aws

참조 안내서

AWS 계정 관리

AWS 계정 관리: 참조 안내서

Table of Contents

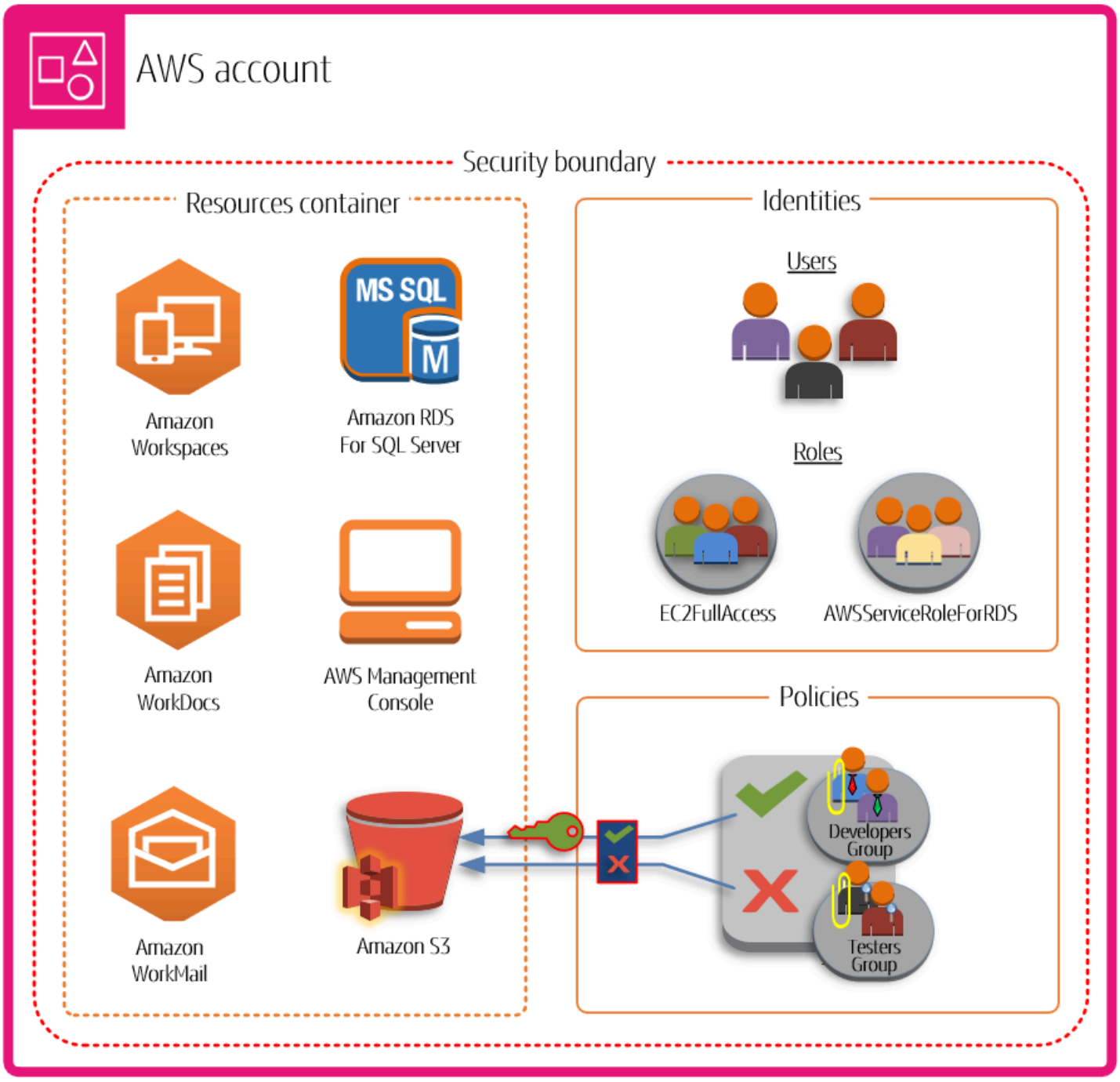
란 무엇입니까 AWS 계정?

는 사용자가 설정한 공식적인 비즈니스 관계를 AWS 계정 나타냅니다 AWS. 에서 AWS 리소스를 생성하고 관리하며 AWS 계정, 계정은 액세스 및 결제를 위한 자격 증명 관리 기능을 제공합니다. 각 AWS 계정 에는 다른 ID와 구별되는 고유한 ID가 있습니다 AWS 계정.

클라우드 리소스 및 데이터는 AWS 계정에 포함되어 있습니다. 계정은 자격 증명 및 액세스 관리 격리 경계 역할을 합니다. 두 계정 간에 리소스와 데이터를 공유해야 하는 경우 이 액세스를 명시적으로 허용해야 합니다. 기본적으로 계정 간에는 액세스할 수 없습니다. 예를 들어 프로덕션 및 비프로덕션 리소스와 데이터를 포함하도록 다른 계정을 지정하는 경우 기본적으로 이러한 환경 간에 액세스가 허용되지 않습니다.

AWS 계정 는 AWS 서비스 액세스의 기본 부분이기도 합니다. 다음 그림과 같이는 두 가지 기본 함수를 AWS 계정 제공합니다.

- 리소스 컨테이너 - AWS 계정 는 AWS 고객으로서 생성하는 모든 AWS 리소스의 기본 컨테이너입니다. 예를 들어 Amazon Simple Storage Service(Amazon S3) 버킷, Amazon Relational Database Service(Amazon RDS) 데이터베이스 및 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스는 모두 리소스입니다. 모든 리소스는 리소스를 포함하거나 소유한 계정의 계정 ID가 포함된 Amazon 리소스 이름(ARN)으로 고유하게 식별됩니다.
- 보안 경계 - AWS 계정 는 AWS 리소스의 기본 보안 경계이기도 합니다. 계정에서 생성한 리소스는 계정의 자격 증명을 가진 사용자만 사용할 수 있습니다. 계정에서 생성할 수 있는 주요 리소스 중에는 사용자 및 역할과 같은 자격 증명이 있습니다. ID에는 누군가가 AWS에 로그인(인증)하는 데 사용할 수 있는 자격 증명이 있습니다. ID에는 사용자가 계정의 리소스로 수행할 수 있는 작업(권한 부여)을 지정하는 권한 정책도 있습니다.



여러를 사용하는 것이 환경 규모를 조정하는 모범 사례 AWS 계정 입니다. 비용의 자연스러운 결제 경계를 제공하고, 보안을 위해 리소스를 격리하고, 개인과 팀에 유연성을 제공하고, 새로운 비즈니스 프로세스에 적응할 수 있기 때문입니다. 자세한 내용은 여러 AWS 계정을 사용할 때의 이점 단원을 참조하십시오.

의 기능 AWS 계정

AWS 계정 에는 다음과 같은 핵심 기능이 포함되어 있습니다.

- 비용 모니터링 및 제어 - 계정은 AWS 비용이 할당되는 기본 수단입니다. 이러한 사실 때문에 다양한 비즈니스 단위 및 워크로드 그룹에 대해 다양한 계정을 사용하면 클라우드 지출을 더 쉽게 추적, 제어, 예측, 예산 책정 및 보고하는 데 도움이 될 수 있습니다. 계정 수준에서의 비용 보고 외에도는 특정 AWS Organizations 시점에를 사용하기로 선택한 경우 전체 계정 세트에서 비용을 통합하고 보고할 수 있는 기본 제공 지원 AWS 도 제공합니다. 또한 AWS Service Quotas를 사용하면 AWS 비용에 큰 영향을 미칠 수 있는 AWS 리소스 및 악의적인 작업의 예기치 않은 과도한 프로비저닝으로부터 보호할 수 있습니다.
- 격리 단위 - AWS 계정 는 AWS 리소스의 보안, 액세스 및 청구 경계를 제공하여 리소스 자율성 및 격리를 달성하는 데 도움이 됩니다. 설계상 계정 내에서 프로비저닝된 모든 리소스는 자체 AWS 환경 내에서도 다른 계정에 프로비저닝된 리소스와 논리적으로 격리됩니다. 이 격리 경계는 애플리케이션 관련 문제, 잘못된 구성 또는 악의적인 작업의 위험을 제한하는 방법을 제공합니다. 한 계정 내에서 문제가 발생하면 다른 계정에 포함된 워크로드의 영향을 줄이거나 제거할 수 있습니다.
- 비즈니스 워크로드 미러링 - 여러 계정을 사용하여 서로 다른 계정에서 일반적인 비즈니스 목적으로 워크로드를 그룹화합니다. 따라서 소유권 및 의사 결정을 해당 계정과 정렬하고 다른 계정의 워크로드를 보호하고 관리하는 방법과의 종속성과 충돌을 방지할 수 있습니다. 전체 비즈니스 모델에 따라 서로 다른 계정에서 서로 다른 사업부 또는 자회사를 격리하도록 선택할 수 있습니다. 또한 이 접근 방식은 시간이 지남에 따라 해당 단위의 매각을 용이하게 할 수 있습니다.

처음 AWS 사용하시나요?

를 처음 사용하는 경우 AWS첫 번째 단계는에 가입하는 것입니다 AWS 계정. 가입하면는 사용자가 제공한 세부 정보가 포함된 계정을 AWS 생성하고 해당 계정을 할당합니다. 를 생성한 후 루트 사용자로 AWS 계정로그인하고 루트 사용자에 대해 멀티 팩터 인증(MFA)을 활성화하고 사용자에게 관리 액세스 권한을 할당합니다.

새 계정 설정 방법에 대한 단계별 지침은 시작하기 AWS 계정 섹션을 참조하세요.

관련 AWS 서비스

AWS 계정 는 다음 서비스에서 원활하게 작동합니다.

- IAM

AWS 계정 는 AWS Identity and Access Management (IAM)과 긴밀하게 통합됩니다. IAM을 계정과 함께 사용하여 계정의 다른 사용자가 업무 수행에 필요한 수준의 액세스 권한을 갖게 할 수 있습니다. 또한 IAM을 사용하여 계정별 정보뿐만 아니라 모든 AWS 리소스에 대한 액세스를 제어할 수 있습니다. AWS 계정구조의 설정 과정을 너무 많이 진행하기 전에, IAM의 주요 개념과 모범 사례를 숙지하는 것이 중요합니다. 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하십시오.

- AWS Organizations

  회사가 규모가 크거나 성장할 가능성이 있는 경우 회사의 특정 구조를 반영하는 여러 AWS 계정을 설정할 수 있습니다.는 다중 계정 환경을 구축하고 관리할 수 있는 기본 인프라와 기능을 AWS Organizations 제공합니다. 기존 계정을 하나의 조직으로 결합해 중앙에서 계정을 관리할 수 있습니다. 자동으로 조직의 일부가 되는 계정을 만들고, 다른 계정을 조직에 초대할 수 있습니다. 또 계정 일부나 전체에 영향을 주는 정책을 연결할 수도 있습니다. 자세한 내용은 사용 시기 AWS Organizations 단원을 참조하십시오.

- AWS Control Tower

  AWS Control Tower 는 안전한 다중 계정 AWS 환경을 설정하고 관리하는 간소화된 방법을 제공합니다.는를 사용하여 다중 계정 환경 생성을 AWS Control Tower 자동화하여 초기 계정 세트와 환경의 일부 기본 가드레일 및 구성을 AWS Organizations인스턴스화합니다. AWS Control Tower 를 사용하여 몇 단계로 새 AWS 계정 를 프로비저닝하는 동시에 계정이 조직 정책을 준수하는지 확인할 수 있습니다. 자세한 내용은 사용 시기 AWS Control Tower 단원을 참조하십시오.

사용 AWS 계정 루트 사용자

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

일상적인 작업에 루트 사용자를 사용하지 않으려면 AWS IAM Identity Center에서 관리 사용자를 설정하는 방법을 알아봅니다. 추가 루트 사용자 보안 권장 사항은 AWS 계정의 루트 사용자 모범 사례를 참조하십시오.

> **Important**
>
> 에 대한 루트 사용자 자격 증명이 있는 사람은 누구나 결제 정보를 포함하여 계정의 모든 리소스에 AWS 계정 무제한으로 액세스할 수 있습니다.

루트 사용자의 비밀번호를 변경하거나 재설정하고 루트 사용자의 액세스 키(액세스 키 ID 및 보안 액세스 키)를 생성하거나 삭제할 수 있습니다. 루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 로그인 사용 설명서의 루트 사용자 AWS Management Console 로에 로그인을 참조하세요. AWS

AWS 계정 관리 지원

AWS 계정 관리 지원 포럼을 사용하여 피드백과 질문을 게시할 수 있습니다. AWS 포럼에 대한 일반적인 내용은 섹션을 참조하세요AWS re:Post.

원하는 답변을 찾을 수 없는 경우를 사용하여 계정 또는 결제 관련 지원 사례를 생성할 AWS re:Post 수 있습니다 AWS Management Console. 자세한 내용은 Example: Create a support case for account and billing 섹션을 참조하세요.

기타 AWS 리소스

- AWS 훈련 및 과정 - 역할 기반 및 특수 과정과 자기 주도형 랩으로 연결되는 링크로, AWS 기술을 연마하고 실용적인 경험을 얻는 데 도움이 됩니다.
- AWS 개발자 도구 - 혁신적인 애플리케이션을 구축하는 데 도움이 되는 설명서, 코드 예제, 릴리스 정보 및 기타 정보를 제공하는 개발자 도구 및 리소스에 대한 링크입니다 AWS.
- AWS Support 센터 - AWS 지원 사례를 생성하고 관리하기 위한 허브입니다. 또한 포럼, 기술 FAQ, 서비스 상태 및 AWS Trusted Advisor 등의 기타 유용한 자료에 대한 링크가 있습니다.
- AWS 지원 - 클라우드에서 애플리케이션을 구축하고 실행하는 데 도움이 되는 one-on-one 빠른 응답 지원 채널인 AWS 지원에 대한 정보를 제공하는 기본 웹 페이지입니다.
- 문의처 - AWS 결제, 계정, 이벤트, 남용 및 기타 문제에 대한 문의를 위한 중앙 연락 창구입니다.
- AWS 사이트 약관 - 저작권 및 상표, 계정, 라이선스 및 사이트 액세스, 기타 주제에 대한 자세한 정보입니다.

시작하기 AWS 계정

를 처음 사용하는 경우 AWS첫 번째 단계는에 가입하는 것입니다 AWS 계정. 이렇게 하면 AWS 는 사용자가 제공한 세부 정보를 사용하여 계정을 생성하고 할당합니다.

이 섹션의 주제는 새로운에 대해 알아보고 설정하는 데 도움이 됩니다 AWS 계정.

주제

- 새 AWS 계정생성 사전 조건
- 생성 AWS 계정
- 루트 사용자의 다중 인증(MFA) 활성화
- 관리자 사용자 생성하기
- 에 액세스 AWS 계정

새 AWS 계정생성 사전 조건

에 가입하려면 다음 정보를 제공해야 AWS 계정합니다.

- 루트 사용자 이메일 주소 - 이메일 주소는 루트 사용자의 로그인 이름으로 사용되며 계정 복구에 필요합니다. 해당 주소로 전송된 이메일 메시지를 수신할 수 있어야 합니다. 특정 작업을 수행하기 전에 이 주소로 전송된 이메일에 대한 액세스 권한이 있는지 확인해야 합니다.

  > **Important**
  >
  > 이 계정이 비즈니스용인 경우 직원이 직무를 변경하거나 퇴사 AWS 계정 하더라도 회사가에 대한 액세스 권한을 유지할 수 있도록 안전한 기업 배포 목록(예: `it.admins@example.com`)을 사용합니다. 이메일 주소를 사용하여 계정의 루트 사용자 자격 증명을 재설정할 수 있으므로 이 배포 목록 또는 주소에 대한 액세스를 보호하세요.

- AWS 계정 이름 - 계정 이름은 인보이스와 같은 여러 위치와 Billing and Cost Management 대시보드 및 콘솔과 같은 AWS Organizations 콘솔에 표시됩니다. 인식하기 쉬운 계정 이름을 부여할 수 있도록 표준 방법을 사용하여 계정 이름을 지정하는 것을 권장합니다. 회사 계정인 경우 조직-목적-환경(예: AnyCompany-감사-제품)과 같은 이름 지정 표준을 사용하는 것이 좋습니다. 개인 계정인 경우 이름-성-목적(예: paulo-santos-testaccount) 등의 이름 지정 표준을 사용하는 것이 좋습니다.
- 주소 - 연락처 및 결제 주소가 인도에 있는 경우 계정의 사용자 계약은 인도의 현지 AWS 판매자인 Amazon Web Services India Private Limited(AWS 인도)와 체결됩니다. 확인 과정의 일환으로 CVV

를 제공해야 합니다. 은행에 따라 일회용 비밀번호를 입력해야 할 수도 있습니다. AWS 인도는 확인 프로세스의 일환으로 결제 방법 2INR을 청구합니다. AWS 인도는 확인이 완료된 후 2INR을 환불합니다.

- 전화번호 - 이 번호는 계정 소유권을 확인할 때 사용할 수 있습니다. 해당 전화번호에 수신되는 전화를 받을 수 있어야 합니다.

> **Important**
>
> 이 계정이 비즈니스용인 경우 직원이 직무를 변경하거나 퇴사 AWS 계정 하더라도 회사가에 대한 액세스 권한을 유지할 수 있도록 회사 전화번호를 사용합니다.

생성 AWS 계정

이 주제에서는에서 관리하지 AWS 계정 않는 독립 실행형를 생성하는 방법을 설명합니다 AWS Organizations. AWS Organizations에서 관리하는 조직의 일부인 계정을 생성하려면 AWS Organizations 사용 설명서의 Creating a member account in your organization을 참조하세요.

이 지침은 인도 AWS 계정 외부에서를 생성하기 위한 것입니다. 인도에서 계정을 생성하려면 AWS 인도를 AWS 계정 사용하여 생성 섹션을 참조하세요.

AWS Management Console

를 생성하려면 AWS 계정

1. Amazon Web Services 홈 페이지 를 엽니다.
2. 생성을 AWS 계정 선택합니다.

> **Note**
>
> AWS 최근에에 로그인한 경우 해당 옵션이 없을 수 있습니다. 대신 콘솔에 로그인을 선택합니다. 그 다음 AWS 계정새로 생성 옵션이 보이지 않는 경우 먼저 다른 계정으로 로그인을 선택하고 AWS 계정새로 생성을 선택합니다.

3. 계정 정보를 입력하고 그 다음 이메일 주소 확인을 선택합니다. 그러면 지정된 이메일 주소로 확인 코드가 전송됩니다.

> **Important**
>
> 계정의 루트 사용자의 중요한 특성으로 인해 개인만이 아닌 그룹에서 액세스할 수 있는 이메일 주소를 사용하는 것이 좋습니다. 이렇게 하면에 가입한 사람이 회사를 AWS 계정 떠나도 이메일 주소에 계속 액세스할 AWS 계정 수 있기 때문에를 계속 사용할 수 있습니다.
> AWS 계정과 연결된 이메일 주소에 대한 액세스 권한을 잃으면 비밀번호를 잃어버린 경우 계정에 대한 액세스를 복구할 수 없습니다.

4. 확인 코드를 입력한 다음 확인을 선택합니다.
5. 루트 사용자의 강력한 암호를 입력하고 확인한 다음 계속을 선택합니다. 암호가 다음 조건을 충족해야 AWS 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 동일해서는 안 됩니다.
6. 비즈니스 또는 개인을 선택합니다. 개인 계정과 비즈니스 계정의 특성과 기능은 동일합니다.
7. 회사 또는 개인 정보를 입력합니다.

> **Important**
>
> 비즈니스의 경우 다음을 입력하는 AWS 계정것이 가장 좋습니다.
>
> - 개인 전화번호의 숫자가 아닌 회사 전화번호입니다.
> - 계정을 사용할 회사 또는 조직에 속한 도메인 이름이 있는 이메일 주소입니다.
>
> 계정의 루트 사용자를 개별 이메일 주소 또는 개인 전화번호로 구성하면 계정이 안전하지 않을 수 있습니다.

8. AWS 고객 동의서를 읽고 수락합니다. AWS 고객 계약의 약관을 읽고 이해해야 합니다.
9. Continue(계속)을 선택합니다. 이때를 사용할 AWS 계정 준비가 되었음을 확인하는 이메일 메시지가 표시됩니다. 가입 시 입력한 이메일 주소와 암호를 사용하여 새 계정에 로그인할 수 있습니다. 그러나 계정 활성화를 완료할 때까지 AWS 는 서비스를 사용할 수 없습니다.

10. 결제 방법에 대한 정보를 입력한 다음 확인 및 계속을 선택합니다. 결제 정보에 다른 AWS 결제 주소를 사용하려면 새 주소 사용을 선택합니다.

    유효한 결제 방법을 추가할 때까지 가입 절차를 진행할 수 없습니다.

11. 목록에서 국가 또는 지역 코드를 선택하고 몇 분 후에 전화를 받을 수 있는 전화번호를 입력합니다.
12. CAPTCHA에 표시된 코드를 입력한 다음 제출합니다.
13. 자동 시스템이 사용자에게 연락하면 수신한 PIN을 입력한 다음 제출합니다.
14. 사용 가능한 AWS Support 계획 중 하나를 선택합니다. 사용 가능한 지원 요금제에 대한 설명은 Compare 지원 plans를 참조하세요.
15. 가입 완료를 선택합니다. 계정이 활성화되고 있음을 나타내는 확인 페이지가 나타납니다.
16. 이메일 및 스팸 폴더에서 계정이 활성화되었음을 확인하는 이메일 메시지를 확인합니다. 활성화는 일반적으로 몇 분이면 되지만 때로는 최대 24시간이 소요될 수 있습니다.

    정품 인증 메시지를 받으면 모든 AWS 서비스에 완전히 액세스할 수 있습니다.

AWS CLI & SDKs

조직의 관리 계정에 로그인한 상태에서 CreateAccount 작업을 실행하여 AWS Organizations 에서 관리하는 조직의 멤버 계정을 생성할 수 있습니다.

AWS Command Line Interface (AWS CLI) 또는 AWS API 작업을 사용하여 조직 AWS 계정 외부에서 독립 실행형를 생성할 수 없습니다.

루트 사용자의 다중 인증(MFA) 활성화

루트 사용자에서 MFA를 활성화하는 것이 좋습니다. MFA는 권한 부여 없이 누군가 계정에 액세스할 위험을 크게 낮춥니다.

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

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 로그인 사용 설명서의 루트 사용자 AWS Management Console 로에 로그인을 참조하세요. AWS
2. 루트 사용자에 MFA를 켭니다.

