViewAccount`) 이 표준 지원이 종료되었습니다.	2024년 1월 1일
지역 주제 다시 작성	확장 및 축소 제어 추가를 포함하여 전체 지역 주제를 완전히 개편했습니다.	2023년 10월 8일
루트 사용자 주제를 IAM 사용 설명서로 재배치했습니다.	루트 사용자에 대한 논의를 하나의 주제로 통합하고, IAM 사용 설명서로 옮겨진 루트 사용자 주제에 대한 상호 참조 링크를 추가했습니다.	2023년 9월 18일
기본 계정 연락처 주제에 새 섹션이 추가되었습니다.	새 전화번호 및 이메일 주소 요구 사항 섹션이 추가되었습니다.	2023년 9월 12일

새 연락처 정보 API	신규 `GetContactInformation` 및 `PutContactInformation` API 지원.	2022년 7월 22일
AWS계정 관리는 이제 AWS Organizations 콘솔을 통한 대체 연락처 업데이트를 지원합니다.	이제 업데이트된 AWS Organizations 관리형 정책에서 제공하는 계정 API 권한을 사용하여 AWS Organizations 콘솔을 통해 조직의 대체 연락처를 업데이트할 수 있습니다.	2022년 2월 8일
최초 릴리스	AWS계정 관리 참조 가이드의 최초 릴리스	2021년 9월 30일

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.