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

관리자 사용자 생성하기

루트 사용자가 수행할 수 있는 작업을 제한할 수 없으므로 루트 사용자가 명시적으로 필요하지 않은 작업에는 루트 사용자를 사용하지 않을 것을 권장합니다. 대신 IAM Identity Center의 관리 사용자에게 관리 액세스 권한을 할당하고 해당 관리 사용자로 로그인하여 일상적인 관리 작업을 수행합니다.

지침은 IAM Identity Center 사용 설명서의 IAM Identity Center 관리 사용자에 대한 AWS 계정 액세스 설정을 참조하세요.

관련 주제

- 루트 사용자 자격 증명 보호에 대한 자세한 내용은 IAM User Guide의 Securing the credentials for the root user을 참조하세요.
- 루트 사용자가 필요한 작업 목록은 IAM User Guide의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

에 액세스 AWS 계정

다음 방법 중 하나로 AWS 계정 에 액세스할 수 있습니다.

AWS Management Console

AWS Management Console는 AWS 계정 설정 및 AWS 리소스를 관리하는 데 사용할 수 있는 브라우저 기반 인터페이스입니다.

AWS 명령줄 도구

AWS 명령줄 도구를 사용하면 시스템의 명령줄에서 명령을 실행하여 AWS 계정 및 AWS 작업을 수행할 수 있습니다. 명령줄로 작업하는 것이 콘솔을 사용하는 것보다 더 빠르고 편리할 수 있습니다. 명령줄 도구는 AWS 작업을 수행하는 스크립트를 빌드하려는 경우에도 유용합니다.는 두 가지 명령줄 도구 세트를 AWS 제공합니다.

- AWS Command Line Interface (AWS CLI). 설치 및 사용에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 AWS CLI참조하세요.

- AWS Tools for Windows PowerShell. Tools for Windows PowerShell 설치 및 사용에 대한 자세한 내용은 AWS Tools for Windows PowerShell 사용 설명서를 참조하세요.

AWS SDK

AWS SDKs는 다양한 프로그래밍 언어 및 플랫폼(예: Java, Python, Ruby, .NET, iOS 및 Android)을 위한 라이브러리 및 샘플 코드로 구성됩니다. SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. 다운로드 및 설치 방법을 포함하여 AWS SDKs에 대한 자세한 내용은 Amazon Web Services용 도구를 참조하세요.

AWS 계정 관리 HTTPS 쿼리 API

AWS 계정 관리 HTTPS 쿼리 API를 사용하면 AWS 계정 및에 프로그래밍 방식으로 액세스할 수 있습니다 AWS. HTTPS 쿼리 API를 이용하면 HTTPS 요청을 서비스에 바로 보낼 수 있습니다. HTTPS API를 사용할 때는 자격 증명을 사용하여 요청에 디지털 방식으로 서명하는 코드를 포함해야 합니다. 자세한 내용은 Calling the API by making HTTP Query requests을 참조하세요.

AWS 계정 거버넌스 구조 계획

단일 계정으로 AWS 여정을 시작했을 수도 있지만 워크로드의 크기와 복잡성이 증가함에 따라 여러 계정을 설정하는 것이 AWS 좋습니다. 중소기업이든 대기업이든 데이터와 워크로드 요구 사항을 충족하는 거버넌스 구조 계획을 생성하는 것이 좋습니다.

이 섹션에서는 다중 계정 거버넌스 구조를 활성화 AWS 하는 데 도움이 되는에서 사용할 수 있는 이점 및 거버넌스 서비스를 다룹니다.

주제

여러 AWS 계정을 사용할 때의 이점

AWS 계정 에서 기본 보안 경계를 형성합니다 AWS 클라우드. 리소스의 컨테이너 역할을 하여 안전하고 잘 관리되는 환경을 만드는 데 필수적인 중요한 격리 계층을 제공합니다. 자세한 내용은 란 무엇입니까 AWS 계정? 단원을 참조하십시오.

리소스를 별도로 분리하면 클라우드 환경에서 다음 원칙을 지원하는 데 AWS 계정 도움이 됩니다.

- 보안 통제 – 애플리케이션마다 보안 프로필이 다를 수 있으므로 이에 대한 통제 정책 및 메커니즘이 다를 수 있습니다. 예를 들어 감사자와 대화하고 PCI(Payment Card Industry) 보안 표준이 적용되는 워크로드의 모든 요소를 호스팅 AWS 계정 하는 단일를 가리키는 것이 훨씬 쉽습니다.
- 격리 - AWS 계정 는 보안 보호의 단위입니다. 잠재적 위험과 보안 위협은 다른 사람에게 영향을 주지 AWS 계정 않고 내에 포함되어야 합니다. 팀이나 보안 프로필이 다르기 때문에 보안 요구 사항이 다를 수 있습니다.
- 많은 팀 – 팀마다 책임과 리소스 요건이 다릅니다. 팀이 서로를 분리하도록 이동하여 서로 간섭하지 않도록 할 수 있습니다 AWS 계정.
- 데이터 격리 - 팀을 격리하는 것 외에도 데이터 저장소를 계정별로 격리하는 것도 중요합니다. 이렇게 하면 해당 데이터 저장소에 액세스하고 관리할 수 있는 사람의 수를 제한하는 데 도움이 될 수 있습니다. 이것으로 아주 사적인 데이터의 노출을 억제할 수 있어 유럽 연합의 일반 데이터 보호 규정(GDPR)을 준수하는 데 도움이 될 수 있습니다.

- 비즈니스 프로세스 – 사업부 또는 제품마다 목적 및 프로세스가 완전히 다를 수 있습니다. 여러를 사용하면 사업부의 특정 요구 사항을 지원할 AWS 계정수 있습니다.
- 청구 - 청구 단계에서 계정이 항목을 구분할 수 있는 유일한 방법입니다. 여러 계정을 사용하면 청구 단계에서 사업부, 직무 팀 또는 개별 사용자 간에 항목을 구분할 수 있습니다. 행 항목을 구분하면서 모든 청구서를 단일 지급인(AWS Organizations 및 통합 결제 사용)에 통합할 수 있습니다 AWS 계정.
- 할당량 할당 - AWS 서비스 할당량은 각각에 대해 개별적으로 적용됩니다 AWS 계정. 워크로드를 AWS 계정 여러 개로 분리하여 서로의 할당량을 소비하는 것을 방지할 수 있습니다.

문서에 설명된 모든 권장 사항 및 절차는 AWS Well-Architected Framework를 준수합니다. 이 프레임워크는 유연하고, 복원력이 뛰어나며, 확장 가능한 클라우드 인프라를 설계하는 데 도움을 주기 위한 것입니다. 소규모로 시작하더라도 프레임워크의 이 지침을 준수하여 진행하는 것이 좋습니다. 규모가 커져도 현재의 운영에 영향을 주지 않으면서 환경을 안전하게 확장할 수 있습니다.

여러 관리 AWS 계정

여러 계정을 추가하기 전에 계정을 관리할 계획을 세우는 것이 좋습니다. 이를 위해 조직의 모든를 관리하는 무료 AWS 서비스AWS Organizations인를 AWS 계정 사용하는 것이 좋습니다.

AWS 또한는 Organizations에 AWS 관리형 자동화 계층을 추가하고 AWS CloudTrail AWS Config Amazon CloudWatch 등과 같은 다른 AWS 서비스와 자동으로 통합 AWS Control Tower하는 AWS Service Catalog를 제공합니다. 이러한 서비스에는 추가 비용이 발생할 수 있습니다. 자세한 내용은 AWS Control Tower 요금을 참조하세요.

다음 사항도 참조하세요.

- 사용 시기 AWS Organizations
- 사용 시기 AWS Control Tower

사용 시기 AWS Organizations

AWS Organizations 는를 그룹 AWS 계정 으로 관리하는 데 사용할 수 있는 AWS 서비스입니다. 이렇게 하면 계정의 모든 청구서를 그룹화하고 한 명의 결제자가 처리하는 통합 결제와 같은 기능이 제공됩니다. 정책 기반 제어를 사용하여 조직의 보안을 중앙에서 관리할 수도 있습니다. 에 대한 자세한 내용은 AWS Organizations 사용 설명서를 AWS Organizations참조하세요.

트러스트된 액세스

AWS Organizations 를 사용하여 계정을 그룹으로 관리하는 경우 조직의 대부분의 관리 작업은 조직의 관리 계정에서만 수행할 수 있습니다. 기본적으로 여기에는 조직 자체 관리와 관련된 작업만 포함됩니다. Organizations와 해당 AWS 서비스 간에 신뢰할 수 있는 액세스를 활성화하여이 추가 기능을 다른 서비스로 확장할 수 있습니다. 신뢰할 수 있는 액세스는 지정된 AWS 서비스에 조직 및 조직에 포함된 계정에 대한 정보에 액세스할 수 있는 권한을 부여합니다. 계정 관리에 대한 신뢰할 수 있는 액세스를 활성화하면 계정 관리 서비스는 조직 및 해당 관리 계정에게 조직의 모든 멤버 계정에 대한 기본 또는 대체 연락처 정보와 같은 메타데이터에 액세스할 수 있는 권한을 부여합니다.

자세한 내용은 AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화 단원을 참조하십시오.

위임된 관리자

신뢰할 수 있는 액세스를 활성화한 후 멤버 계정 중 하나를 AWS Account Management의 위임된 관리자 계정으로 지정할 수도 있습니다. 이렇게 하면 위임된 관리자 계정이 조직의 멤버 계정에 대해 이전에 관리 계정만 수행할 수 있었던 것과 동일한 계정 관리 메타데이터 관리 작업을 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 내용은 AWS 계정 관리에 대한 위임된 관리자 계정 활성화 단원을 참조하십시오.

서비스 제어 정책

AWS 계정 가에서 관리하는 조직의 일부인 경우 조직의 AWS Organizations관리자는 멤버 계정의 보안 주체가 수행할 수 있는 작업을 제한할 수 있는 서비스 제어 정책(SCPs)을 적용할 수 있습니다. SCP는 권한을 부여하지 않습니다. 대신 멤버 계정에서 사용할 수 있는 권한을 제한하는 필터입니다. 멤버 계정의 사용자 또는 역할(위탁자)은 계정에 적용되는 SCP와 위탁자에 연결된 IAM 권한 정책이 허용하는 것과 교차하는 작업만 수행할 수 있습니다. 예를 들어 SCP 사용하여 계정의 위탁자가 자기 계정의 대체 연락처를 수정하지 못하도록 할 수 있습니다.

에 적용되는 SCPs의 예는 섹션을 AWS 계정참조하세요AWS Organizations 서비스 제어 정책을 사용하여 액세스 제한.

AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화

AWS Account Management에 대한 신뢰할 수 있는 액세스를 활성화하면 관리 계정의 관리자가의 각 멤버 계정과 관련된 정보 및 메타데이터(예: 기본 또는 대체 연락처 세부 정보)를 수정할 수 있습니다 AWS Organizations. 자세한 내용은 AWS Organizations 사용 설명서에서 AWS Account Management 및 AWS Organizations을 참조하세요. 신뢰할 수 있는 액세스의 작동 방식에 대한 일반적인 내용은 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요.

신뢰할 수 있는 액세스가 활성화되면 accountID 파라미터를 지원하는 계정 관리 API 작업에서 해당 파라미터를 사용할 수 있습니다. 이 파라미터는 관리 계정이나 조직의 위임된 관리자 계정(활성화된 경우)에서 자격 증명을 사용하여 작업을 호출한 경우에만 성공적으로 사용할 수 있습니다. 자세한 내용은 AWS 계정 관리에 대한 위임된 관리자 계정 활성화 단원을 참조하십시오.

다음 절차에 따라 조직의 계정 관리에 대한 신뢰할 수 있는 액세스를 활성화합니다.

최소 권한

이 작업을 수행하려면 다음 요구 사항을 충족해야 합니다.

- 이 작업은 조직의 관리 계정에서만 수행할 수 있습니다.
- 조직의 모든 기능을 활성화해야 합니다.

AWS Management Console

AWS 계정 관리에 대해 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 서비스를 선택합니다.
3. 서비스 목록에서 AWS 계정 관리를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.

AWS CLI & SDKs

AWS 계정 관리에 대해 신뢰할 수 있는 액세스를 활성화하려면

다음 명령을 실행한 후 조직의 관리 계정에서 자격 증명을 사용하여 --accountId 파라미터로 조직의 멤버 계정을 참조하는 계정 관리 API 작업을 호출할 수 있습니다.

- AWS CLI: enable-aws-service-access

  다음 예시에서는 호출 계정의 조직에서 AWS Account Management에 대한 신뢰할 수 있는 액세스를 활성화합니다.

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

성공 시 이 명령은 출력을 생성하지 않습니다.

AWS 계정 관리에 대한 위임된 관리자 계정 활성화

위임된 관리자 계정을 활성화하면의 다른 멤버 계정에 대한 AWS 계정 관리 API 작업을 호출할 수 있습니다 AWS Organizations. 조직에 위임된 관리자 계정을 등록한 후 해당 계정의 사용자와 역할은 선택적 `AccountId` 파라미터를 지원하여 조직 모드에서 작동할 수 있는 `account` 네임스페이스의 AWS CLI 및 AWS SDK 작업을 호출할 수 있습니다.

조직의 멤버 계정을 위임된 관리자 계정으로 등록하려면 다음 절차를 따르세요.

AWS CLI & SDKs

계정 관리에 위임된 관리자 계정을 등록하려면

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

> 최소 권한
>
> 이 작업을 수행하려면 다음 요구 사항을 충족해야 합니다.
>
> - 이 작업은 조직의 관리 계정에서만 수행할 수 있습니다.
> - 조직의 모든 기능을 활성화해야 합니다.
> - 조직의 계정 관리에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다.

다음 서비스 위탁자를 지정해야 합니다.

```
account.amazonaws.com
```

- AWS CLI: register-delegated-administrator

  다음 예에서는 조직의 멤버 계정을 계정 관리 서비스의 위임된 관리자로 등록합니다.

```
$ aws organizations register-delegated-administrator \
```

```
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

성공 시 이 명령은 출력을 생성하지 않습니다.

이 명령을 실행한 후 계정 123456789012의 자격 증명을 사용하여 `--account-id` 파라미터를 사용하여 조직의 멤버 계정을 참조하는 계정 관리 AWS CLI 및 SDK API 작업을 호출할 수 있습니다.

AWS Management Console

이 작업은 AWS 계정 관리 콘솔에서 지원되지 않습니다. 이 작업은 AWS CLI 또는 AWS SDKs.

AWS Organizations 서비스 제어 정책을 사용하여 액세스 제한

이 주제에서는 AWS Organizations 에서 서비스 제어 정책(SCP)을 사용하여 조직 내 계정의 사용자 및 역할이 수행할 수 있는 작업을 제한하는 방법을 보여주는 예제를 설명합니다. 서비스 제어 정책에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 다음 주제를 참조하세요.

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

Example 예제 1: 계정이 자신의 대체 연락처를 수정하지 못하도록 방지

다음 예에서는 독립 실행형 계정 모드의 멤버 계정에서 `PutAlternateContact` 및 `DeleteAlternateContact` API 작업을 호출하지 못하도록 거부합니다. 이렇게 하면 영향을 받는 계정의 위탁자가 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: 멤버 계정이 조직의 다른 멤버 계정의 대체 연락처를 수정하지 못하도록 방지

다음 예에서는 Resource 요소를 “*”로 일반화합니다. 즉, 독립 실행형 모드 요청과 조직 모드 요청 모두에 적용됩니다. 즉, 계정 관리의 위임된 관리자 계정이라도 SCP가 적용되는 경우 조직 내 모든 계정에 대한 대체 연락처가 변경되지 않습니다.

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

Example 예제 3: OU의 멤버 계정이 자신의 대체 연락처를 수정하지 못하도록 방지

다음 SCP 예에는 계정의 조직 경로를 두 개의 OU 목록과 비교하는 조건이 포함되어 있습니다. 이렇게 하면 지정된 OU의 모든 계정에서 위탁자가 자신의 대체 연락처를 수정하지 못하게 됩니다.

```
{
    "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/"
                    ]
                }
            }
    ]
}
```

사용 시기 AWS Control Tower

AWS Organizations 는 전체 AWS 환경을 중앙에서 관리하고 보호할 수 있는 기본 서비스입니다. 이 AWS Organizations중심 접근 방식의 중요한 구성 요소는 입니다 AWS Control Tower.는 Organizations 내에서 관리 콘솔 AWS Control Tower 역할을 하여 규범적 모범 사례를 적용하여 안전한 다중 계정 AWS 환경을 설정하고 관리하는 간소화된 방법을 제공합니다.

에서 제공하는이 보안 모범 사례 접근 방식은의 핵심 기능을 AWS Control Tower 확장합니다 AWS Organizations.는 일련의 예방 및 탐지 가드레일을 AWS Control Tower 적용하여 조직과 계정이 권장 보안 및 규정 준수 표준을 준수하도록 합니다.

를 사용하여 잘 설계된 AWS Organizations 구조를 구축하면 확장 가능하고 안전하며 규정을 준수하는 AWS 환경을 빠르게 배포할 AWS Control Tower수 있습니다. 클라우드 관리 및 거버넌스에 대한 이러한 중앙 집중식 접근 방식은 최고 수준의 보안 및 규정 준수를 AWS 클라우드 유지하면서의 모든 기능을 활용하려는 기업에 필수적입니다.

자세한 정보는 AWS Control Tower사용 설명서의 AWS Control Tower (이)란 무엇입니까? 섹션을 참조하세요.

API 작업 모드 이해

AWS 계정의 속성으로 작업하는 API 작업은 항상 두 가지 작업 모드 중 하나에서 작동합니다.

- 독립 실행형 컨텍스트 - 이 모드는 계정의 사용자 또는 역할이 동일한 계정의 계정 속성에 액세스하거나 변경할 때 사용됩니다. 독립형 컨텍스트 모드는 계정 관리 AWS CLI 또는 AWS SDK 작업 중 하나를 호출할 때 `AccountId` 파라미터를 포함하지 않을 때 자동으로 사용됩니다.
- 조직 컨텍스트 - 이 모드는 조직의 한 계정에 있는 사용자 또는 역할이 동일한 조직의 다른 멤버 계정에 액세스하거나 계정 속성을 변경할 때 사용됩니다. Account Management AWS CLI 또는 AWS SDK 작업 중 하나를 호출할 때 `AccountId` 파라미터를 포함하면 조직 컨텍스트 모드가 자동으로

사용됩니다. 조직의 관리 계정 또는 계정 관리의 위임된 관리자 계정에서만 이 모드의 작업을 호출할 수 있습니다.

AWS CLI 및 AWS SDK 작업은 독립 실행형 또는 조직 컨텍스트에서 작동할 수 있습니다.

- `AccountId` 파라미터를 포함하지 않으면 작업이 독립 실행형 컨텍스트에서 실행되고 요청을 수행하는 데 사용한 계정에 요청이 자동으로 적용됩니다. 이는 계정이 조직의 멤버인지 여부와 관계없이 적용됩니다.
- `AccountId` 파라미터를 포함하면 조직 컨텍스트에서 작업이 실행되고 지정된 조직 계정에서 작업이 작동합니다.
  - 작업을 호출하는 계정이 계정 관리 서비스의 관리 계정 또는 위임된 관리자 계정인 경우 `AccountId` 파라미터에서 해당 조직의 멤버 계정을 지정하여 지정된 계정을 업데이트할 수 있습니다.
  - 대체 연락 작업 중 하나를 호출하고 `AccountId` 파라미터에 자체 계정 번호를 지정할 수 있는 조직의 유일한 계정은 계정 관리 서비스의 위임된 관리자 계정으로 지정된 계정입니다. 관리 계정을 포함한 다른 모든 계정은 `AccessDenied` 예외를 받습니다.
- 독립 실행형 모드에서 작업을 실행하는 경우 모든 리소스를 허용하는 `"*"`의 `Resource` 요소 또는 독립 실행형 계정에 대한 구문을 사용하는 ARN을 포함하는 IAM 정책을 사용하여 작업을 실행할 수 있어야 합니다.
- 조직 모드에서 작업을 실행하는 경우 모든 리소스를 허용하는 `"*"`의 `Resource` 요소가 포함된 IAM 정책 또는 조직의 멤버 계정에 대한 구문을 사용하는 ARN을 사용하여 작업을 실행할 수 있어야 합니다.

계정 속성을 업데이트할 수 있는 권한 부여

대부분의 AWS 작업과 마찬가지로 IAM 권한 정책을 사용하여에 대한 계정 속성을 추가, 업데이트 또는 삭제할 수 AWS 계정 있는 권한을 부여합니다. IAM 위탁자(사용자 또는 역할)에 IAM 권한 정책을 연결할 때 위탁자가 어떤 리소스에서 어떤 조건에서 수행할 수 있는지 지정합니다.

다음은 권한 정책을 생성하기 위한 계정 관리별 몇 가지 고려 사항입니다.

에 대한 Amazon 리소스 이름 형식 AWS 계정

- 정책 설명의 `resource` 요소에 포함할 수 AWS 계정 있는의 Amazon 리소스 이름(ARN)은 참조하려는 계정이 독립 실행형 계정인지 아니면 조직에 있는 계정인지에 따라 다르게 구성됩니다. API 작업 모드 이해의 이전 섹션을 참조하세요.

- 독립 실행형 계정의 계정 ARN:

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

  AccountID 파라미터를 포함하지 않고 독립 실행형 모드에서 계정 속성 작업을 실행할 때 이 형식을 사용해야 합니다.

- 조직의 멤버 계정에 대한 계정 ARN는 다음과 같습니다.

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

  AccountID 파라미터를 포함하여 조직 모드에서 계정 속성 작업을 실행할 때 이 형식을 사용해야 합니다.

IAM 정책의 컨텍스트 키

또한 계정 관리 서비스는 부여한 권한에 대한 세분화된 제어를 제공하는 여러 계정 관리 서비스별 조건 키를 제공합니다.

account:AccountResourceOrgPaths

account:AccountResourceOrgPaths 컨텍스트 키를 사용하면 조직의 계층 구조를 통해 특정 조직 단위(OU)로 가는 경로를 지정할 수 있습니다. 해당 OU에 포함된 멤버 계정만 조건과 일치합니다. 다음 예시 코드 조각은 지정된 두 OU에 있는 계정에만 적용할 수 있는 정책을 제한합니다.

account:AccountResourceOrgPaths는 다중 값 문자열 유형이므로 ForAnyValue 또는 ForAllValues 다중 값 문자열 연산자 를 사용해야 합니다. 또한 조직의 OU에 대한 경로를 참조하더라도 조건 키의 접두사는 account입니다.

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

account:AccountResourceOrgTags

account:AccountResourceOrgTags 컨텍스트 키를 사용하면 조직의 계정에 연결할 수 있는 태그를 참조할 수 있습니다. 태그는 계정의 리소스를 분류하고 레이블을 지정하는 데 사용할 수 있는 키/값 문자열 페어입니다. 태그 지정에 대한 자세한 내용은 AWS Resource Groups 사용 설명서의 Tag Editor를 참조하세요. 속성 기반 액세스 제어 전략의 일부로 태그를 사용하는 방법에 대한 자세한 내용은 IAM User Guide의 AWS용 ABAC란 무엇입니까?를 참조하세요. 다음 예시 코드 조각은 project 키와 값이 blue 또는 red인 태그가 있는 조직의 계정에만 적용되도록 정책을 제한합니다.

account:AccountResourceOrgTags는 다중 값 문자열 유형이므로 ForAnyValue 또는 ForAllValues 다중 값 문자열 연산자 를 사용해야 합니다. 또한 조직의 멤버 계정에서 태그를 참조하더라도 조건 키의 접두사는 account입니다.

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

> **Note**
>
> 조직의 계정에만 태그를 연결할 수 있습니다. 독립 실행형 에는 태그를 연결할 수 없습니다 AWS 계정.

구성 AWS 계정

이 섹션에는 관리 방법을 설명하는 주제가 포함되어 있습니다 AWS 계정.

> **Note**
>
> AWS 계정 가 Amazon Web Services India Private Limited(AWS 인도)를 사용하여 인도에서 생성된 경우 추가 고려 사항이 있습니다. 자세한 내용은 인도의 계정 관리 단원을 참조하십시오.

주제

AWS 계정 별칭 생성

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

계정 별칭을 생성하거나 업데이트하는 방법을 알아보려면 IAM 사용 설명서의 AWS 계정 ID에 별칭 사용을 참조하세요.

계정 AWS 리전 에서 활성화 또는 비활성화

AWS 리전은 다수의 가용 영역이 포함된 전 세계의 물리적 위치입니다. 가용 영역은 하나 이상의 개별 AWS 데이터 센터로 구성되며, 각 데이터 센터는 중복 전원, 네트워킹 및 연결을 갖추고 별도의 시설에

있습니다. 즉, 각 AWS 리전 는 물리적으로 격리되어 있고 다른 리전과 독립적입니다. 리전에서는 내결함성, 안정성 및 복원성을 지원하고 지연 시간을 줄일 수도 있습니다. 사용 가능한 리전 및 향후 리전의 맵에 대한 자세한 내용은 Regions and Availability Zones을 참조하세요.

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

계정을 통해 자신이 사용할 수 있는 리전을 결정합니다.

- 는 요구 사항을 충족하는 위치에서 AWS 리소스를 시작할 수 있도록 여러 리전을 AWS 계정 제공합니다. 예를 들어 유럽의 고객들과 좀더 가까운 곳에 위치하거나 또는 법적 요구사항을 준수하기 위해 유럽에 소재한 위치에서 Amazon EC2 인스턴스를 실행할 필요가 있을 수 있습니다.
- An AWS GovCloud(미국 서부) 계정은 AWS GovCloud(미국 서부) 리전 및 AWS GovCloud(미국 동부) 리전에 대한 액세스를 제공합니다. 자세한 내용은 AWS GovCloud (US) 단원을 참조하십시오.
- Amazon AWS (중국) 계정은 베이징 및 닝샤 리전에만 액세스할 수 있습니다. 자세한 내용은 중국 Amazon Web Services를 참조하세요.

리전 이름 및 해당 코드 목록은 AWS General Reference Guide의 Regional endpoints를 참조하세요. 각 리전(엔드포인트 제외)에서 지원되는 AWS 서비스 목록은 AWS 리전 서비스 목록을 참조하세요.

> **Important**
>
> AWS 에서는 지연 시간을 줄이기 위해 글로벌 엔드포인트 대신 리전 AWS Security Token Service (AWS STS) 엔드포인트를 사용할 것을 권장합니다. 리전 AWS STS 엔드포인트의 세션 토큰은 모든 AWS 리전에서 유효합니다. 리전 AWS STS 엔드포인트를 사용하는 경우 변경할 필요가 없습니다. 그러나 전역 AWS STS 엔드포인트(https://sts.amazonaws.com)의 세션 토큰은 AWS 리전 활성화하거나 기본적으로 활성화된 에서만 유효합니다. 계정에 새 리전을 활성화하려는 경우 리전 AWS STS 엔드포인트의 세션 토큰을 사용하거나 전역 AWS STS 엔드포인트를 활성화하여 모든에서 유효한 세션 토큰을 발급할 수 있습니다 AWS 리전. 모든 리전에서 유효한 세션 토큰이 더 큽니다. 세션 토큰을 저장하는 경우 이러한 더 큰 토큰이 시스템에 영향을 미칠 수 있습니다. AWS STS 엔드포인트가 AWS 리전과 작동하는 방식에 대한 자세한 내용은 AWS 리전 AWS STS 에서 관리를 참조하세요.

주제

- 리전 활성화 및 비활성화 전 고려 사항

- 독립 실행형 계정에 대해 리전 활성화 또는 비활성화
- 조직에서 리전 활성화 또는 비활성화

리전 활성화 및 비활성화 전 고려 사항

리전을 활성화 또는 비활성화하기 전에 다음을 고려하는 것이 중요합니다.

- 2019년 3월 20일 이전에 도입된 리전은 기본적으로 활성화되어 있으며 AWS , 기본적으로 모든 새 리전이 활성화되어 AWS 리전 있으므로 이러한 리전에서 즉시 리소스 생성 및 관리를 시작할 수 있습니다. 기본적으로 활성화되는 리전은 활성화하거나 비활성화할 수 없습니다. 오늘에서 리전을 AWS 추가하면 새 리전이 기본적으로 비활성화됩니다. 사용자가 새 리전에서 리소스를 생성하고 관리할 수 있게 하려면 해당 리전을 활성화해야 합니다. 다음 리전은 기본적으로 활성화됩니다.

명칭	코드
미국 동부(버지니아 북부)	us-east-1
미국 동부(오하이오)	us-east-2
미국 서부(캘리포니아 북부)	us-west-1
미국 서부(오리건)	us-west-2
아시아 태평양(도쿄)	ap-northeast-1
아시아 태평양(서울)	ap-northeast-2
아시아 태평양(오사카)	ap-northeast-3
아시아 태평양(뭄바이)	ap-south-1
아시아 태평양(싱가포르)	ap-southeast-1
아시아 태평양(시드니)	ap-southeast-2
캐나다(중부)	ca-central-1
유럽(프랑크푸르트)	eu-central-1
유럽(스톡홀름)	eu-north-1

명칭	코드
유럽(아일랜드)	eu-west-1
유럽(런던)	eu-west-2
유럽(파리)	eu-west-3
남아메리카(상파울루)	sa-east-1

- 리전 옵션 상태에 관계없이 리전 간 추론 지오그래피에서 모든 대상 리전을 사용할 수 있습니다. Amazon Bedrock(리전 간 추론을 통한 처리량 증가 참조) 및 Amazon Q Developer(Amazon Q Developer의 리전 간 처리 참조)를 포함한 특정 AWS 생성형 AI 서비스는 리전 간 추론을 사용합니다. 이러한 서비스를 사용하는 경우 선택한 리전 내에서 리소스 및 IAM 데이터에 대해 활성화하지 않은 리전을 AWS 리전포함하여 최적의를 자동으로 선택합니다. 이렇게 하면 사용 가능한 컴퓨팅 및 모델 가용성을 극대화하여 고객 경험이 향상됩니다.
- IAM 권한을 사용하여 리전에 대한 액세스를 제어할 수 있습니다. – AWS Identity and Access Management (IAM)에는 리전을 활성화, 비활성화, 가져오기 및 나열할 수 있는 사용자를 제어할 수 있는 네 가지 권한이 포함되어 있습니다. 자세한 내용은 IAM User Guide의 AWS: AWS 리전활성화 및 비활성화 허용을 참조하세요. `aws:RequestedRegion` 조건 키를 사용하여의에 대한 액세스를 제어할 수도 AWS 서비스 있습니다 AWS 리전.
- 리전 활성화 무료 - 리전을 활성화하는 데 드는 비용은 없습니다. 새 리전에서 생성하는 리소스에만 요금이 부과됩니다.
- 리전을 비활성화하면 리전의 리소스에 대한 IAM 액세스가 비활성화됩니다. - Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 같은 AWS 리소스가 여전히 포함된 리전을 비활성화하면 해당 리전의 리소스에 대한 IAM 액세스가 손실됩니다. 예를 들어 AWS Management Console 를 사용하여 비활성화된 리전에 있는 EC2 인스턴스의 구성을 보거나 변경할 수 없습니다.
- 리전을 비활성화해도 활성 리소스에 대한 요금 계속 부과 - 아직 AWS 리소스가 포함된 리전은 비활성화해도 해당 리소스(있는 경우)에 대한 요금은 표준 요금으로 계속 발생합니다. 예를 들어 Amazon EC2 인스턴스가 있는 리전을 비활성화하여 인스턴스에 액세스할 수 없게 되었더라도 그러한 인스턴스의 요금은 그대로 지불해야 합니다.
- 리전 비활성화가 항상 즉시 표시에 반영되는 것은 아님 - 리전 비활성화 후 서비스 및 콘솔에 일시적으로 표시될 수 있습니다. 리전 비활성화가 적용되는 데는 몇 분에서 몇 시간이 걸립니다.
- 어떤 경우에는 리전을 활성화하는 데에 몇 분에서 몇 시간이 걸리기도 함 - 리전을 활성화하면 AWS에서 해당 리전의 계정을 준비하는 작업(예: IAM 리소스를 해당 리전으로 배포)을 수행합니다. 이 프로세스는 대부분의 계정에서 몇 분이 걸리지만 때로는 몇 시간이 걸릴 수도 있습니다. 이 프로세스가 완료될 때까지는 해당 리전을 사용할 수 없습니다.

- 조직은 AWS 조직 전체에서 지정된 시간에 50개의 리전 옵션 요청을 열 수 있음 - 관리 계정은 언제든지 조직에 대한 완료 보류 중인 50개의 미결 요청을 가질 수 있습니다. 한 요청은 한 계정에 대한 한 특정 리전의 활성화 또는 비활성화와 같습니다.
- 단일 계정에는 지정된 시간에 6개의 리전 설정 요청이 진행 중일 수 있음 - 한 요청은 한 계정에 대한 특정 리전의 활성화 또는 비활성화와 같습니다.
- Amazon EventBridge 통합 - 고객은 EventBridge에서 리전 설정 상태 업데이트 알림을 구독할 수 있습니다. 각 상태 변경에 대해 EventBridge 알림을 생성해 고객이 워크플로를 자동화할 수 있습니다.
- 표현식 리전 설정 상태 - 옵트인 리전을 활성화/비활성화하는 비동기적 특성으로 인해 리전 설정 요청에 대한 네 가지 잠재적 상태가 있습니다.
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  `ENABLING` 또는 `DISABLING` 상태인 경우 옵트인 또는 옵트아웃을 취소할 수 없습니다. 그렇지 않으면 `ConflictException`이 발생합니다. 완료된(활성화/비활성화) 리전 옵션 요청은 주요 기본 AWS 서비스의 프로비저닝에 따라 달라집니다. 상태가 임에도 불구하고 즉시 사용할 수 없는 일부 AWS 서비스가 있을 수 있습니다`ENABLED`.
- 와의 전체 통합 AWS Organizations - 관리 계정은 해당 AWS 조직의 모든 멤버 계정에 대한 리전 옵션을 수정하거나 읽을 수 있습니다. 멤버 계정은 리전 상태도 읽거나 쓸 수 있습니다.

독립 실행형 계정에 대해 리전 활성화 또는 비활성화

AWS 계정 가 액세스할 수 있는 리전을 업데이트하려면 다음 절차의 단계를 수행합니다. 아래 AWS Management Console 절차는 항상 독립 실행형 컨텍스트에서만 작동합니다. 를 사용하여 작업을 호출 AWS Management Console 하는 데 사용한 계정에서 사용 가능한 리전만 보거나 업데이트할 수 있습니다.

AWS Management Console

독립 실행형에 대해 리전을 활성화 또는 비활성화하려면 AWS 계정

> **최소 권한**
>
> 다음 절차의 단계를 수행하려면 IAM 사용자나 역할에 다음 권한이 있어야 합니다.

- `account:ListRegions` (의 목록 AWS 리전 과 현재 활성화 또는 비활성화 여부를 보는 데 필요).
- `account:EnableRegion`
- `account:DisableRegion`

1. AWS 계정 루트 사용자 또는 최소 권한이 있는 IAM 사용자 또는 역할로 AWS Management Console에 로그인합니다.
2. 창 오른쪽 상단에 있는 계정 이름을 선택한 후 계정을 선택합니다.
3. 계정 페이지에서 AWS 리전 섹션으로 이동합니다.

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

4. 작업 열에 옵션이 AWS 리전 있는 각 항목 옆에서 계정의 사용자가 해당 리전의 리소스를 생성하고 액세스할 수 있도록 할지 여부에 따라 활성화 또는 비활성화를 선택합니다.
5. 확인 메시지가 나타나면 선택을 확인합니다.
6. 변경을 모두 마치고 업데이트를 선택합니다.

AWS CLI & SDKs

다음 AWS CLI 명령 또는 이에 상응하는 AWS SDK 작업을 사용하여 리전 옵트 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 사용자에게 리전 설정 정보를 읽을 수만 있는 권한을 부여하고 다른 사용자에게 읽기 및 쓰기 기능을 부여할 수 있습니다.

다음 예에서는 조직의 지정된 멤버 계정에 리전을 활성화합니다. 사용된 자격 증명은 조직의 관리 계정 또는 계정 관리의 위임된 관리자 계정에서 가져온 것이어야 합니다.

동일한 명령을 사용하여 리전을 비활성화한 다음 enable-region을 disable-region로 교체할 수도 있습니다.

```
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"
  }
```

조직에서 리전 활성화 또는 비활성화

의 멤버 계정에 대해 활성화된 리전을 업데이트하려면 다음 절차의 단계를 AWS Organizations수행합니다.

> **Note**
>
> AWS Organizations 관리형 정책 AWSOrganizationsReadOnlyAccess 또는 AWSOrganizationsFullAccess는 AWS Organizations 콘솔에서 AWS 계정 데이터에 액세

스할 수 있도록 계정 관리 APIs에 액세스할 수 있는 권한을 제공하도록 업데이트됩니다. 업데이트된 관리형 정책을 보려면 조직 AWS 관리형 정책에 대한 업데이트를 참조하세요.

> **Note**
>
> 멤버 계정과 함께 사용할 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 먼저 다음을 수행해야 합니다.
>
> - 조직의 모든 기능을 활성화하여 멤버 계정의 설정을 관리합니다. 이렇게 하면 관리자가 멤버 계정을 제어할 수 있습니다. 이는 조직을 생성할 때 기본적으로 설정됩니다. 조직이 통합 결제로만 설정된 상태에서 모든 기능을 활성화하려는 경우 Enabling all features in your organization를 참조하세요.
> - AWS 계정 관리 서비스에 대해 신뢰할 수 있는 액세스를 활성화합니다. 이를 설정하려면 AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화 섹션을 참조하세요.

AWS Management Console

조직에서 리전을 활성화 또는 비활성화하려면

1. 조직의 관리 계정 자격 증명을 사용하여 AWS Organizations 콘솔에 로그인합니다.
2. AWS 계정 페이지에서 업데이트하려는 계정을 선택합니다.
3. 계정 설정 탭을 선택합니다.
4. 리전에서 활성화 또는 비활성화할 리전을 선택합니다.
5. 작업 을 선택한 다음 활성화 또는 비활성화 옵션을 선택합니다.
6. 활성화 옵션을 선택한 경우 표시된 텍스트를 검토한 다음 리전 활성화를 선택합니다.
7. 비활성화 옵션을 선택한 경우 표시된 텍스트를 검토하고 비활성화를 입력하여 확인한 다음 리전 비활성화를 선택합니다.

AWS CLI & SDKs

다음 AWS CLI 명령 또는 이에 상응하는 AWS SDK 작업을 사용하여 조직 멤버 계정에 대한 리전 옵트 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 사용자에게 리전 설정 정보를 읽을 수만 있는 권한을 부여하고 다른 사용자에게 읽기 및 쓰기 기능을 부여할 수 있습니다.

다음 예에서는 조직의 지정된 멤버 계정에 리전을 활성화합니다. 사용된 자격 증명은 조직의 관리 계정 또는 계정 관리의 위임된 관리자 계정에서 가져온 것이어야 합니다.

동일한 명령을 사용하여 리전을 비활성화한 다음 enable-region을 disable-region로 교체할 수도 있습니다.

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

성공 시 이 명령은 출력을 생성하지 않습니다.

> **Note**
>
> 조직은 지정된 시간에 최대 20개의 리전 요청만 가질 수 있습니다. 그렇지 않으면 TooManyRequestsException을 수신할 수 있습니다.

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"
}
```

에 대한 결제 업데이트 AWS 계정

AWS Billing 및 Cost Management 콘솔을 사용하여 모든 AWS 계정 결제 기본 설정을 업데이트할 수 있습니다. 계정의 결제 관련 설정을 업데이트하는 방법을 알아보려면 AWS 결제 및 비용 관리 사용 설명서를 참조하세요.

루트 사용자 이메일 주소 업데이트

의 루트 사용자 이메일 주소 업데이트해야 하는 다양한 비즈니스 이유가 있습니다 AWS 계정. 보안 및 관리 복원력을 예로 들 수 있습니다. 이 주제에서는 독립형 계정과 멤버 계정 모두에 대한 루트 사용자 이메일 주소 업데이트하는 프로세스를 안내합니다.

> **Note**
>
> 에 대한 변경 사항이 모든 곳에 전파되는 데 최대 4시간이 걸릴 AWS 계정 수 있습니다.

루트 사용자 이메일은 계정이 독립 실행형인지 아니면 조직의 일부인지에 따라 다르게 업데이트할 수 있습니다.

- 독립 실행형 AWS 계정 - 조직과 연결 AWS 계정 되지 않은 경우 AWS 관리 콘솔을 사용하여 루트 사용자 emailAmazon 업데이트할 수 있습니다. 이 작업을 수행하는 방법을 알아보려면 독립형에 대한 루트 사용자 emailAmazon 업데이트를 참조하세요 AWS 계정.
- AWS 계정 조직 내 - AWS 조직의 일부인 멤버 계정의 경우 관리 계정 또는 위임된 관리자 계정의 사용자는 AWS Organizations 콘솔에서 또는 AWS CLI 및 SDK를 통해 프로그래밍 방식으로 멤버 계정의 루트 사용자 이메일 중앙에서 업데이트할 수 있습니다. SDKs 이 작업을 수행하는 방법을 알아보려면 조직의 모든에 대한 루트 사용자 emailAmazon 업데이트를 참조 AWS 계정 하세요.

주제

- 독립형에 대한 루트 사용자 이메일 업데이트 AWS 계정
- 조직의 모든 AWS 계정 에 대한 루트 사용자 emailAmazon 업데이트

독립형에 대한 루트 사용자 이메일 업데이트 AWS 계정

독립 실행형의 루트 사용자 이메일 주소 편집하려면 다음 절차의 단계를 AWS 계정수행합니다.

AWS Management Console

> **Note**
>
> 추가 IAM 권한이 AWS 계정 루트 사용자필요하지 않은 로 로그인해야 합니다. IAM 사용자 또는 역할로는 이 단계를 수행할 수 없습니다.

1. AWS 계정의 이메일 주소와 암호를 사용하여에 AWS Management Console로 로그인합니다 AWS 계정 루트 사용자.
2. 콘솔의 오른쪽 상단 모서리 부분에서 계정 이름이나 번호를 선택한 후 계정을 선택합니다.
3. 계정 페이지의 계정 세부 정보 옆에 있는 작업을 선택한 다음 이메일 주소 및 암호 업데이트를 선택합니다.
4. 계정 세부 정보 페이지의 이메일 주소 옆에 있는 편집을 선택합니다.
5. 계정 이메일 편집 페이지에서 새 이메일 주소, 새 이메일 주소 확인 및 현재 암호 확인 필드를 작성합니다. 그런 다음 저장 후 계속을 선택합니다. `no-reply@verify.signin.aws`에서 새 이메일 주소로 확인 코드가 전송됩니다.
6. 계정 이메일 편집 페이지의 확인 코드에서 이메일에서 받은 코드를 입력한 다음 업데이트 확인을 선택합니다.

> **Note**
>
> 확인 코드가 도착하는 데 최대 5분이 걸릴 수 있습니다. 받은편지함으로 이메일이 오지 않았다면 스팸 및 정크 폴더를 확인합니다.

AWS CLI & SDKs

이 작업은 AWS CLI 또는 AWS SDKs. 이 작업은를 사용해야만 수행할 수 있습니다 AWS Management Console.

조직의 모든 AWS 계정 에 대한 루트 사용자 emailAmazon 업데이트

AWS Organizations 콘솔을 사용하여 조직의 멤버 계정에 대한 루트 사용자 이메일 주소 편집하려면 다음 절차의 단계를 수행합니다.

> **Note**
>
> 멤버 계정의 루트 사용자 이메일 주소 업데이트하기 전에이 작업의 영향을 이해하는 것이 좋습니다. 자세한 내용은 AWS Organizations 사용 설명서의를 사용하여 멤버 계정의 루트 사용자 이메일 주소A 업데이트를 AWS Organizations 참조하세요.

루트 사용자로 로그인한 후의 계정 페이지에서 멤버 계정의 루트 사용자 이메일 주소 직접 업데이트할 수도 있습니다. AWS Management Console step-by-step 지침은에 제공된 단계를 따릅니다독립형에 대한 루트 사용자 이메일 업데이트 AWS 계정.

AWS Management Console

> **Notes**
>
> - 멤버 계정에 대해 조직의 관리 계정 또는 위임된 관리자 계정에서 이 절차를 수행하려면 Account Management 서비스에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다.
> - 이 절차를 사용하여 작업을 호출하는 데 사용하는 것과 다른 조직의 계정에 액세스할 수 없습니다.

콘솔을 사용하여 AWS Organizations 멤버 계정의 루트 사용자 이메일 주소 업데이트하려면

1. AWS Organizations 콘솔에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 루트 사용자(권장되지 않음)로 로그인해야 합니다.
2. AWS 계정 페이지에서 루트 사용자 이메일 주소 업데이트할 멤버 계정을 선택합니다.
3. 계정 세부 정보 섹션에서 작업 버튼을 선택한 다음 이메일 주소 업데이트를 선택합니다.
4. 이메일에서 루트 사용자의 새 이메일 주소를 입력한 다음 저장을 선택합니다. 그러면 일회용 암호(OTP)가 새 이메일 주소로 전송됩니다.

> **Note**
>
> 코드를 기다리는 동안 Organizations 콘솔에서 이 페이지를 닫아야 하는 경우 코드를 보낸 후 24시간 이내에 OTP 프로세스를 반환하고 완료할 수 있습니다. 이렇게 하려면 계정 세부 정보 페이지에서 작업 버튼을 선택한 다음 이메일 업데이트 완료를 선택합니다.

5. 검증 코드에 이전 단계에서 새 이메일 주소로 전송된 코드를 입력한 다음 확인을 선택합니다. 이렇게 하면 계정의 루트 사용자에게 업데이트가 커밋됩니다.

AWS CLI & SDKs

다음 AWS CLI 명령 또는 이에 상응하는 AWS SDK 작업을 사용하여 루트 사용자 이메일 주소(기본 이메일 주소라고도 함)를 검색하거나 업데이트할 수 있습니다.

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

> **Notes**
>
> - 멤버 계정에 대해 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 Account Management 서비스에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다.
> - 작업을 호출하는 데 사용하는 것과 다른 조직의 계정에 액세스할 수 없습니다.

> **최소 권한**
>
> 각 작업의 경우 해당 작업에 매핑하는 다음 권한이 있어야 합니다.
>
> - `account:GetPrimaryEmail`
> - `account:StartPrimaryEmailUpdate`
> - `account:AcceptPrimaryEmailUpdate`

이러한 개별 권한을 사용하는 경우 일부 사용자에게 루트 사용자 이메일 주소 정보만 읽을 수 있는 권한을 부여하고 다른 사용자에게 읽기 및 쓰기 기능을 모두 부여할 수 있습니다.

루트 사용자 이메일 주소 프로세스를 완료하려면 아래 예제에 표시된 순서대로 기본 이메일 APIs를 함께 사용해야 합니다.

Example **`GetPrimaryEmail`**

다음 예시에서는 조직의 지정된 멤버 계정에서 루트 사용자 이메일 주소 검색합니다. 사용된 자격 증명은 조직의 관리 계정 또는 계정 관리의 위임된 관리자 계정에서 가져온 것이어야 합니다.

```
$ aws account get-primary-email --account-id 123456789012
```

Example **`StartPrimaryEmailUpdate`**

다음 예시에서는 루트 사용자 이메일 주소 업데이트 프로세스를 시작하고, 새 이메일 주소를 식별하고, 조직의 지정된 멤버 계정에 대한 새 이메일 주소로 일회용 암호(OTP)를 보냅니다. 사용된 보안 인증 정보는 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email
 john@examplecorp.com
```

Example **`AcceptPrimaryEmailUpdate`**

다음 예제에서는 OTP 코드를 수락하고 조직의 지정된 멤버 계정으로 새 이메일 주소를 설정합니다. 사용된 보안 인증 정보는 조직의 관리 계정 또는 Account Management의 위임된 관리자 계정에서 가져온 것이어야 합니다.

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

루트 사용자 암호 업데이트

AWS 계정루트 사용자 암호를 편집하려면 다음 절차의 단계를 수행합니다.

AWS Management Console

루트 사용자 암호를 편집하려면

> **Note**
>
> 추가 IAM 권한이 AWS 계정 루트 사용자필요하지 않은 로 로그인해야 합니다. IAM 사용자 또는 역할로는 이 단계를 수행할 수 없습니다.

1. AWS 계정의 이메일 주소와 암호를 사용하여에 AWS Management Console로 로그인합니다 AWS 계정 루트 사용자.
2. 콘솔의 오른쪽 상단 모서리 부분에서 계정 이름이나 번호를 선택한 후 계정을 선택합니다.
3. 계정 페이지의 계정 세부 정보 옆에 있는 작업을 선택한 다음 이메일 주소 및 암호 업데이트를 선택합니다.
4. 계정 세부 정보 페이지의 암호 옆에 있는 편집을 선택합니다.
5. 암호 편집 페이지에서 현재 암호, 새 암호 및 새 암호 확인 필드를 입력합니다. 그런 다음 암호 업데이트를 선택합니다. 루트 사용자 비밀번호 설정에 대한 모범 사례를 포함한 추가 지침은 IAM User Guide의 Change the password for the AWS 계정 루트 사용자을 참조하세요.

AWS CLI & SDKs

이 작업은 AWS CLI 또는 AWS SDKs. 이 작업은를 사용해야만 수행할 수 있습니다 AWS Management Console.

AWS 계정 이름 업데이트

여러을 관리할 때는 식별 및 정리를 위해 사업부 및 애플리케이션에 맞는 명확한 이름 지정 규칙을 AWS 계정사용합니다. 재구성, 합병, 인수 또는 명명 규칙 업데이트 중에 일관된 식별 및 관리 표준을 유지하기 위해 계정 이름을 변경해야 할 수 있습니다.

계정 이름은 인보이스, Billing and Cost Management 대시보드 및 콘솔과 같은 콘솔과 같은 여러 위치에 표시됩니다 AWS Organizations . 계정 이름을 쉽게 인식할 수 있도록 표준 방법을 사용하여 계정 이름을 지정하는 것이 좋습니다. 회사 계정의 경우 조직 목적 환경(예: sales-catalog-prod)과 같은 이름 지정 표준을 사용하는 것이 좋습니다. 개인 정보 보호 및 보안상의 이유로 개인 식별 정보(PII)를 반영하는 계정 이름을 사용하지 마세요.

- 독립 실행형 AWS 계정 - 조직과 연결 AWS 계정 되지 않은 경우 AWS Management Console또는 AWS CLI 및 SDKs. 이 작업을 수행하는 방법은 독립 실행형의 계정 이름 업데이트 AWS 계정 섹션을 참조하세요.
- AWS 계정 조직 내 -의 일부인 멤버 계정의 경우 관리 계정 또는 위임된 관리자 계정의 AWS Organizations사용자는 AWS Organizations 콘솔에서 또는 AWS CLI 및 SDKs. 이 작업을 수행하는 방법은 조직 AWS 계정 내의 계정 이름 업데이트 섹션을 참조하세요.

> **Note**
>
> 에 대한 변경 사항이 모든 곳에 전파되는 데 최대 4시간이 걸릴 AWS 계정 수 있습니다.

주제

독립 실행형의 계정 이름 업데이트 AWS 계정

독립 실행형의 계정 이름을 변경하려면 다음 절차의 단계를 AWS 계정수행합니다.

AWS Management Console

> **최소 권한**
>
> 루트 사용자, IAM 사용자 또는 IAM 역할을 사용하여 계정 이름을 업데이트할 수 있습니다. 루트 사용자를 사용하는 경우 계정 이름을 업데이트하는 데 추가 IAM 권한이 필요하지 않습니다. IAM 사용자 또는 IAM 역할을 사용하는 경우 최소한 다음 IAM 권한이 있어야 합니다.
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

독립 실행형 계정의 계정 이름을 업데이트하려면

1. AWS 계정의 이메일 주소와 암호를 사용하여에 AWS Management Console로 로그인합니다 AWS 계정 루트 사용자.

2. 콘솔의 오른쪽 상단 모서리 부분에서 계정 이름이나 번호를 선택한 후 계정을 선택합니다.
3. 계정 페이지의 계정 세부 정보 옆에 있는 작업을 선택한 다음 계정 이름 업데이트를 선택합니다.
4. 이름에서 업데이트하려는 새 계정 이름을 입력한 다음 저장을 선택합니다.

AWS CLI & SDKs

> **최소 권한**
>
> 루트 사용자, IAM 사용자 또는 IAM 역할을 사용하여 계정 이름을 업데이트할 수 있습니다. 다음 단계를 수행하려면 IAM 사용자 또는 IAM 역할에 최소한 다음 IAM 권한이 있어야 합니다.
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

독립 실행형 계정의 계정 이름을 업데이트하려면

다음 작업 중 하나를 사용할 수 있습니다.

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

조직 AWS 계정 내의 계정 이름 업데이트

모든 기능 모드가 AWS Organizations 있는 에서는 관리 계정과 위임된 관리자 계정 모두에서 권한이 부여된 IAM 사용자 또는 IAM 역할이 계정 이름을 중앙에서 관리할 수 있습니다.

조직의 멤버 계정의 계정 이름을 변경하려면 다음 절차의 단계를 수행합니다.

요구 사항

AWS Organizations 콘솔을 사용하여 계정 이름을 업데이트하려면 몇 가지 예비 설정을 수행해야 합니다.

- 조직에서 멤버 계정의 설정을 관리하려면 모든 기능을 활성화해야 합니다. 이렇게 하면 관리자가 멤버 계정을 제어할 수 있습니다. 이는 조직을 생성할 때 기본적으로 설정됩니다. 조직이 통합 결제로만 설정되어 있고 모든 기능을 활성화하려는 경우 조직의 모든 기능 활성화를 참조하세요.
- AWS 계정 관리 서비스에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다. 이를 설정하려면 AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화 섹션을 참조하세요.

AWS Management Console

> **최소 권한**
>
> 멤버 계정의 계정 이름을 업데이트하려면 IAM 사용자 또는 IAM 역할에 다음 권한이 있어야 합니다.
>
> - `organizations:DescribeOrganization`(콘솔 전용)
> - `account:PutAccountName`

멤버 계정의 계정 이름을 업데이트하려면

1. https://console.aws.amazon.com/organizations/에서 Organizations 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 AWS 계정를 선택합니다.
3. AWS 계정 페이지에서 업데이트할 멤버 계정을 선택하고 작업 드롭다운 메뉴를 선택한 다음 계정 이름 업데이트를 선택합니다.
4. 이름에서 업데이트된 이름을 입력하고 저장을 선택합니다.

AWS CLI & SDKs

> **최소 권한**
>
> 멤버 계정의 계정 이름을 업데이트하려면 IAM 사용자 또는 IAM 역할에 다음 권한이 있어야 합니다.
>
> - `organizations:DescribeOrganization`(콘솔 전용)

- `account:PutAccountName`

멤버 계정의 계정 이름을 업데이트하려면

다음 작업 중 하나를 사용할 수 있습니다.

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-id 111111111111 \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

의 대체 연락처 업데이트 AWS 계정

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

계정과 연결된 다음 각 연락 유형 중 하나만 지정할 수 있습니다.

- 결제 연락처
- 운영 연락처
- 보안 연락처

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

- 독립 실행형 AWS 계정 - 조직과 연결 AWS 계정 되지 않은 경우 AWS 관리 콘솔을 사용하거나 AWS CLI 및 SDKs. 이 작업을 수행하는 방법을 알아보려면 독립 실행형의 대체 연락처 업데이트를 참조하세요 AWS 계정.
- AWS 계정 조직 내 - AWS 조직의 일부인 멤버 계정의 경우 관리 계정 또는 위임된 관리자 계정의 사용자는 AWS Organizations 콘솔에서 조직의 모든 멤버 계정을 중앙에서 업데이트하거나 AWS CLI

및 SDKs. 이 작업을 수행하는 방법을 알아보려면 조직의 모든에 대한 대체 연락처 업데이트를 참조 AWS 계정 하세요.

주제

전화번호 및 이메일 주소 요구 사항

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

- 전화번호는 숫자, 공백 및 "+-()" 문자만 포함할 수 있습니다.
- 이메일 주소는 최대 254자까지 입력할 수 있으며 표준 영숫자 문자 외에도 이메일 주소의 로컬 부분에 "+=.#|!&-_" 특수 문자를 포함할 수 있습니다.

독립 실행형의 대체 연락처 업데이트 AWS 계정

독립 실행형의 대체 연락처를 추가하거나 편집하려면 다음 절차의 단계를 AWS 계정수행합니다. 아래 AWS Management Console 절차는 항상 독립 실행형 컨텍스트에서만 작동합니다. 를 사용하여 작업을 호출 AWS Management Console 하는 데 사용한 계정의 대체 연락처에만 액세스하거나 변경할 수 있습니다.

AWS Management Console

독립 실행형 AWS 계정에 대한 대체 연락처를 추가하거나 편집하려면

> 최소 권한
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - `account:GetAlternateContact`(대체 연락처 세부 정보를 보려면)
> - `account:PutAlternateContact`(대체 연락처를 설정하거나 업데이트하려면)

- `account:DeleteAlternateContact`(대체 연락처를 삭제하려면)

1. 최소 권한이 있는 IAM 사용자 또는 역할로 AWS Management Console에 로그인합니다.
2. 창 오른쪽 상단에 있는 계정 이름을 선택한 후 계정을 선택합니다.
3. 계정 페이지에서 대체 연락처로 스크롤하고 제목 오른쪽에서 편집을 선택합니다.

> **Note**
>
> Edit 옵션이 나타나지 않으면 계정의 루트 사용자나 위에 지정된 최소 권한이 있는 사용자로 로그인하지 않은 것일 수 있습니다.

4. 사용 가능한 모든 필드의 값을 변경합니다.

> **Important**
>
> 비즈니스의 경우 개인 소유가 아닌 회사 전화번호와 이메일 주소를 입력하는 AWS 계정것이 가장 좋습니다.

5. 변경을 모두 마치고 업데이트를 선택합니다.

AWS CLI & SDKs

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

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

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

최소 권한

각 작업의 경우 해당 작업에 매핑하는 다음 권한이 있어야 합니다.

- `GetAlternateContact`(대체 연락처 세부 정보를 보려면)
- `PutAlternateContact`(대체 연락처를 설정하거나 업데이트하려면)
- `DeleteAlternateContact`(대체 연락처를 삭제하려면)

이러한 개별 권한을 사용하는 경우 일부 사용자에게 연락처 정보를 읽을 수만 있는 권한을 부여하고 다른 사용자에게 읽기 및 쓰기 기능을 부여할 수 있습니다.

Example

다음 예에서는 호출자 계정의 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 예에서는 호출자 계정의 새 작업 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**
>
> 동일한 고객 응대 유형 AWS 계정 과 동일한 고객 응대 유형에서 여러 `PutAlternateContact` 작업을 수행하는 경우는 먼저 새 고객 응대를 추가하고, 동일한 AWS 계정 및 고객 응대 유형에 대한 모든 연속 호출은 기존 고객 응대를 업데이트합니다.

Example

다음 예에서는 호출자 계정의 보안 대체 연락처를 삭제합니다.

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

성공 시 이 명령은 출력을 생성하지 않습니다.

> **Note**
>
> 동일한 연락처를 두 번 이상 삭제하려고 하면 첫 번째 삭제가 자동으로 성공합니다. 이후의 모든 시도는 `ResourceNotFound` 예외를 생성합니다.

조직의 모든 AWS 계정 에 대한 대체 연락처 업데이트

조직의 AWS 계정 에 대한 대체 연락처 세부 정보를 추가하거나 편집하려면 다음 절차의 단계를 수행합니다.

요구 사항

AWS Organizations 콘솔을 사용하여 대체 연락처를 업데이트하려면 몇 가지 예비 설정을 수행해야 합니다.

- 조직에서 멤버 계정의 설정을 관리하려면 모든 기능을 활성화해야 합니다. 이렇게 하면 관리자가 멤버 계정을 제어할 수 있습니다. 이는 조직을 생성할 때 기본적으로 설정됩니다. 조직이 통합 결제로만 설정되어 있고 모든 기능을 활성화하려는 경우 조직의 모든 기능 활성화를 참조하세요.
- AWS 계정 관리 서비스에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다. 이를 설정하려면 AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화 섹션을 참조하세요.

> **Note**
>
> AWS Organizations 관리형 정책 `AWSOrganizationsReadOnlyAccess` 또는 `AWSOrganizationsFullAccess`는 콘솔에서 AWS 계정 데이터에 액세스할 수 있도록 계정 관리 APIs에 AWS Organizations 액세스할 수 있는 권한을 제공하도록 업데이트됩니다. 업데이트된 관리형 정책을 보려면 조직 AWS 관리형 정책에 대한 업데이트를 참조하세요.

AWS Management Console

조직의 AWS 계정 에 대한 대체 연락처를 추가하거나 편집하려면

1. 조직 관리 계정의 자격 증명을 사용하여 AWS Organizations 콘솔에 로그인합니다.
2. AWS 계정에서 업데이트하려는 계정을 선택합니다.
3. 연락처 정보를 선택하고 대체 연락처에서 연락처 유형인 결제 연락처, 보안 연락처 또는 운영 연락처를 찾습니다.
4. 새 연락처를 추가하려면 추가를 선택하고 기존 연락처를 업데이트하려면 편집을 선택합니다.
5. 사용 가능한 모든 필드의 값을 변경합니다.

   > **Important**
   >
   > 비즈니스의 경우 개인 소유가 아닌 회사 전화번호와 이메일 주소를 입력하는 AWS 계정것이 가장 좋습니다.

6. 변경을 모두 마치고 업데이트를 선택합니다.

AWS CLI & SDKs

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

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Notes**
>
> - 멤버 계정을 대상으로 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 계정 서비스에 신뢰할 수 있는 액세스를 활성화해야 합니다.
> - 작업을 호출하는 데 사용하는 것과 다른 조직의 계정에 액세스할 수 없습니다.

> **최소 권한**
>
> 각 작업의 경우 해당 작업에 매핑하는 다음 권한이 있어야 합니다.
>
> - `GetAlternateContact`(대체 연락처 세부 정보를 보려면)
> - `PutAlternateContact`(대체 연락처를 설정하거나 업데이트하려면)
> - `DeleteAlternateContact`(대체 연락처를 삭제하려면)
>
> 이러한 개별 권한을 사용하는 경우 일부 사용자에게 연락처 정보를 읽을 수만 있는 권한을 부여하고 다른 사용자에게 읽기 및 쓰기 기능을 부여할 수 있습니다.

Example

다음 예에서는 조직에 있는 호출자 계정의 현재 결제 대체 연락처를 검색합니다. 사용된 자격 증명은 조직의 관리 계정 또는 계정 관리의 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 조직에 있는 지정된 멤버 계정의 작업 대체 연락처를 설정합니다. 사용된 자격 증명은 조직의 관리 계정 또는 계정 관리의 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**
>
> 동일한 고객 응대 유형 AWS 계정 과 동일한 고객 응대 유형에서 여러 `PutAlternateContact` 작업을 수행하는 경우는 먼저 새 고객 응대를 추가하고, 동일한 AWS 계정 및 고객 응대 유형에 대한 모든 연속 호출은 기존 고객 응대를 업데이트합니다.

Example

다음 예에서는 조직에 있는 지정된 멤버 계정의 보안 대체 연락처를 삭제합니다. 사용된 자격 증명은 조직의 관리 계정 또는 계정 관리의 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 삭제가 자동으로 성공합니다. 이후의 모든 시도는 `ResourceNotFound` 예외를 생성합니다.

account:AlternateContactTypes 컨텍스트 키

`account:AlternateContactTypes` 컨텍스트 키를 사용하여 IAM 정책에서 허용되는(또는 거부되는) 세 가지 결제 유형을 지정할 수 있습니다. 예를 들어, 다음 예의 IAM 권한 정책은 이 조건 키를 사용하여 연결된 위탁자가 조직에 있는 특정 계정의 `BILLING` 대체 연락처만 검색하고 수정하지 않도록 허용합니다.

`account:AlternateContactTypes`는 다중 값 문자열 유형이므로 [ForAnyValue 또는 ForAllValues 다중 값 문자열 연산자](#) 를 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"
                    ]
                }
            }
        }
    ]
}
```

AWS 계정의 기본 연락처 업데이트

연락처의 전체 이름, 회사 이름, 우편 주소, 전화번호, 웹 사이트 주소 등 계정에 연결된 연락처 정보를 업데이트할 수 있습니다.

계정이 독립 실행형인지 아니면 조직의 일부인지에 따라 기본 계정 연락처를 다르게 편집합니다.

- 독립 실행형 AWS 계정 - 조직과 연결 AWS 계정 되지 않은 경우 AWS 관리 콘솔을 사용하거나 AWS CLI 및 SDKs. 이 작업을 수행하는 방법을 알아보려면 독립 실행형 AWS 계정 기본 연락처 업데이트를 참조하세요.
- AWS 계정 조직 내 - AWS 조직의 일부인 멤버 계정의 경우 관리 계정 또는 위임된 관리자 계정의 사용자는 AWS Organizations 콘솔에서 조직의 모든 멤버 계정을 중앙에서 업데이트하거나 AWS CLI 및 SDKs. 이 작업을 수행하는 방법을 알아보려면 조직의 AWS 계정 기본 연락처 업데이트를 참조하세요.

주제

전화번호 및 이메일 주소 요구 사항

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

- 전화번호는 숫자만 포함해야 합니다.
- 전화번호는 + 및 국가 코드로 시작해야 하며 국가 코드 뒤에 앞자리 0 또는 추가 공백이 없어야 합니다. 예: +1(미국/캐나다) 또는 +44(영국).
- 전화번호에는 지역 코드, 교환 코드 및 로컬 코드 사이에 하이픈 또는 공백 "-"이 포함되어서는 안 됩니다. 예: +12025550179.
- 보안을 위해 전화번호는 AWS에서 SMS를 수신할 수 있어야 합니다. 대부분의 수신자 부담 전화번호는 SMS를 지원하지 않으므로 허용되지 않습니다.
- 비즈니스의 경우 개인 소유가 아닌 회사 전화번호와 이메일 주소를 입력하는 AWS 계정것이 가장 좋습니다. 개인의 이메일 주소 또는 전화번호로 계정 루트 사용자를 구성하면 해당 개인이 회사를 떠날 경우 계정을 복구하기 어려울 수 있습니다.

독립 실행형의 기본 연락처 업데이트 AWS 계정

독립 실행형의 기본 연락처 세부 정보를 편집하려면 다음 절차의 단계를 AWS 계정수행합니다. 아래 AWS Management Console 절차는 항상 독립 실행형 컨텍스트에서만 작동합니다. 를 사용하여 작업을 호출 AWS Management Console 하는 데 사용한 계정의 기본 연락처 정보에만 액세스하거나 변경할 수 있습니다.

AWS Management Console

독립 실행형 AWS 계정의 기본 연락처를 편집하려면

> 최소 권한
>
> 다음 단계를 수행하려면 적어도 다음과 같은 IAM 권한이 있어야 합니다.
>
> - `account:GetContactInformation`(기본 연락처 세부 정보를 보려면)
> - `account:PutContactInformation`(기본 연락처 세부 정보를 업데이트하려면)

1. 최소 권한이 있는 IAM 사용자 또는 역할로 AWS Management Console에 로그인합니다.
2. 창 오른쪽 상단에 있는 계정 이름을 선택한 후 계정을 선택합니다.
3. 아래로 스크롤하여 연락처 정보 섹션으로 이동한 다음 옆에 있는 편집을 선택합니다.
4. 사용 가능한 모든 필드의 값을 변경합니다.
5. 변경을 모두 마치고 업데이트를 선택합니다.

AWS CLI & SDKs

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

- GetContactInformation
- PutContactInformation

Notes

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

최소 권한

각 작업의 경우 해당 작업에 매핑하는 다음 권한이 있어야 합니다.

- `account:GetContactInformation`
- `account:PutContactInformation`

이러한 개별 권한을 사용하는 경우 일부 사용자에게 연락처 정보를 읽을 수만 있는 권한을 부여하고 다른 사용자에게 읽기 및 쓰기 기능을 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 호출자 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.

조직의 모든 AWS 계정 에 대한 기본 연락처 업데이트

조직의 AWS 계정 에서 기본 연락처 세부 정보를 편집하려면 다음 절차의 단계를 수행합니다.

추가 요구 사항

AWS Organizations 콘솔을 사용하여 기본 연락처를 업데이트하려면 몇 가지 예비 설정을 수행해야 합니다.

- 조직에서 멤버 계정의 설정을 관리하려면 모든 기능을 활성화해야 합니다. 이렇게 하면 관리자가 멤버 계정을 제어할 수 있습니다. 이는 조직을 생성할 때 기본적으로 설정됩니다. 조직이 통합 결제로만 설정되어 있고 모든 기능을 활성화하려는 경우 조직의 모든 기능 활성화를 참조하세요.
- AWS 계정 관리 서비스에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다. 이를 설정하려면 AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화 섹션을 참조하세요.

AWS Management Console

조직의 AWS 계정 에 대한 기본 연락처를 편집하려면

1. 조직 관리 계정의 자격 증명을 사용하여 AWS Organizations 콘솔에 로그인합니다.
2. AWS 계정에서 업데이트하려는 계정을 선택합니다.
3. 연락처 정보를 선택하고 기본 연락처를 찾습니다.
4. 편집을 선택합니다.
5. 사용 가능한 모든 필드의 값을 변경합니다.
6. 변경을 모두 마치고 업데이트를 선택합니다.

AWS CLI & SDKs

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

- GetContactInformation
- PutContactInformation

> **Notes**
>
> - 멤버 계정을 대상으로 조직의 관리 계정 또는 위임된 관리자 계정에서 이러한 작업을 수행하려면 계정 서비스에 신뢰할 수 있는 액세스를 활성화해야 합니다.
> - 작업을 호출하는 데 사용하는 것과 다른 조직의 계정에 액세스할 수 없습니다.

> **최소 권한**
>
> 각 작업의 경우 해당 작업에 매핑하는 다음 권한이 있어야 합니다.
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> 이러한 개별 권한을 사용하는 경우 일부 사용자에게 연락처 정보를 읽을 수만 있는 권한을 부여하고 다른 사용자에게 읽기 및 쓰기 기능을 부여할 수 있습니다.

Example

다음 예에서는 조직의 지정된 멤버 계정에 대한 현재 기본 연락처 정보를 검색합니다. 사용된 자격 증명은 조직의 관리 계정 또는 계정 관리의 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 멤버 계정에 대한 기본 연락처 정보를 설정합니다. 사용된 자격 증명은 조직의 관리 계정 또는 계정 관리의 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.

AWS 계정 식별자 보기

AWS 는 AWS 계정각각에 다음과 같은 고유 식별자를 할당합니다.

AWS 계정 ID

AWS 계정을 고유하게 식별하는 12자리 숫자(예: 012345678901)입니다. 많은 AWS 리소스에는 Amazon 리소스 이름(ARNs)에 계정 ID가 포함됩니다. 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 사용하여에 로그인할 수 있습니다. 계정 ID 식별 정보와 마찬가지로 신중하게 사용하고 공유해야 하지만 비밀, 민감한 또는 기밀 정보로 간주되지 않습니다.

정식 사용자 ID

난독화된 AWS 계정 ID 형식79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be인와 같

은 영숫자 식별자입니다. Amazon Simple Storage Service(Amazon S3)를 사용하여 버킷 및 객체에 대한 교차 계정 액세스 권한을 부여할 AWS 계정 때이 ID를 사용하여를 식별할 수 있습니다. 루트 사용자 또는 IAM 사용자로 AWS 계정 의 정식 사용자 ID를 검색할 수 있습니다.

이러한 식별자 AWS 를 보려면 로 인증해야 합니다.

> **Warning**
>
> AWS 리소스를 공유하기 위해 AWS 계정 식별자가 필요한 타사에 AWS 자격 증명(암호 및 액세스 키 포함)을 제공하지 마십시오. 이렇게 하면 사용자가 보유한 AWS 계정 에 동일한 액세스 권한을 부여할 수 있습니다.

AWS 계정 ID 찾기

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

루트 사용자로 계정 ID 찾기

AWS Management Console

루트 사용자로 로그인할 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 모음에서 계정 이름 또는 번호를 선택한 다음 내 보안 자격 증명을 선택합니다.

> **Tip**
>
> Security credentials 옵션이 표시되지 않으면 IAM 사용자 대신 IAM 역할을 가진 페더레이션 사용자로 로그인한 것일 수 있습니다. 이 경우 옆에 있는 항목 계정과 계정 ID 번호를 찾습니다.

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

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 사용합니다.

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

IAM 사용자로 계정 ID 찾기

AWS Management Console

IAM 사용자로 로그인할 때 AWS 계정 ID를 찾으려면

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

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

   > **Tip**
   >
   > Security credentials 옵션이 표시되지 않으면 IAM 사용자 대신 IAM 역할을 가진 페더레이션 사용자로 로그인한 것일 수 있습니다. 이 경우 옆에 있는 항목 계정과 계정 ID 번호를 찾습니다.

2. 페이지 상단의 계정 세부 정보 아래에 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.
>
> - IAM 사용자 또는 역할로 명령을 실행할 때 다음 사항이 있어야 합니다.
>   - `sts:GetCallerIdentity`

다음과 같이 get-caller-identity 명령을 사용합니다.

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

AWS 계정의 정식 사용자 ID 찾기

AWS Management Console 또는를 AWS 계정 사용하여의 정식 사용자 ID를 찾을 수 있습니다 AWS CLI. 의 정식 사용자 ID AWS 계정 는 해당 계정에만 해당됩니다. 루트 사용자, 페더레이션 사용자 또는 IAM 사용자 AWS 계정 로서의 정식 사용자 ID를 검색할 수 있습니다.

루트 사용자 또는 IAM 사용자로 정식 ID 찾기

AWS Management Console

루트 사용자 또는 IAM 사용자로 콘솔에 로그인한 경우 계정의 정식 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 로그인하는 경우 다음이 있어야 합니다.
>   - `account:GetAccountInformation`

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

   > **Tip**
   >
   > Security credentials 옵션이 표시되지 않으면 IAM 사용자 대신 IAM 역할을 가진 페더레이션 사용자로 로그인한 것일 수 있습니다. 이 경우 옆에 있는 항목 계정과 계정 ID 번호를 찾습니다.

3. 계정 세부 정보 섹션에서 정식 사용자 ID가 정식 사용자 ID 옆에 나타납니다. 정식 사용자 ID를 사용하여 Amazon S3 액세스 제어 목록(ACL)을 구성합니다.

AWS CLI & SDKs

를 사용하여 정식 사용자 ID를 찾으려면 AWS CLI

동일한 AWS CLI 및 API 명령은 AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할에 적용됩니다.

다음과 같이 list-buckets 명령을 사용합니다.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
```

```
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

IAM 역할이 있는 페더레이션 사용자로 정식 ID 찾기

AWS Management Console

IAM 역할이 있는 페더레이션 사용자로 로그인할 때 계정의 정식 사용자 ID를 찾으려면

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

1. IAM 역할이 있는 페더레이션 사용자 AWS Management Console 로에 로그인합니다.
2. Amazon S3 콘솔에서 버킷 이름을 선택하여 버킷에 대한 세부 정보를 봅니다.
3. 권한 탭을 선택합니다.
4. 액세스 제어 리스트 섹션에서 버킷 소유자에 AWS 계정 의 정식 사용자 ID가 표시됩니다.

AWS CLI & SDKs

를 사용하여 정식 사용자 ID를 찾으려면 AWS CLI

동일한 AWS CLI 및 API 명령은 AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할에 적용됩니다.

다음과 같이 list-buckets 명령을 사용합니다.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

AWS 계정 관리의 보안

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

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

- 클라우드 보안 -에서 AWS 서비스를 실행하는 인프라를 보호할 AWS 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 규정 AWS 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. 계정 관리에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 서비스 범위 내규정 준수 프로그램 섹션을 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 여러분은 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다

이 설명서는 AWS Account Management를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 보안 및 규정 준수 목표에 맞게 계정 관리를 구성하는 방법을 보여줍니다. 또한 Account Management 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- AWS 계정 관리의 데이터 보호
- AWS PrivateLinkAWS 계정 관리용
- AWS 계정 관리를 위한 자격 증명 및 액세스 관리
- AWSAWS 계정 관리에 대한 관리형 정책
- AWS 계정 관리에 대한 규정 준수 검증
- AWS 계정 관리의 복원력
- 의 인프라 보안 AWS Account Management

AWS 계정 관리의 데이터 보호

AWS 공동 책임 모델 AWS 계정 관리의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사

용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

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

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

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

AWS PrivateLinkAWS 계정 관리용

Amazon Virtual Private Cloud(VPC)를 사용하여 AWS 리소스를 호스팅하는 경우 퍼블릭 인터넷을 통과하지 않고도 VPC 내에서 AWS 계정 관리 서비스에 액세스할 수 있습니다.

Amazon VPC를 사용하면 사용자 지정 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. VPC를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC에 대한 자세한 내용은 Amazon VPC 사용 설명서를 참조하세요.

Amazon VPC를 계정 관리에 연결하려면 먼저 VPC를 다른 AWS 서비스에 연결할 수 있는 인터페이스 VPC 엔드포인트를 정의해야 합니다. 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 참조하십시오.

엔드포인트 만들기

AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK, AWS 계정 관리 API 또는를 사용하여 VPC에서 AWS 계정 관리 엔드포인트를 생성할 수 있습니다 AWS CloudFormation.

Amazon VPC 콘솔 또는를 사용하여 엔드포인트를 생성하고 구성하는 방법에 대한 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 AWS CLI참조하세요.

> **Note**
>
> 엔드포인트를 생성할 때 다음 형식을 사용하여 VPC를 연결할 서비스로 계정 관리를 지정해야 합니다.
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> 표시된 대로 정확히 문자열을 사용하여 `us-east-1` 리전을 지정해야 합니다. 글로벌 서비스인 Account Management는 해당 AWS 리전에서만 호스팅됩니다.

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

Amazon VPC 엔드포인트 정책

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

- 계정 관리를 위한 Amazon Virtual Private Cloud 엔드포인트 정책
- 자세한 내용은 AWS PrivateLink 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

계정 관리를 위한 Amazon Virtual Private Cloud 엔드포인트 정책

계정 관리에 대한 Amazon VPC 엔드포인트 정책을 만들어 다음을 지정할 수 있습니다.

- 작업을 수행할 수 있는 위탁자.
- 위탁자가 수행할 수 있는 작업입니다.
- 작업을 수행할 수 있는 리소스.

다음 예제는 계정 123456789012의 Alice라는 IAM 사용자 한 명이 모든에 대한 대체 연락처 정보를 검색하고 변경할 수 있도록 허용 AWS 계정하지만 모든 계정의 대체 연락처 정보를 삭제할 수 있는 모든 IAM 사용자 권한을 거부하는 Amazon VPC 엔드포인트 정책을 보여줍니다.

```
{
    "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"
        }
    ]
}
```

AWS 조직의 멤버 계정 중 하나에 있는 보안 주체에게 조직의 일부인 계정에 대한 액세스 권한을 부여하려면 Resource 요소가 다음 형식을 사용해야 합니다.

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

엔드포인트 정책 생성에 대한 자세한 내용은 AWS PrivateLink 안내서의 Controlling Access to Services with VPC Endpoints를 참조하세요.

AWS 계정 관리를 위한 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 어떤 사용자가 계정 관리 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 소유)될 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

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

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

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

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

ID를 통한 인증

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

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

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

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

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

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

페더레이션 자격 증명

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

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명 액세스 시 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

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

IAM 사용자 및 그룹

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

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

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

IAM 역할

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

CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에

나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

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

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

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

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

ID 기반 정책

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

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는

독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

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

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

액세스 제어 목록(ACL)

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

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

기타 정책 타입

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

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔

터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.

- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

AWS 계정 관리에서 IAM을 사용하는 방법

IAM을 사용하여 계정 관리에 대한 액세스를 관리하기 전에 계정 관리와 함께 사용할 수 있는 IAM 기능을 알아보세요.

AWS 계정 관리와 함께 사용할 수 있는 IAM 기능

IAM 기능	계정 관리 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예

IAM 기능	계정 관리 지원
ACLs	아니요
ABAC(정책 내 태그)	아니요
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 연결 역할	아니요

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

계정 관리 자격 증명 기반 정책

ID 기반 정책 지원: 예

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

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

계정 관리의 자격 증명 기반 정책 예시

계정 관리 자격 증명 기반 정책의 예를 보려면 AWS 계정 관리에 대한 자격 증명 기반 정책 예제 섹션을 참조하세요.

계정 관리 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

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

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

계정 관리의 정책 작업

정책 작업 지원: 예

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

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

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

계정 관리 작업 목록을 보려면 서비스 승인 참조의 AWS 계정 관리에서 정의한 작업을 참조하세요.

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 계정의 대체 연락처로 작동하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

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

계정 관리 자격 증명 기반 정책의 예를 보려면 AWS 계정 관리에 대한 자격 증명 기반 정책 예제 섹션을 참조하세요.

계정 관리를 위한 정책 리소스

정책 리소스 지원: 예

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

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

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

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

계정 관리 서비스는 IAM 정책의 `Resources` 요소에서 AWS 계정다음과 같은 특정 리소스 유형을 지원하므로 정책을 필터링하고 이러한 유형 간에 구별할 수 있습니다.

- account

  이 `resource` 유형은 AWS Organizations 서비스에서 관리하는 조직의 멤버 계정이 아닌 독립 실행형 AWS 계정 만 일치합니다.
- accountInOrganization

  이 `resource` 유형은 AWS Organizations 서비스에서 관리하는 조직의 멤버 계정 AWS 계정 인 만 일치합니다.

계정 관리 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의 AWS 계정 관리에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS 계정 관리에서 정의한 작업을 참조하세요.

계정 관리 자격 증명 기반 정책의 예를 보려면 AWS 계정 관리에 대한 자격 증명 기반 정책 예제 섹션을 참조하세요.

계정 관리에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

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

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

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

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

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

계정 관리 서비스는 IAM 정책에 대한 세분화된 필터링을 제공하는 데 사용할 수 있는 다음과 같은 조건 키를 지원합니다.

- account:TargetRegion

  이 조건 키는 AWS 리전 코드 목록으로 구성된 인수를 가져옵니다. 지정된 리전에 적용되는 작업에만 영향을 미치도록 정책을 필터링할 수 있습니다.

- account:AlternateContactTypes

  이 조건 키는 대체 연락 유형 목록을 가져옵니다.

  - BILLING

  - OPERATIONS
  - SECURITY

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

- account:AccountResourceOrgPaths

  이 조건 키는 조직의 계층 구조에서 특정 조직 단위(OU)까지의 경로 목록으로 구성된 인수를 사용합니다. 이를 통해 일치하는 OU의 대상 계정에만 영향을 미치도록 정책을 필터링할 수 있습니다.

  ```
  o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- account:AccountResourceOrgTags

  이 조건 키는 태그 키 및 값 목록으로 구성된 인수를 가져옵니다. 이로 인해 조직의 멤버이고 지정된 태그 키 및 값으로 태그가 지정된 계정에만 영향을 미치도록 정책을 필터링할 수 있습니다.

계정 관리 조건 키 목록을 보려면 서비스 승인 참조의 AWS 계정 관리에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 AWS 계정 관리에서 정의한 작업을 참조하세요.

계정 관리 자격 증명 기반 정책의 예를 보려면 AWS 계정 관리에 대한 자격 증명 기반 정책 예제 섹션을 참조하세요.

계정 관리 액세스 제어 목록

ACL 지원: 아니요

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

계정 관리에서 속성 기반 액세스 제어(ABAC)

ABAC 지원(정책의 태그): 아니요

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

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

AWS 계정 관리의 경우 태그 기반 액세스 제어는 `account:AccountResourceOrgTags/key-name` 조건 키를 통해서만 지원됩니다. 계정 네임스페이스APIs에는 표준 `aws:ResourceTag/key-name` 조건 키가 지원되지 않습니다.

지원되는 조건 키를 사용하는 JSON 정책 예제

다음 예제 정책은 조직에서 "CostCenter" 키와 "12345" 또는 "67890" 값으로 태그가 지정된 계정의 연락처 정보를 볼 수 있는 액세스를 허용합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "account:GetContactInformation",
            "account:GetAlternateContact"
         ],
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "account:AccountResourceOrgTags/CostCenter":[
                  "12345",
                  "67890"
               ]
            }
         }
      }
   ]
}
```

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여 및 IAM 자습서를 사용하여 속성을 기반으로 권한 정의: 태그를 기반으로 AWS 리소스에 액세스할 수 있는 권한 정의를 참조하세요.

계정 관리에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

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

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

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

계정 관리의 서비스 간 위탁자 권한

전달 액세스 세션(FAS) 지원: 예

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

계정 관리를 위한 서비스 역할

서비스 역할 지원: 아니요

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

계정 관리에 대한 서비스 연결 역할

서비스 링크 역할 지원: 아니요

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

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

AWS 계정 관리에 대한 자격 증명 기반 정책 예제

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

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

각 리소스 유형에 대한 ARNs 형식을 포함하여 Account Management에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS Account Management에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

주제

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

정책 모범 사례

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

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.

- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

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

의 계정 페이지 사용 AWS Management Console

의 계정 페이지에 액세스하려면 최소 권한 집합이 있어야 AWS Management Console합니다. 이러한 권한은에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 보안 인증 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(IAM 사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

사용자와 역할이 계정 관리 콘솔을 사용할 수 있도록 하려면 `AWSAccountManagementReadOnlyAccess` 또는 `AWSAccountManagementFullAccess` AWS 관리형 정책을 엔터티에 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. 그 대신, 대부분의 경우 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 선택할 수 있습니다.

의 계정 페이지에 대한 읽기 전용 액세스 권한 제공 AWS Management Console

다음 예에서는 AWS Management Console의 계정 페이지에 대한 AWS 계정 읽기 전용 액세스 권한을 IAM 사용자에게 부여하려고 합니다. 이 정책이 연결된 사용자는 아무것도 변경할 수 없습니다.

`account:GetAccountInformation` 작업은 계정 페이지에서 대부분의 설정을 볼 수 있는 액세스 권한을 부여합니다. 그러나 현재 활성화된 AWS 리전을 보려면 `account:ListRegions` 작업도 포함해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantReadOnlyAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

의 계정 페이지에 대한 전체 액세스 권한 제공 AWS Management Console

다음 예에서는 AWS 계정 의 IAM 사용자에게 AWS Management Console의 계정 페이지에 대한 전체 액세스 권한을 부여하려고 합니다. 이 정책이 연결된 사용자는 계정의 설정을 변경할 수 있습니다.

이 예제 정책은 사용 가능한 각 쓰기 권한(CloseAccount 제외)을 추가하여 이전 예제 정책을 기반으로 구축하며, 이를 통해 사용자는 `account:EnableRegion` 및 `account:DisableRegion` 권한을 포함한 계정의 대부분의 설정을 변경할 수 있습니다.

```
{
    "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": "*"
        }
```

```
    ]
}
```

AWS 계정 관리에 자격 증명 기반 정책(IAM 정책) 사용

AWS 계정 및 IAM 사용자에 대한 자세한 내용은 IAM 사용 설명서의 IAM이란 무엇입니까?를 참조하세요.

고객 관리형 정책을 업데이트하는 방법에 대한 지침은 IAM 사용 설명서의 IAM 정책 편집을 참조하세요.

AWS 계정 관리 작업 정책

이 표에는 계정 설정에 대한 액세스 권한을 부여하는 권한이 요약되어 있습니다. 이러한 권한을 사용하는 정책의 예는 AWS 계정 관리에 대한 자격 증명 기반 정책 예제단원을 참조하세요.

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

권한 이름	액세스 레벨	설명
`account:ListRegions`	목록	사용 가능한 리전을 나열할 수 있는 권한을 부여합니다.
`account:GetAccountInformation`	읽기	계정에 대한 계정 정보를 검색할 수 있는 권한을 부여합니다.
`account:GetAlternateContact`	읽기	계정의 대체 연락처를 검색할 수 있는 권한을 부여합니다.
`account:GetContactInformation`	읽기	계정의 기본 연락처 정보를 검색하는 권한을 부여합니다.

권한 이름	액세스 레벨	설명
account:GetPrimaryEmail	읽기	계정의 기본 이메일 주소를 검색할 수 있는 권한을 부여합니다.
account:GetRegionOptStatus	읽기	리전의 옵트인 상태를 가져올 수 있는 권한을 부여합니다.
account:AcceptPrimaryEmailUpdate	쓰기	AWS 조직 내 멤버 계정의 기본 이메일 주소 업데이트를 수락할 수 있는 권한을 부여합니다.
account:CloseAccount	쓰기	계정을 해지할 수 있는 권한을 부여합니다. **Note** 이 권한은 콘솔에만 해당합니다. 이 권한으로 이용할 수 있는 API 액세스는 없습니다.
account:DeleteAlternateContact	쓰기	계정의 대체 연락처를 삭제할 수 있는 권한을 부여합니다.
account:DisableRegion	쓰기	리전 사용을 비활성화할 수 있는 권한을 부여합니다.
account:EnableRegion	쓰기	리전 사용을 활성화할 수 있는 권한을 부여합니다.
account:PutAccountName	쓰기	계정의 이름을 업데이트할 수 있는 권한을 부여합니다.
account:PutAlternateContact	쓰기	계정의 대체 연락처를 수정할 수 있는 권한을 부여합니다.

권한 이름	액세스 레벨	설명
account:PutContactInformation	쓰기	계정의 기본 연락처 정보를 업데이트하는 권한을 부여합니다.
account:StartPrimaryEmailUpdate	쓰기	AWS 조직 내 멤버 계정의 기본 이메일 주소 업데이트를 시작할 수 있는 권한을 부여합니다.

AWS 계정 관리 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 계정 관리 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

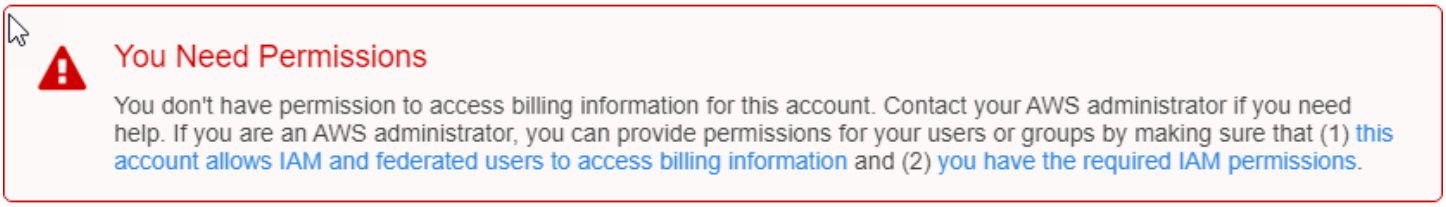
주제

- 계정 페이지에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행할 권한이 없음
- 내 외부의 사람이 내 계정 세부 정보에 액세스 AWS 계정 하도록 허용하고 싶습니다.

계정 페이지에서 작업을 수행할 권한이 없음

에서 작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 문의하여 지원을 받아야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

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



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

`iam:PassRole`을 수행할 권한이 없음

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

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

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

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

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

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

내 외부의 사람이 내 계정 세부 정보에 액세스 AWS 계정 하도록 허용하고 싶습니다.

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

자세히 알아보려면 다음을 참조하세요.

- 계정 관리에서 이러한 기능을 지원하는지 여부를 알아보려면 AWS 계정 관리에서 IAM을 사용하는 방법 섹션을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

AWSAWS 계정 관리에 대한 관리형 정책

AWS Account Management는 현재 사용할 수 있는 두 가지 AWS 관리형 정책을 제공합니다.

- AWS 관리형 정책: AWSAccountManagementReadOnlyAccess
- AWS 관리형 정책: AWSAccountManagementFullAccess
- AWS 관리형 정책에 대한 계정 관리 업데이트

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

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

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

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSAccountManagementReadOnlyAccess

`AWSAccountManagementReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 다음 항목만 볼 수 있는 읽기 전용 권한을 제공합니다.

- 에 대한 메타데이터 AWS 계정
- 에 대해 활성화 또는 비활성화 AWS 리전 된 AWS 계정 (콘 AWS 솔을 사용해야만 계정의 리전 상태를 볼 수 있음)

이를 위해 `Get*` 또는 `List*` 작업의 실행 권한을 부여합니다. 계정 메타데이터를 수정하거나 계정에 AWS 리전 대해 활성화 또는 비활성화할 수 있는 기능을 제공하지 않습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- account - 보안 주체가 메타데이터 정보를 검색할 수 있도록 허용합니다 AWS 계정. 또한 위탁자가 AWS Management Console에서 계정에 대해 활성화된 AWS 리전 을 나열할 수 있습니다.

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

AWS 관리형 정책: AWSAccountManagementFullAccess

AWSAccountManagementFullAccess 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 다음을 보거나 수정할 수 있는 전체 관리 액세스 권한을 제공합니다.

- 에 대한 메타데이터 AWS 계정
- 에 대해 활성화 또는 비활성화 AWS 리전 된 AWS 계정 (콘 AWS 솔을 사용해야만 계정의 상태를 보거나 리전을 활성화 또는 비활성화할 수 있음)

이를 위해 account 작업 실행 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- account - 보안 주체가 메타데이터 정보를 보거나 수정할 수 있도록 허용합니다 AWS 계정. 또한 위탁자가 AWS Management Console에서 계정에 대해 활성화된 AWS 리전 을 나열하고 그들을 활성화 또는 비활성화할 수 있도록 허용합니다.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "account:*",
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책에 대한 계정 관리 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Account Management의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 계정 관리 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWS 계정 관리가 새로운 AWS 관리형 정책으로 시작되고 변경 사항 추적 시작	Account Management는 다음과 같은 AWS 관리형 정책으로 처음 시작되었습니다. • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	2021년 9월 30일

AWS 계정 관리에 대한 규정 준수 검증

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

특정 규정 준수 프로그램 범위의 AWS 서비스 목록은 규정 준수 AWS 서비스 프로그램 범위의 규정 준수. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 AWS Artifact 사용 설명서의 에서 보고서 다운로드 AWS Artifact에서 를 참조하세요.

에서 서비스를 사용할 때 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 계정 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 -이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔에 기준 환경을 배포 AWS 하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 -이 백서에서는 기업이 AWS 를 사용하여 HIPAA 적격 애플리케이션을 생성하는 방법을 설명합니다.

> **Note**
>
> 모든가 HIPAA에 적합한 AWS 서비스 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하세요.

- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 업계 및 위치에 적용될 수 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 보안 업계 표준 및 모범 사례 준수를 확인하는 데 도움이 AWS 되는 내 보안 상태를 포괄적 AWS 서비스 으로 볼 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

AWS 계정 관리의 복원력

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

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

의 인프라 보안 AWS Account Management

관리형 서비스인에서 실행되는 AWS 서비스는 AWS 글로벌 네트워크 보안으로 보호 AWS 계정 됩니다. AWS 보안 서비스 및가 인프라를 보호하는 방법에 AWS 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 계정 설정에 액세스합니다. 고객은 다음을 지원해야 합니다.

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

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

모니터링 AWS 계정

모니터링은 AWS 계정 관리 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.는 계정 관리를 모니터링하고, 문제가 있을 때 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 AWS 제공합니다.

- AWS CloudTrail는에 의해 또는를 대신하여 수행된 API 호출 및 관련 이벤트를 캡처(로그) AWS 계정하고 사용자가 지정한 Amazon Simple Storage Service(Amazon S3) 버킷에 로그 파일을 씁니다. 이로 인해 어떤 사용자 및 계정이 AWS를 호출했는지 어떤 소스 IP 주소에 호출이 이루어졌는지 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.
- Amazon EventBridge는 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에 자동으로 응답하여 AWS 서비스에 추가 자동화를 추가합니다. AWS 서비스의 이벤트는 거의 실시간으로 EventBridge로 전달됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.

를 사용하여 AWS Account Management API 호출 로깅 AWS CloudTrail

AWS 계정 관리 APIs는 사용자 AWS CloudTrail, 역할 또는 계정 관리 작업을 호출하는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 모든 계정 관리 API 직접 호출을 이벤트로 캡처합니다. 캡처된 호출에는 계정 관리 작업에 대한 모든 호출이 포함됩니다. 추적을 생성하면 계정 관리 작업을 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 계정 관리 작업이라는 요청, 요청을 수행하는 데 사용된 IP 주소, 요청을 수행한 사람 및 시기, 추가 세부 정보를 결정할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 계정 관리 정보

계정을 생성할 AWS 계정 때에서 CloudTrail이 켜집니다. Account Management 작업에서 활동이 발생하면 CloudTrail은 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트의 해당 활동을 기록합니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 정보는 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

계정 관리 작업에 대한 이벤트를 AWS 계정포함하여에서 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로에서 추적을 생성하면 추적 AWS Management Console이 모든에 적용됩니다 AWS 리전. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 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 CloudTrail 는이 가이드의 API 참조 섹션에 있는 모든 계정 관리 API 작업을 기록합니다. 예컨대, `CreateAccount`, `DeleteAlternateContact`및 `PutAlternateContact`작업에 대한 호출은 CloudTrail 로그 파일의 항목을 생성합니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 루트 사용자 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 요청이 이루어졌는지 여부
- IAM 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청을 했는지 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 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

예제 1: 다음 예제는 GetAlternateContact 작업에 대한 호출이 계정의 현재 OPERATIONS 대체 연락처를 검색하는 CloudTrail 로그 항목을 보여줍니다. 작업에서 반환되는 값은 로깅된 정보에 포함되지 않습니다.

Example 예시 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: 다음 예제는 PutAlternateContact 작업에 대한 호출에 대해 새 BILLING 대체 연락처를 계정에 추가하기 위한 CloudTrail 로그 항목을 보여줍니다.

```
{
  "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: 다음 예제는 DeleteAlternateContact 작업에 대한 호출에 대해 현재 OPERATIONS 대체 연락처를 삭제하기 위한 CloudTrail 로그 항목을 보여줍니다.

```
{
  "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"
}
```


EventBridge를 사용하여 계정 관리 이벤트 모니터링

Amazon EventBridge(이전 명칭: CloudWatch Events)를 사용하면 다른 AWS 서비스를 사용하는 특정 이벤트를 모니터링하고 대상 작업을 시작할 수 있습니다. 의 이벤트 AWS 서비스 는 거의 실시간으로 EventBridge로 전달됩니다.

EventBridge를 사용하면 수신 이벤트를 확인한 후 처리 대상으로 라우팅하는 규칙을 생성할 수 있습니다.

자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 시작하기를 참조하세요.

계정 관리 이벤트

다음은 계정 관리 이벤트의 예제입니다. 이벤트는 최선의 작업에 근거하여 생성됩니다.

CloudTrail을 통한 리전 및 API 직접 호출 활성화 및 비활성화와 관련된 이벤트만 현재 계정 관리에 사용할 수 있습니다.

이벤트 유형

- 리전 활성화 및 비활성화 이벤트

리전 활성화 및 비활성화 이벤트

콘솔 또는 API에서 계정의 리전을 활성화하거나 비활성화하면 비동기 작업이 시작됩니다. 초기 요청은 대상 계정에서 CloudTrail 이벤트로 기록됩니다. 또한 활성화 또는 비활성화 프로세스가 시작되면 EventBridge 이벤트가 호출 계정으로 전송되고, 프로세스가 완료되면 다시 전송됩니다.

다음 예시 이벤트는 `2020-09-30`에 `ap-east-1` 리전이 계정 `123456789012`에 대해 `ENABLED`된 것임을 나타내는 요청을 전송하는 방법을 보여줍니다.

```
{
   "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"
   }
}
```

GetRegionOptStatus 및 ListRegions API가 반환하는 상태와 일치하는 네 가지 가능한 상태가 있습니다:

- ENABLED - 표시된 accountId에서 리전이 성공적으로 활성화
- ENABLING - 표시된 accountId에서 리전이 활성화되고 있음
- DISABLED - 표시된 accountId에서 리전이 성공적으로 비활성화
- DISABLING - 표시된 accountId에서 리전이 비활성화되고 있음

다음 샘플 이벤트 패턴은 모든 리전 이벤트를 캡처하는 규칙을 생성합니다.

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

다음 샘플 이벤트 패턴은 ENABLED 및 DISABLED 리전 이벤트만 캡처하는 규칙을 생성합니다.

```
{
```

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

문제 해결 AWS 계정

다음 주제의 정보를 사용하여 AWS 계정의 문제를 진단하고 해결합니다. 루트 사용자에 대한 도움말은 IAM User Guide의 Troubleshooting issues with the root user을 참조하세요. 로그인 프로세스에 대한 도움말은 AWS Sign-In User Guide의 Troubleshooting AWS 계정 sign-in issues을 참조하세요.

주제 문제 해결

- AWS 계정 생성 문제 해결
- AWS 계정 해지 문제 해결
- 기타 AWS 계정문제 해결

AWS 계정 생성 문제 해결

다음 표의 참조 링크를 사용하여 새를 생성하는 데 발생하는 문제를 진단하고 수정할 수 있습니다 AWS 계정.

문제	참조 링크	소스
가입하거나 계정을 생성하는 방법을 모름	생성 AWS 계정	이 설명서는
새 계정 또는 입력한 PIN이 작동하지 않는지 확인하기 AWS 위해에서 전화를 받지 못한 경우 어떻게 해야 합니까?	https://repost.aws/knowledge-center/phone-verify-no-call	AWS re:Post
AWS 계정 전화로 확인하려고 할 때 "최대 시도 실패 횟수" 오류를 해결하려면 어떻게 해야 합니까?	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post
24시간 후에도 계정이 활성화되지 않음	https://repost.aws/knowledge-center/create-and-activate-aws-account	AWS re:Post

문제	참조 링크	소스
새 계정이 생성된 후 로그인할 수 없음	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html	AWS 로그인 사용 설명서

추가 도움말이 필요하면 특정 문제와 관련된 AWS re:Post 콘텐츠를 검색하는 것이 좋습니다. 추가 지원이 필요한 경우 AWS Support에 문의하세요.

AWS 계정 해지 문제 해결

아래 정보를 사용하여 계정 해지 프로세스 중에 발견된 일반적인 문제를 진단하고 수정할 수 있습니다. 계정 해지 프로세스에 대한 일반적인 내용은 닫기 AWS 계정 섹션을 참조하세요.

주제

- 계정을 삭제하거나 취소하는 방법을 모름
- 계정 페이지에 계정 해지 버튼이 표시되지 않음
- 계정을 해지했지만 여전히 확인 이메일을 받지 못함
- 계정을 해지하려고 할 때 "ConstraintViolationException" 오류 발생
- 멤버 계정을 해지하려고 할 때 "CLOSE_ACCOUNT_QUOTA_EXCEEDED" 오류 발생
- 관리 계정을 해지하기 전에 AWS 조직을 삭제해야 합니까?

계정을 삭제하거나 취소하는 방법을 모름

닫기 AWS 계정의 지침에 따라 계정을 해지하세요.

계정 페이지에 계정 해지 버튼이 표시되지 않음

루트 사용자로 로그인하지 않은 경우 계정 페이지에 계정 해지 버튼이 표시되지 않습니다. 계정을 닫으려면 루트 사용자 AWS Management Console 로에 로그인해야 합니다. 로그인할 수 없는 경우 Troubleshooting issues with the root user을 참조하세요.

계정을 해지했지만 여전히 확인 이메일을 받지 못함

이 확인 이메일은의 루트 사용자 이메일 주소만 전송됩니다 AWS 계정. 몇 시간 내에이 이메일을 받지 못하면 루트 사용자 AWS Management Console 로에 로그인하여 계정이 해지되었는지 확인할 수 있

습니다. 계정이 성공적으로 해지된 경우 계정이 해지되었음을 나타내는 메시지가 표시됩니다. 해지한 계정이 멤버 계정인 경우 해지된 계정에 AWS Organizations 콘솔SUSPENDED에서 로 레이블이 지정되어 있는지 확인하여 해지 성공 여부를 확인할 수 있습니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 멤버 계정 해지를 참조하세요.

관리 계정을 해지하려고 하는데 계정 해지에 대한 이메일 확인이 수신되지 않는 경우 조직에 활성 멤버 계정이 있을 가능성이 높습니다. 조직에 활성 멤버 계정이 없는 경우에만 관리 계정을 해지할 수 있습니다. 조직에 활성 멤버 계정이 남아 있지 않은지 확인하려면 AWS Organizations 콘솔로 이동하여 모든 멤버 계정이 계정 이름 Suspended 옆에 표시되는지 확인합니다. 그런 다음 관리 계정을 해지할 수 있습니다.

계정을 해지하려고 할 때 "ConstraintViolationException" 오류 발생

AWS Organizations 콘솔을 사용하여 관리 계정을 해지하려고 하는데, 이는 불가능합니다. 관리 계정을 닫으려면 관리 계정의 루트 사용자 AWS Management Console 로에 로그인하고 계정 페이지에서 닫아야 합니다. 자세한 내용은 AWS Organizations 사용 설명서의 Closing a management account in your organization를 참조하세요.

멤버 계정을 해지하려고 할 때 "CLOSE_ACCOUNT_QUOTA_EXCEEDED" 오류 발생

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. 계정의 10%가 1,000개를 초과하더라도 해지할 수 있는 계정의 개수는 최소 10개, 최대 1,000개입니다. 조직 할당량에 대한 자세한 내용은 AWS Organizations 사용 설명서의 Quotas for AWS Organizations을 참조하세요.

관리 계정을 해지하기 전에 AWS 조직을 삭제해야 합니까?

아니요. 관리 계정을 해지하기 전에 AWS 조직을 삭제할 필요가 없습니다. 그러나 조직에 활성 멤버 계정이 없는 경우에만 관리 계정을 해지할 수 있습니다. 조직에 활성 멤버 계정이 남아 있지 않은지 확인하려면 AWS Organizations 콘솔로 이동하여 모든 멤버 계정이 계정 이름 Suspended 옆에 표시되는지 확인합니다. 그런 다음 관리 계정을 해지할 수 있습니다.

기타 AWS 계정문제 해결

여기의 정보를 사용하면 AWS 계정과 관련된 문제를 해결하는 데 도움이 됩니다.

문제

- 내의 신용 카드를 변경해야 합니다. AWS 계정
- 사기 AWS 계정 활동을 보고해야 합니다.
- 를 닫아야 합니다. AWS 계정

내의 신용 카드를 변경해야 합니다. AWS 계정

의 신용 카드를 변경하려면 로그인할 수 있어야 AWS 계정합니다. AWS 에는 계정 소유자임을 증명해야 하는 보호 기능이 있습니다. 지침은 AWS Billing 사용 설명서의 Managing your credit card payment methods를 참조하세요.

사기 AWS 계정 활동을 보고해야 합니다.

를 사용하여 사기 행위가 의심 AWS 계정 되고 보고하려는 경우 AWS 리소스 남용을 보고하는 방법을 참조하세요.

Amazon.com에서 구매한 상품에 문제가 있는 경우 Amazon Customer Service를 참조하세요.

를 닫아야 합니다. AWS 계정

닫기 관련 문제를 해결하는 데 도움이 필요하면 섹션을 AWS 계정참조하세요닫기 AWS 계정.

닫기 AWS 계정

가 더 이상 필요하지 않은 경우이 섹션의 지침에 따라 언제든지 닫을 AWS 계정수 있습니다. 계정을 해지한 후 계정을 해지한 날로부터 90일 이내에 다시 열 수 있습니다. 계정을 해지한 날과 AWS 가 계정을 영구적으로 해지한 날 사이의 기간을 해지 후 기간이라고 합니다.

계정을 해지하기 전에 알아야 할 사항

를 닫기 전에 다음 사항을 고려해야 AWS 계정합니다.

- 계정을 해지하면 이 계정에 대한 AWS 고객 계약 종료 알림 역할을 합니다.
- 닫기 AWS 계정 전에에서 리소스를 삭제할 필요가 없습니다. 그러나 보관하려는 리소스 또는 데이터는 백업하는 것이 좋습니다. 특정 리소스를 백업하는 방법에 대한 지침은 해당 서비스에 대한 적절한 AWS 설명서를 참조하세요.
- 해지 후 기간 동안 계정을 다시 열 수 있습니다. 계정에 남아 있는 서비스의 요금은 계정을 다시 열면 다시 시작됩니다. 또한 모든 미지급 인보이스와 미결 예약 인스턴스 및 절감형 플랜 대한 책임도 남아있습니다.
- 계정 해지 전에 사용한 서비스에 대한 모든 미결 수수료 및 요금은 사용자가 부담합니다. 계정을 해지한 다음 달에 AWS 청구서를 받게 됩니다. 예를 들어 1월 15일에 계정을 해지한 경우 2월 초에 1월 1일부터 1월 15일까지 발생한 사용량에 대한 청구서를 받게 됩니다. 계정을 해지한 후에도 만료될 때까지 예약 인스턴스 및 절감형 플랜에 대한 청구서를 계속 받게 됩니다.
- 계정에서 이전에 사용 가능했던 AWS 서비스에 더 이상 액세스할 수 없습니다. 그러나 해지 후 기간 동안만 해지된 AWS 계정 에 로그인하고 액세스하여 과거 결제 정보, 액세스 계정 설정 또는 연락처 AWS Support을 볼 수 있습니다.
- 해지 시 AWS 계정 에 등록된 것과 동일한 이메일 주소를 다른 AWS 계정의 기본 이메일과 사용할 수 없습니다. 다른 AWS 계정에 동일한 이메일 주소를 사용하려면 해지 전에 업데이트하는 것이 좋습니다. 자세한 내용은 루트 사용자 이메일 주소 업데이트 단원을 참조하십시오.
- AWS 계정 루트 사용자에 다중 인증(MFA)이 활성화되어 있거나 IAM 사용자에 MFA 디바이스를 구성한 경우, 계정을 해지할 때 MFA가 자동으로 제거되지 않습니다. 해지 후 기간인 90일 동안 MFA를 켜 두도록 선택한 경우, 해당 기간 동안 계정에 액세스해야 할 수도 있으므로 해지 후 기간이 만료될 때까지 MFA 디바이스를 활성 상태로 유지합니다. 참고로 하드웨어 TOTP 토큰 디바이스는 계정이 영구적으로 해지된 후에는 다른 사용자와 연결할 수 없습니다. 나중에 다른 사용자와 하드웨어 TOTP 토큰을 사용하려면 계정을 해지하기 전에 하드웨어 MFA 디바이스를 비활성화하는 옵션도 있습니다. IAM 사용자를 위한 MFA 디바이스는 계정 관리자가 삭제해야 합니다.

멤버 계정에 대한 추가 고려 사항

- 멤버 계정을 해지하는 경우 해지 후 기간이 끝날 때까지 해당 계정이 조직에서 제거되지 않습니다. 해지 후 기간 동안에는 해지된 멤버 계정이 여전히 조직의 계정 할당량 계산에 반영됩니다. 계정 수가 할당량에 반영되지 않도록 하려면 계정을 해지하기 전에 Remove a member account from your organization하세요.
- 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. 계정의 10%가 1,000개를 초과하더라도 해지할 수 있는 계정의 개수는 최소 10개, 최대 1,000개입니다. 조직 할당량에 대한 자세한 내용은 Quotas for AWS Organizations을 참조하세요.
- AWS Control Tower를 사용하는 경우 계정을 해지하기 전에 멤버 계정의 관리를 취소해야 합니다. AWS Control Tower 사용 설명서에서 멤버 계정 관리 해제를 참조하세요.

서비스별 고려 사항

- AWS Marketplace 구독은 계정 해지 시 자동으로 취소되지 않습니다. 구독이 있는 경우 먼저 구독에서 소프트웨어의 모든 인스턴스를 종료합니다. 그런 다음 AWS Marketplace 콘솔의 구독 관리 페이지로 이동하여 구독을 취소합니다.
- 계정이 해지되면는 도메인을 일시 중지하기 전에 최대 5일 동안 매일 이메일을 AWS 보냅니다. 도메인이 일시 중지된 후 도메인의 등록 기관에 따라 30일 이내에 도메인을 삭제하거나 도메인을 등록 기관에 릴리스합니다. 자세한 내용은 My AWS 계정 is closed or permanently closed, and my domain is registered with Route 53을 참조하세요.
- AWS CloudTrail 는 기본 보안 서비스입니다. 즉, 사용자가 종료하기 AWS 계정 전에에서 추적을 명시적으로 삭제하지 않는 한 사용자가 생성한 추적 AWS 계정 은 계속 존재하고가 종료된 후에도 이벤트를 전달할 수 있습니다. AWS 계정 가 닫힌 후 추적 삭제를 요청하는 방법에 대한 자세한 내용은 CloudTrail 사용 설명서의 AWS 계정 종결 및 추적을 참조하세요.

계정을 해지하는 방법

다음 절차를 AWS 계정 사용하여를 닫을 수 있습니다. 해지하려는 계정 유형[독립 실행형, 멤버, 관리형 및 AWS GovCloud (US)]에 따라 각 탭에 다른 지침이 제공됩니다.

계정을 해지하는 과정에서 문제가 발생하면 AWS 계정 해지 문제 해결 섹션을 참조하세요.

Standalone account

독립 실행형 계정은의 일부가 아닌 개별 관리형 계정입니다 AWS Organizations.

계정 페이지에서 독립 실행형 계정을 해지하려면

1. 종료 AWS 계정 하려는 의 루트 사용자 AWS Management Console 로에 로그인합니다. IAM 사용자 또는 역할로 로그인한 상태에서는 계정을 해지할 수 없습니다.
2. 상단 오른쪽 모서리의 탐색 모음에서 계정 이름이나 번호를 선택한 다음 계정을 선택합니다.
3. 계정 페이지에서 계정 해지 버튼을 선택합니다.
4. 계정 ID(해지 대화 상자 상단에 표시됨)를 입력하여 계정 해지 프로세스를 읽고 이해했는지 확인합니다.
5. 계정 해지 버튼을 선택하여 계정 해지 프로세스를 시작합니다.
6. 몇 분 내에 계정이 해지되었다는 확인 이메일을 받게 됩니다.

> **Note**
>
> 이 작업은 AWS CLI 또는 AWS SDKs. 이 작업은를 사용해야만 수행할 수 있습니다 AWS Management Console.

Member account

멤버 계정은의 일부인 AWS 계정 입니다 AWS Organizations.

AWS Organizations 콘솔에서 멤버 계정을 해지하려면

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. 이 옵션은 조직이 모든 기능 모드에 있는 AWS 경우에만 사용할 수 있습니다.

> **Note**
>
> 조직에서 통합 결제 모드를 사용하는 경우 콘솔에서 닫기 버튼을 볼 수 없습니다. 통합 결제 모드에서 계정을 해지하려면 루트 사용자로 해지하려는 계정에 로그인합니다. 계

정 페이지에서 계정 닫기 버튼을 선택하고 계정 ID를 입력한 다음 계정 닫기 버튼을 선택합니다.

4. 계정 해지 지침을 읽고 이해해야 합니다.
5. 멤버 계정 ID를 입력한 다음 계정 해지를 선택하여 계정 해지 절차를 시작합니다.

> **Note**
>
> 해지하는 모든 멤버 계정에는 원래 해지 날짜 후 최대 90일 동안 AWS Organizations 콘솔의 계정 이름 옆에 SUSPENDED 레이블이 표시됩니다. 90일이 지나면 멤버 계정이 더 이상 AWS Organizations에 표시되지 않습니다.

계정 페이지에서 멤버 계정을 해지하려면

선택적으로의 계정 페이지에서 직접 AWS 멤버 계정을 해지할 수 있습니다 AWS Management Console. 단계별 지침은 독립 실행형 계정 탭의 지침을 따르세요.

AWS CLI 및 SDKs를 사용하여 멤버 계정을 해지하려면

AWS CLI 및 SDKs를 사용하여 멤버 계정을 해지하는 방법에 대한 지침은 AWS Organizations 사용 설명서의 조직의 멤버 계정 해지를 참조하세요.

Management account

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

> **Note**
>
> AWS Organizations 콘솔에서 직접 관리 계정을 해지할 수 없습니다.

계정 페이지에서 관리 계정을 해지하려면

1. 종료하려는 관리 계정의 루트 사용자 AWS Management Console 로에 로그인합니다. IAM 사용자 또는 역할로 로그인한 상태에서는 계정을 해지할 수 없습니다.
2. 조직에 활성 멤버 계정이 남아 있지 않은지 확인합니다. 이렇게 하려면 AWS Organizations 콘솔 로 이동하여 모든 멤버 계정이 계정 이름 옆에 Suspended가 표시되는지 확인합니다. 아직

활성 상태인 멤버 계정이 있는 경우 다음 단계로 이동하기 전에 멤버 계정 탭에 제공된 계정 해지 지침을 따라야 합니다.

3. 상단 오른쪽 모서리의 탐색 모음에서 계정 이름이나 번호를 선택한 다음 계정을 선택합니다.
4. 계정 페이지에서 계정 해지 버튼을 선택합니다.
5. 계정 ID(해지 대화 상자 상단에 표시됨)를 입력하여 계정 해지 프로세스를 읽고 이해했는지 확인합니다.
6. 계정 해지 버튼을 선택하여 계정 해지 프로세스를 시작합니다.
7. 몇 분 내에 계정이 해지되었다는 확인 이메일을 받게 됩니다.

> **Note**
>
> 이 작업은 AWS CLI 또는 AWS SDKs. 이 작업은를 사용해야만 수행할 수 있습니다 AWS Management Console.

AWS GovCloud (US) account

AWS GovCloud (US) 계정은 결제 및 결제를 AWS 계정 위해 항상 단일 표준에 연결됩니다.

AWS GovCloud (US) 계정을 해지하려면

AWS GovCloud (US) 계정에 연결된이 AWS 계정 있는 경우 계정을 해지하기 전에 표준 계정을 해지해야 합니다 AWS GovCloud (US) . 데이터를 백업하고 의도하지 않은 AWS GovCloud (US) 요금을 방지하는 방법을 비롯한 자세한 내용은 AWS GovCloud (US) 사용 설명서의 AWS GovCloud (US) 계정 해지를 참조하세요.

계정을 해지한 후 예상되는 사항

계정을 해지한 직후 다음과 같은 상황이 발생합니다.

- 루트 사용자의 이메일 주소로 계정 해지를 확인하는 이메일을 받게 됩니다. 몇 시간 내에 이 이메일을 받지 못한 경우 AWS 계정 해지 문제 해결 섹션을 참조하세요.
- 해지한 모든 멤버 계정은 원래 해지 날짜 후 최대 90일 동안 AWS Organizations 콘솔에서 해당 계정 이름 옆에 SUSPENDED 레이블을 표시합니다. 90일이 지나면 AWS Organizations 콘솔에 멤버 계정이 더 이상 표시되지 않습니다.

- 의 서비스에 액세스할 수 있는 권한을 AWS 계정 다른 계정에 부여한 경우 계정 해지 후 해당 계정의 액세스 요청이 실패합니다. 를 다시 열면 필요한 권한을 부여한 경우 AWS 계정다른 사용자가 계정의 AWS 서비스 및 리소스에 다시 액세스할 AWS 계정 수 있습니다.

계정 해지가 모든 리전 및 서비스에서 즉시 발생하지 않을 수 있으며 완료하는 데 몇 시간이 걸릴 수 있습니다.

해지 후 기간

해지 후 기간은 계정을 해지한 날부터가를 AWS 영구적으로 해지한 날까지의 기간을 나타냅니다 AWS 계정. 해지 후 기간은 90일입니다. 해지 후 기간에는 계정을 다시 열어야지만 남아 있는 콘텐츠 또는 AWS 서비스에 액세스할 수 있습니다. 해지 후 기간이 AWS 지나면가를 영구적으로 해지 AWS 계정하고 더 이상 다시 열 수 없습니다. AWS 는 계정의 콘텐츠 및 리소스도 삭제합니다(CloudTrail 추적 제외). 계정이 영구적으로 해지된 후에는 해당 AWS 계정 ID를 재사용할 수 없습니다.

다시 열기 AWS 계정

90일 이내에 계정이 영구적으로 해지되며, 그 이후에는 계정을 다시 열 수 없고 계정에 남아 있는 콘텐츠 AWS 가 삭제됩니다. 계정이 영구적으로 해지되기 전에 다시 열려면 (1) 가능한 한 빨리 AWS Support에 문의해야 하며, (2) 계정 해지일로부터 60일 이내에 청구서에 지정된 필수 정보 제공을 포함하여 미결제 잔액에 대한 전액을 지불해야 합니다.

> **Note**
>
> 계정에 남아 있는 서비스의 요금은 계정을 다시 열면 다시 시작됩니다.

API 참조

계정 관리(account) 네임스페이스의 API 작업을 통해를 수정할 수 있습니다 AWS 계정.

모든는 계정과 연결된 최대 3개의 대체 연락처에 대한 정보를 포함하여 계정에 대한 정보가 포함된 메타데이터를 AWS 계정 지원합니다. 이는 계정의 루트 사용자와 연결된 이메일 주소에 추가됩니다. 계정과 연결된 다음 각 연락 유형 중 하나만 지정할 수 있습니다.

- 결제 연락처
- 운영 연락처
- 보안 연락처

기본적으로 이 가이드에서 설명하는 API 작업은 작업을 호출하는 계정에 직접 적용됩니다. 작업을 호출하는 계정의 자격 증명은 일반적으로 IAM 역할 또는 IAM 사용자이며 API 작업을 호출하려면 IAM 정책에서 적용하는 권한이 있어야 합니다. 또는 관리 계정의 자격 증명 AWS Organizations 에서 이러한 API 작업을 호출하고 조직의 구성원 AWS 계정 인 모든의 계정 ID 번호를 지정할 수 있습니다.

API 버전

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

> **Note**
>
> API를 직접 사용하는 대신 다양한 프로그래밍 언어 및 플랫폼(Java, Ruby, .NET, iOS, Android 등)에 대한 라이브러리 및 샘플 코드로 구성된 AWS SDKs 중 하나를 사용할 수 있습니다. SDKs는 AWS Organizations에 대한 프로그래밍 방식 액세스를 생성하는 편리한 방법을 제공합니다. 예를 들어 SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. 다운로드 및 설치 방법을 포함하여 AWS SDKs에 대한 자세한 내용은 Amazon Web Services용 도구를 참조하세요.

AWS SDKs를 사용하여 Account Management 서비스에 프로그래밍 방식 API 호출을 수행하는 것이 좋습니다. 그러나 계정 관리 Query API를 사용하여 계정 관리 웹 서비스에 직접 호출할 수도 있습니다. 계정 관리 Query API에 대한 자세한 내용은 계정 관리 사용 설명서의 HTTP 쿼리 요청을 통한 API 호출 섹션을 참조하세요. 조직은 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 크기가 더 큰 작업이 필요한 경우 POST 요청을 사용합니다.

요청에 서명하기

HTTP 요청을 보낼 때가 요청을 보낸 사람을 식별할 AWS 수 있도록 요청에 서명해야 AWS합니다. AWS 액세스 키 ID와 보안 액세스 키로 구성된 액세스 키로 요청에 서명합니다. 루트 계정에 대한 액세스 키 페어는 생성하지 않는 것이 좋습니다. 루트 계정에 대한 액세스 키를 보유한 사람은 누구든지 계정의 모든 리소스에 무제한으로 액세스할 수 있습니다. 대신 관리 권한이 있는 IAM 사용자의 액세스 키를 생성합니다. 또 다른 옵션으로 AWS Security Token Service를 사용하여 임시 보안 자격 증명을 생성하고 해당 자격 증명을 사용하여 요청에 서명합니다.

요청에 서명하려면 Signature Version 4를 사용하는 것이 좋습니다. Signature Version 2를 사용하는 기존 애플리케이션이 있는 경우 Signature Version 4를 사용하도록 업데이트할 필요가 없습니다. 그러나 이제 일부 작업에는 Signature Version 4가 필요합니다. Signature Version 4가 필요한 작업에 대한 설명서는 이 요구 사항이 필요합니다. 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하세요.

AWS 명령줄 인터페이스(AWS CLI) 또는 AWS SDKs 중 하나를 사용하여 요청을 할 때 AWS이러한 도구는 도구 구성 시 지정한 액세스 키로 요청에 자동으로 서명합니다.

계정 관리에 대한 지원 및 피드백

우리는 여러분의 의견을 환영합니다. feedback-awsaccounts@amazon.com으로 의견을 보내거나 계정 관리 지원 포럼에 피드백과 질문을 게시합니다. AWS 지원 포럼에 대한 자세한 내용은 포럼 도움말을 참조하세요.

예 제시 방법

요청에 대한 응답으로 계정 관리에서 반환하는 JSON은 줄 바꿈 또는 서식 공백 없이 긴 단일 문자열로 반환됩니다. 가독성을 높이기 위해 이 가이드의 예제에는 줄 바꿈과 공백이 모두 표시됩니다. 예제 입력 파라미터로 인해 긴 문자열이 화면 밖으로 확장되는 경우 줄 바꿈을 삽입하여 가독성을 높입니다. 항상 입력을 단일 JSON 텍스트 문자열로 제출해야 합니다.

API 요청 기록

계정 관리는에 대한 AWS API 호출을 기록하고 Amazon S3 버킷에 로그 파일을 AWS 계정 전달하는 서비스인 CloudTrail을 지원합니다. CloudTrail에서 수집된 정보를 사용하여 계정 관리에 대한 성공적인 요청, 요청자, 요청 시기 등을 결정할 수 있습니다. 계정 관리 및 CloudTrail에 대한 계정 관리의 지원에 대한 자세한 내용은 를 사용하여 AWS Account Management API 호출 로깅 AWS CloudTrail 섹션을 참조하세요. 설정 방법 및 로그 파일을 찾는 방법을 비롯한 CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

작업

다음 작업이 지원됩니다.

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAccountInformation
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAccountName
- PutAlternateContact
- PutContactInformation
- StartPrimaryEmailUpdate

AcceptPrimaryEmailUpdate

StartPrimaryEmailUpdate에서 시작된 요청을 수락하여 지정된 계정에 기본 이메일 주소(루트 사용자 이메일 주소라고도 함)를 업데이트합니다.

Request Syntax

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

{
   "AccountId": "string",
   "Otp": "string",
   "PrimaryEmail": "string"
}
```

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

이 작업은 멤버 계정을 대상으로, 관리 계정이나 조직의 위임된 관리자 계정에서만 호출할 수 있습니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다.

유형: String

패턴: \d{12}

필수 여부: 예

Otp

StartPrimaryEmailUpdate API 호출에 지정된 PrimaryEmail로 전송된 OTP 코드입니다.

유형: String

패턴: [a-zA-Z0-9]{6}

필수 여부: 예

PrimaryEmail

지정된 계정과 함께 사용할 새 기본 이메일 주소입니다. StartPrimaryEmailUpdate API 호출의 PrimaryEmail와 일치해야 합니다.

유형: 문자열

길이 제약: 최소 길이는 5입니다. 최대 길이는 64.

필수 항목 여부: 예

응답 구문

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

{
   "Status": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Status

수락된 기본 이메일 업데이트 요청의 상태를 검색합니다.

타입: 문자열

유효 값: `PENDING | ACCEPTED`

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

ConflictException

리소스의 현재 상태에 충돌이 발생하여 요청을 처리할 수 없습니다. 예를 들어, 현재 비활성화된 리전(비활성화 상태)을 활성화하려고 하거나 계정의 루트 사용자 이메일을 이미 사용 중인 이메일 주소로 변경하려고 하면 이 문제가 발생합니다.

HTTP 상태 코드: 409

InternalServerException

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

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스 지정으로 인해 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

DeleteAlternateContact

에서 지정된 대체 연락처를 삭제합니다 AWS 계정.

대체 고객 응대 작업을 사용하는 방법에 대한 자세한 내용은 의 대체 고객 응대 업데이트를 참조하세요 AWS 계정.

> **Note**
>
> 에서 AWS 계정 관리하는에 대한 대체 연락처 정보를 업데이트하려면 먼저 AWS 계정 관리와 조직 간의 통합을 활성화 AWS Organizations해야 합니다. 자세한 내용은 AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화를 참조하세요.

Request Syntax

```
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 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 액세스하거나 수정할 계정의 12자리 AWS 계정 ID 번호를 지정합니다.

이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 AWS 계정으로 설정됩니다.

이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 하며, 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있

어야 하며, 조직은 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 말고, 검색하거나 수정하려는 연락처의 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: `\d{12}`

필수 여부: 아니요

AlternateContactType

삭제할 대체 연락처를 지정합니다.

타입: 문자열

유효 값: `BILLING | OPERATIONS | SECURITY`

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스 지정으로 인해 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

예

예시 1

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

샘플 요청

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

{
   "AccountName":"MyAccount"
}
```

샘플 응답

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

예시 2

다음 예에서는 조직의 지정된 멤버 계정에 대한 대체 결제 연락처를 삭제합니다. 조직의 관리 계정 또는 계정 관리 서비스의 위임된 관리자 계정의 자격 증명을 사용해야 합니다.

샘플 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

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK

- AWS SDK for Ruby V3

DisableRegion

계정의 특정 리전을 비활성화(옵트아웃)합니다.

> **Note**
>
> 리전을 비활성화하면 해당 리전에 있는 모든 리소스에 대한 모든 IAM 액세스가 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 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 Amazon Web Services 계정으로 설정됩니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 마세요. 대신 연락처가 검색하거나 수정하려는 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: `\d{12}`

필수 여부: 아니요

RegionName

지정된 리전 이름에 리전 코드를 지정합니다(예: `af-south-1`). 리전을 비활성화하면는 해당 리전의 IAM 리소스를 삭제하는 등 계정에서 해당 리전을 비활성화하는 작업을 AWS 수행합니다. 이 프로세스는 대부분의 계정에서 몇 분이 걸리지만 몇 시간이 걸릴 수도 있습니다. 비활성화 프로세스가 완전히 완료될 때까지 리전을 활성화할 수 없습니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

ConflictException

리소스의 현재 상태에 충돌이 발생하여 요청을 처리할 수 없습니다. 예를 들어, 현재 비활성화된 리전(비활성화 상태)을 활성화하려고 하거나 계정의 루트 사용자 이메일을 이미 사용 중인 이메일 주소로 변경하려고 하면 이 문제가 발생합니다.

HTTP 상태 코드: 409

InternalServerException

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

HTTP 상태 코드: 500

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

EnableRegion

계정의 특정 리전을 활성화(옵트인)합니다.

Request Syntax

```
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 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 Amazon Web Services 계정으로 설정됩니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 마세요. 대신 연락처가 검색하거나 수정하려는 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: \d{12}

필수 여부: 아니요

RegionName

지정된 리전 이름에 리전 코드를 지정합니다(예: af-south-1). 리전을 활성화하면 AWS 에서 해당 리전의 계정을 준비하는 작업(예: IAM 리소스를 해당 리전으로 배포)을 수행합니다. 이 프로세스는 대부분의 계정에서 몇 분이 걸리지만 몇 시간이 걸릴 수도 있습니다. 이 프로세스가 완료될 때까지는 해당 리전을 사용할 수 없습니다. 또한 활성화 프로세스가 완전히 완료될 때까지 리전을 비활성화할 수 없습니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

ConflictException

리소스의 현재 상태에 충돌이 발생하여 요청을 처리할 수 없습니다. 예를 들어, 현재 비활성화된 리전(비활성화 상태)을 활성화하려고 하거나 계정의 루트 사용자 이메일을 이미 사용 중인 이메일 주소로 변경하려고 하면 이 문제가 발생합니다.

HTTP 상태 코드: 409

InternalServerException

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

HTTP 상태 코드: 500

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

GetAccountInformation

계정 이름, 계정 ID, 계정 생성 날짜 및 시간을 포함하여 지정된 계정에 대한 정보를 검색합니다. 이 API를 사용하려면 IAM 사용자 또는 역할에 `account:GetAccountInformation` IAM 권한이 있어야 합니다.

Request Syntax

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

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

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 액세스하거나 수정할 계정의 12자리 AWS 계정 ID 번호를 지정합니다.

이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 AWS 계정으로 설정됩니다.

이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 하며, 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, Account Management 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정이 할당되어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 말고, 검색하거나 수정하려는 연락처의 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: \d{12}

필수 여부: 아니요

응답 구문

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

{
   "AccountCreatedDate": "string",
   "AccountId": "string",
   "AccountName": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AccountCreatedDate

계정이 생성된 날짜 및 시간입니다.

유형: 타임스탬프

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

이 작업은 멤버 계정을 대상으로, 관리 계정이나 조직의 위임된 관리자 계정에서만 호출할 수 있습니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다.

유형: String

패턴: `\d{12}`

AccountName

계정의 이름입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

패턴: `[ -;=?-~]+`

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

예

예시 1

다음 예제에서는 작업을 호출하는 데 자격 증명이 사용되는 계정의 계정 정보를 검색합니다.

샘플 요청

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

{}
```

샘플 응답

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

{
   "AccountId": "123456789012",
   "AccountName": "MyAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

예시 2

다음 예시에서는 조직의 지정된 멤버 계정에 대한 계정 정보를 검색합니다. 조직의 관리 계정 또는 계정 관리 서비스의 위임된 관리자 계정의 자격 증명을 사용해야 합니다.

샘플 요청

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

{
   "AccountId": "123456789012"
}
```

샘플 응답

```
HTTP/1.1 200 OK
```

```
Content-Type: application/json

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go v2용 SDK
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

GetAlternateContact

에 연결된 지정된 대체 연락처를 검색합니다 AWS 계정.

대체 고객 응대 작업을 사용하는 방법에 대한 자세한 내용은 의 대체 고객 응대 업데이트를 참조하세요 AWS 계정.

> **Note**
>
> 에서 AWS 계정 관리하는에 대한 대체 연락처 정보를 업데이트하려면 먼저 AWS 계정 관리와 조직 간의 통합을 활성화 AWS Organizations해야 합니다. 자세한 내용은 AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화를 참조하세요.

Request Syntax

```
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 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 액세스하거나 수정할 계정의 12자리 AWS 계정 ID 번호를 지정합니다.

이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 AWS 계정으로 설정됩니다.

이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 하며, 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있

어야 하며, 조직은 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 AccountId를 지정할 수 없습니다. AccountId 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 말고, 검색하거나 수정하려는 연락처의 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: \d{12}

필수 여부: 아니요

AlternateContactType

검색할 대체 연락처를 지정합니다.

타입: 문자열

유효 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 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

AlternateContact

지정된 대체 연락처의 세부 정보가 포함된 구조입니다.

타입: AlternateContact 객체

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스 지정으로 인해 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

예

예시 1

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

샘플 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"
   }
}
```

예시 2

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

샘플 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

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

GetContactInformation

AWS 계정의 기본 연락처 정보를 검색합니다.

기본 연락처 작업을 사용하는 방법에 대한 자세한 내용은 의 기본 연락처 업데이트를 참조하세요 AWS 계정.

Request Syntax

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

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

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 Amazon Web Services 계정으로 설정됩니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 AccountId를 지정할 수 없습니다. AccountId 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 마세요. 대신 연락처가 검색하거나 수정하려는 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

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 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

ContactInformation

AWS 계정과 연결된 기본 연락처 정보의 세부 정보를 포함합니다.

타입: ContactInformation 객체

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스 지정으로 인해 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

GetPrimaryEmail

지정된 계정의 기본 이메일 주소를 검색합니다.

Request Syntax

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

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

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

이 작업은 멤버 계정을 대상으로, 관리 계정이나 조직의 위임된 관리자 계정에서만 호출할 수 있습니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다.

유형: String

패턴: `\d{12}`

필수 여부: 예

응답 구문

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

{
   "PrimaryEmail": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

PrimaryEmail

지정된 계정과 연결된 기본 이메일 주소를 검색합니다.

유형: 문자열

길이 제약: 최소 길이는 5입니다. 최대 길이는 64.

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스 지정으로 인해 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

GetRegionOptStatus

특정 리전의 옵트인 상태를 검색합니다.

Request Syntax

```
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 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 Amazon Web Services 계정으로 설정됩니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 마세요. 대신 연락처가 검색하거나 수정하려는 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: \d{12}

필수 여부: 아니요

RegionName

지정된 리전 이름에 리전 코드를 지정합니다(예: af-south-1). 이 함수는 이 파라미터에 전달하는 리전의 상태를 반환합니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 예

응답 구문

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

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

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

RegionName

전달된 리전 코드입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

RegionOptStatus

리전이 거칠 수 있는 잠재적 상태 중 하나(활성화됨, 활성화 중, 비활성화됨, 비활성화 중, 기본값으로 활성화됨)입니다.

타입: 문자열

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

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

ListRegions

지정된 계정의 모든 리전과 해당 옵트인 상태를 나열합니다. 선택적으로 이 목록은 `region-opt-status-contains` 파라미터로 필터링할 수 있습니다.

Request Syntax

```
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 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 Amazon Web Services 계정으로 설정됩니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 마세요. 대신 연락처가 검색하거나 수정하려는 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: `\d{12}`

필수 여부: 아니요

MaxResults

명령의 출력에서 반환되는 항목의 총 수입니다. 사용 가능한 총 항목 수가 지정된 값을 초과하는 경우 명령의 출력에 `NextToken`이 제공됩니다. 페이지 매김을 재개하려면 후속 명령의 `starting-token` 인수에 `NextToken` 값을 제공합니다. AWS CLI 외부에서 직접 `NextToken` 응답 요소를 사용하지 마십시오. 사용 예제는 AWS 명령줄 인터페이스 사용 설명서의 페이지 매김을 참조하세요.

타입: 정수

유효 범위: 최소값 1. 최대값 50.

필수 여부: 아니요

NextToken

페이지 매김을 시작할 위치를 지정하기 위한 토큰입니다. 이는 이전에 잘린 응답에서 도출된 `NextToken`입니다. 사용 예제는 AWS 명령줄 인터페이스 사용 설명서의 페이지 매김을 참조하세요.

유형: 문자열

길이 제한: 최소 길이는 0. 최대 길이는 1,000.

필수 여부: 아니요

RegionOptStatusContains

지정된 계정의 리전 목록을 필터링하는 데 사용할 리전 상태 목록(활성화 중, 활성화됨, 비활성화 중, 비활성화됨, 기본값으로 활성화됨)입니다. 예를 들어 ENABLING 값을 전달하면 리전 상태가 ENABLING인 리전 목록만 반환됩니다.

유형: 문자열 배열

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

필수 항목 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 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

NextToken

반환해야 할 데이터가 더 있는 경우 이 데이터가 채워집니다. `list-regions`의 `next-token` 요청 파라미터로 전달해야 합니다.

유형: 문자열

Regions

지정된 계정의 리전 목록이거나 필터링된 파라미터가 사용된 경우 `filter` 파라미터에 설정된 필터 기준과 일치하는 리전 목록입니다.

타입: Region 객체 배열

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

PutAccountName

지정된 계정의 계정 이름을 업데이트합니다. 이 API를 사용하려면 IAM 보안 주체에 `account:PutAccountName` IAM 권한이 있어야 합니다.

Request Syntax

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

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

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 액세스하거나 수정할 계정의 12자리 AWS 계정 ID 번호를 지정합니다.

이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 AWS 계정으로 설정됩니다.

이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 하며, 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하며, 조직은 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 말고, 검색하거나 수정하려는 연락처의 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: `\d{12}`

필수 여부: 아니요

AccountName

계정의 이름입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

패턴: `[ -;=?-~]+`

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

예

예시 1

다음 예시에서는 작업을 호출하는 데 자격 증명이 사용되는 계정의 이름을 업데이트합니다.

샘플 요청

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

{
   "AccountName":"MyAccount"
}
```

샘플 응답

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

예시 2

다음 예시에서는 조직의 지정된 멤버 계정의 계정 이름을 업데이트합니다. 조직의 관리 계정 또는 계정 관리 서비스의 위임된 관리자 계정의 자격 증명을 사용해야 합니다.

샘플 요청

```
POST / HTTP/1.1
```

```
X-Amz-Target: AWSAccountV20210201.PutAccountName

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount"
}
```

샘플 응답

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

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

PutAlternateContact

에 연결된 지정된 대체 연락처를 수정합니다 AWS 계정.

대체 고객 응대 작업을 사용하는 방법에 대한 자세한 내용은 의 대체 고객 응대 업데이트를 참조하세요 AWS 계정.

> **Note**
>
> 에서 AWS 계정 관리하는에 대한 대체 연락처 정보를 업데이트하려면 먼저 AWS 계정 관리와 조직 간의 통합을 활성화 AWS Organizations해야 합니다. 자세한 내용은 AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화를 참조하세요.

Request Syntax

```
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 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 액세스하거나 수정할 계정의 12자리 AWS 계정 ID 번호를 지정합니다.

이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 AWS 계정으로 설정됩니다.

이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 하며, 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하며, 조직은 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 말고, 검색하거나 수정하려는 연락처의 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: `\d{12}`

필수 여부: 아니요

AlternateContactType

생성 또는 업데이트하려는 대체 연락처를 지정합니다.

타입: 문자열

유효 값: `BILLING | OPERATIONS | SECURITY`

필수 사항 여부: 예

EmailAddress

대체 연락처의 이메일 주소를 지정합니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 254입니다.

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

필수 여부: 예

Name

대체 연락처의 이름을 지정합니다.

유형: 문자열

길이 제한: 최소 길이는 1. 최대 길이는 64.

필수 여부: 예

PhoneNumber

대체 연락처의 전화번호를 지정합니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 25입니다.

패턴: `[\s0-9()+-]+`

필수 여부: 예

Title

대체 연락처의 제목을 지정합니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 항목 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

예

예시 1

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

샘플 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
```

예시 2

다음 예제에서는 조직의 지정된 멤버 계정의 결제 대체 연락처를 설정하거나 덮어씁니다. 조직의 관리 계정 또는 계정 관리 서비스의 위임된 관리자 계정의 자격 증명을 사용해야 합니다.

샘플 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

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

PutContactInformation

AWS 계정의 기본 연락처 정보를 업데이트합니다.

기본 연락처 작업을 사용하는 방법에 대한 자세한 내용은 의 기본 연락처 업데이트를 참조하세요 AWS 계정.

Request Syntax

```
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 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 지정하지 않으면 기본적으로 작업을 호출하는 데 사용되는 자격 증명의 Amazon Web

Services 계정으로 설정됩니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직에 모든 기능이 활성화되어 있어야 하며, 조직은 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하며, 선택적으로 위임된 관리자 계정이 할당되어 있어야 합니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다. `AccountId` 파라미터를 포함하지 않고 독립 실행형 컨텍스트에서 작업을 호출해야 합니다.

조직의 멤버가 아닌 계정에서 이 작업을 호출하려면 이 파라미터를 지정하지 마세요. 대신 연락처가 검색하거나 수정하려는 계정에 속한 자격 증명을 사용하여 작업을 호출합니다.

유형: String

패턴: `\d{12}`

필수 여부: 아니요

ContactInformation

AWS 계정과 연결된 기본 연락처 정보의 세부 정보를 포함합니다.

타입: ContactInformation객체

필수 여부: 예

응답 구문

```
HTTP/1.1 200
```

Response Elements

작업이 성공하면 서비스가 비어 있는 HTTP 본문과 함께 HTTP 200 응답을 다시 전송합니다.

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

InternalServerException

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

HTTP 상태 코드: 500

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

StartPrimaryEmailUpdate

지정된 계정의 기본 이메일 주소를 업데이트하는 프로세스를 시작합니다.

Request Syntax

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

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

URI 요청 파라미터

요청은 URI 파라미터를 사용하지 않습니다.

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

AccountId

이 작업을 사용하여 AWS 계정 액세스하거나 수정할의 12자리 계정 ID 번호를 지정합니다. 이 파라미터를 사용하려면 호출자가 조직의 관리 계정 또는 위임된 관리자 계정의 자격 증명이어야 합니다. 지정된 계정 ID는 동일한 조직의 멤버 계정이어야 합니다. 조직은 모든 기능을 활성화해야 하며, 계정 관리 서비스에 대해 신뢰할 수 있는 액세스가 활성화되어 있어야 하고, 선택 사항으로 위임된 관리자 계정이 할당되어 있어야 합니다.

이 작업은 멤버 계정을 대상으로, 관리 계정이나 조직의 위임된 관리자 계정에서만 호출할 수 있습니다.

> **Note**
>
> 관리 계정은 자체 `AccountId`를 지정할 수 없습니다.

유형: String

패턴: `\d{12}`

필수 여부: 예

PrimaryEmail

지정된 계정에서 사용할 새 기본 이메일 주소(루트 사용자 이메일 주소라고도 함)입니다.

유형: 문자열

길이 제약: 최소 길이는 5입니다. 최대 길이는 64.

필수 항목 여부: 예

응답 구문

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

{
   "Status": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

Status

기본 이메일 업데이트 요청의 상태입니다.

타입: 문자열

유효 값: PENDING | ACCEPTED

오류

모든 작업에 공통되는 오류에 대한 내용은 일반적인 오류 섹션을 참조하세요.

AccessDeniedException

호출 자격 증명에 최소 필수 권한이 없어 작업이 실패했습니다.

HTTP 상태 코드: 403

ConflictException

리소스의 현재 상태에 충돌이 발생하여 요청을 처리할 수 없습니다. 예를 들어, 현재 비활성화된 리전(비활성화 상태)을 활성화하려고 하거나 계정의 루트 사용자 이메일을 이미 사용 중인 이메일 주소로 변경하려고 하면 이 문제가 발생합니다.

HTTP 상태 코드: 409

InternalServerException

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

HTTP 상태 코드: 500

ResourceNotFoundException

찾을 수 없는 리소스 지정으로 인해 작업이 실패했습니다.

HTTP 상태 코드: 404

TooManyRequestsException

너무 잦은 호출 및 스로틀 제한 초과로 인해 작업이 실패했습니다.

HTTP 상태 코드: 429

ValidationException

입력 파라미터 중 하나가 유효하지 않아 작업이 실패했습니다.

HTTP 상태 코드: 400

참고

언어별 AWS SDKs

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go용 SDK v2
- AWS Java V2용 SDK
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS PHP V3용 SDK
- AWS Python용 SDK
- AWS SDK for Ruby V3

다른 AWS 서비스의 관련 작업

다음 작업은와 관련이 AWS Account Management 있지만 네임스페이스의 AWS Organizations 일부입니다.

- CreateAccount
- CreateGovCloudAccount
- DescribeAccount

CreateAccount

`CreateAccount` API 작업은 AWS Organizations 서비스에서 관리하는 조직의 컨텍스트에서만 사용할 수 있습니다. API 작업은 해당 서비스의 네임스페이스에 정의됩니다.

자세한 내용은 AWS Organizations API 참조의 CreateAccount를 참조하세요.

CreateGovCloudAccount

`CreateGovCloudAccount` API 작업은 AWS Organizations 서비스에서 관리하는 조직의 컨텍스트에서만 사용할 수 있습니다. API 작업은 해당 서비스의 네임스페이스에 정의됩니다.

자세한 내용은 AWS Organizations API 참조의 CreateGovCloudAccount를 참조하세요.

DescribeAccount

`DescribeAccount` API 작업은 AWS Organizations 서비스에서 관리하는 조직의 컨텍스트에서만 사용할 수 있습니다. API 작업은 해당 서비스의 네임스페이스에 정의됩니다.

자세한 내용은 AWS Organizations API 참조의 DescribeAccount를 참조하세요.

데이터 타입

다음 데이터 타입이 지원됩니다.

- AlternateContact
- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

AWS 계정과 연결된 대체 연락처의 세부 정보가 포함된 구조

내용

AlternateContactType

대체 연락처의 유형입니다.

타입: 문자열

유효 값: `BILLING | OPERATIONS | SECURITY`

필수 여부: 아니요

EmailAddress

이 대체 연락처와 연결된 이메일 주소입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 254입니다.

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

필수 여부: 아니요

Name

이 대체 연락처와 연결된 이름입니다.

유형: 문자열

길이 제한: 최소 길이는 1. 최대 길이는 64.

필수 여부: 아니요

PhoneNumber

이 대체 연락처와 연결된 전화번호입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 25입니다.

패턴: `[\s0-9()+-]+`

필수 여부: 아니요

Title

이 대체 연락처와 연결된 제목입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50입니다.

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- AWS SDK for Ruby V3

ContactInformation

AWS 계정과 연결된 기본 연락처 정보의 세부 정보를 포함합니다.

내용

AddressLine1

기본 연락처 주소의 첫 번째 줄입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 60입니다.

필수 여부: 예

City

기본 연락처 주소의 도시입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 여부: 예

CountryCode

기본 연락처 주소의 ISO-3166 국가 코드 2자입니다.

유형: 문자열

길이 제약 조건: 고정 길이는 2입니다.

필수 여부: 예

FullName

기본 연락처 주소의 전체 이름입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50.

필수 여부: 예

PhoneNumber

기본 연락처 정보의 전화번호입니다. 숫자는 검증되며, 일부 국가에서는 활성화 여부를 확인합니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 20입니다.

패턴: `[+][\s0-9()-]+`

필수 여부: 예

PostalCode

기본 연락처 주소의 우편 번호입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 20입니다.

필수 여부: 예

AddressLine2

기본 연락처 주소의 두 번째 줄입니다(있는 경우).

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 60입니다.

필수 여부: 아니요

AddressLine3

기본 연락처 주소의 세 번째 줄입니다(있는 경우).

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 60입니다.

필수 여부: 아니요

CompanyName

기본 연락처 정보와 연결된 회사의 이름입니다(있는 경우).

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50입니다.

필수 여부: 아니요

DistrictOrCounty

기본 연락처 주소의 시/군/구 또는 카운티입니다(있는 경우).

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50입니다.

필수 여부: 아니요

StateOrRegion

기본 연락처 주소의 상태 또는 리전입니다. 우편 주소가 미국(US) 내에 있는 경우 이 필드의 값은 주 코드 2자(예: `NJ`) 또는 전체 주 이름(예: `New Jersey`)일 수 있습니다. 이 필드는 `US`, `CA`, `GB`, `DE`, `JP`, `IN`, `BR`의 국가에서 필수입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50입니다.

필수 여부: 아니요

WebsiteUrl

기본 연락처 정보와 연결된 웹 사이트의 URL입니다(있는 경우).

유형: 문자열

길이 제약 조건: 최소 길이는 1입니다. 최대 길이는 256.

필수 여부: 아니요

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK

- AWS SDK for Ruby V3

Region

이는 지정된 계정의 리전을 표현하는 구조로, 이름과 옵트인 상태로 구성됩니다.

내용

RegionName

지정된 리전의 리전 코드(예: `us-east-1`)입니다.

유형: 문자열

길이 제약: 최소 길이 1. 최대 길이는 50입니다.

필수 여부: 아니요

RegionOptStatus

리전이 거칠 수 있는 잠재적 상태 중 하나(활성화됨, 활성화 중, 비활성화됨, 비활성화 중, 기본값으로 활성화됨)입니다.

타입: 문자열

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

필수 여부: 아니요

참고

언어별 AWS SDKs

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

ValidationExceptionField

입력이 지정된 필드의 AWS 서비스에서 지정한 제약 조건을 충족하지 못했습니다.

내용

message

검증 예외에 대한 메시지입니다.

유형: 문자열

필수 항목 여부: 예

name

잘못된 항목이 감지된 필드 이름입니다.

유형: 문자열

필수 항목 여부: 예

참고

언어별 AWS SDKs

- AWS SDK for C++
- AWS Java V2용 SDK
- 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 설명서의 AWS API 요청 서명을 참조하세요.

Action

수행할 작업입니다.

타입: 문자열

필수 항목 여부: 예

Version

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

타입: 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.

타입: 문자열

유효 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 서명된 AWS API 요청 생성을 참조하세요.

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

타입: 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 설명서의 AWS API 요청 서명 요소를 참조하세요.

유형: 문자열

필수 항목 여부: 조건부

X-Amz-Security-Token

AWS Security Token Service ()에 대한 호출을 통해 얻은 임시 보안 토큰입니다AWS STS. AWS STS의 임시 보안 인증 정보를 지원하는 서비스 목록은 IAM 사용 설명서의 IAM으로 작업하는AWS 서비스를 참조하세요.

조건:에서 임시 보안 자격 증명을 사용하는 경우 보안 토큰을 포함해야 AWS STS합니다.

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.

타입: 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 서명된 AWS API 요청 생성을 참조하세요.

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

타입: 문자열

필수 항목 여부: 조건부

일반적인 오류

이 섹션에서는 모든 AWS 서비스의 API 작업에 공통적인 오류를 나열합니다. 이 서비스의 API 작업에 대한 오류는 해당 API 작업 항목을 참조하세요.

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 레코드에 없습니다.

HTTP 상태 코드: 403

NotAuthorized

이 작업을 수행하려면 권한이 있어야 합니다.

HTTP 상태 코드: 400

OptInRequired

AWS 액세스 키 ID에는 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 실패했습니다.

HTTP 상태 코드: 503

ThrottlingException

요청 제한 때문에 요청이 거부되었습니다.

HTTP 상태 코드: 400

ValidationError

입력이 AWS 서비스에서 지정한 제약 조건을 충족하지 못합니다.

HTTP 상태 코드: 400

HTTP 쿼리 요청을 통한 API 호출

이 섹션에는 AWS 계정 관리를 위한 쿼리 API 사용에 대한 일반적인 정보가 포함되어 있습니다. API 작업 및 오류에 대한 자세한 정보는 API 참조를 참조하십시오.

> **Note**
>
> AWS Account Management Query API를 직접 호출하는 대신 AWS SDKs. AWS SDKs는 다양한 프로그래밍 언어 및 플랫폼(Java, Ruby, .NET, iOS, Android 등)을 위한 라이브러리 및 샘플 코드로 구성됩니다. SDKs는 AWS 계정 관리 및에 대한 프로그래밍 방식 액세스를 생성하는 편리한 방법을 제공합니다 AWS. 예를 들어 SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. 다운로드 및 설치 방법을 포함하여 AWS SDKs에 대한 자세한 내용은 Amazon Web Services용 도구를 참조하세요.

AWS 계정 관리용 쿼리 API를 사용하면 서비스 작업을 호출할 수 있습니다. 쿼리 API 요청은 수행할 작업을 나타내는 `Action` 파라미터를 포함해야 하는 HTTPS 요청입니다. AWS 계정 관리는 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. 제한은 브라우저에 따라 다르지만, 일반적으로 2,048바이트입니다. 따라서 더 큰 크기가 필요한 쿼리 API 요청의 경우 POST 요청을 사용해야 합니다.

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

주제

- 엔드포인트
- HTTPS 필요
- AWS Account Management API 요청 서명

엔드포인트

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

모든 서비스의 AWS 엔드포인트 및 리전에 대한 자세한 내용은의 리전 및 엔드포인트를 참조하세요AWS 일반 참조.

HTTPS 필요

쿼리 API는 보안 자격 증명과 같이 민감한 정보를 반환할 수 있으므로 HTTPS를 이용해 모든 API 요청을 암호화해야 합니다.

AWS Account Management API 요청 서명

액세스 키 ID와 보안 액세스 키를 사용하여 요청에 서명해야 합니다. AWS Account Management의 일상적인 작업에 AWS 루트 계정 자격 증명을 사용하지 않는 것이 좋습니다. AWS Identity and Access Management (IAM) 사용자에 대한 자격 증명 또는 IAM 역할과 함께를 사용하는 것과 같은 임시 자격 증명을 사용할 수 있습니다.

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

자세한 내용은 다음 자료를 참조하세요.

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

- IAM의 보안 모범 사례 - IAM 서비스를 사용하여 AWS Account Management의 리소스를 포함한 AWS 리소스를 보호하는 데 도움이 되는 제안을 제공합니다.
- IAM의 임시 자격 증명 – 임시 보안 자격 증명을 생성하고 사용하는 방법에 대해 설명합니다.

에 대한 할당량 AWS Account Management

AWS 계정 에는 각 AWS 서비스에 대해 이전에 제한이라고 하는 기본 할당량이 있습니다. 달리 명시되지 않는 한 각 할당량은 AWS 리전고유합니다.

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

리소스	할당량
대상 계정당 최대 StartPrimaryEmailUpdate 요청 수	3회/30초
의 대체 연락처 수 AWS 계정	3 - BILLING, SECURITY 및 OPERATIONS 에 대해 각각 하나씩
계정당 동시 리전 설정 요청 수	6
조직당 동시 리전 설정 요청 수	50
호출자 계정당 AcceptPrimaryEmailUpdate 요청 속도	초당 1회, 초당 1회로 버스트
계정당 DeleteAlternateContact 요청 속도	초당 1회, 초당 6회로 버스트
계정당 DisableRegion 요청 속도	초당 1회, 초당 1회로 버스트
계정당 EnableRegion 요청 속도	초당 1회, 초당 1회로 버스트
호출자 계정당 GetAccountInformation 요청 속도	초당 3회, 초당 3회로 버스트
계정당 GetAlternateContact 요청 속도	초당 10회, 초당 15회로 버스트
계정당 GetContactInformation 요청 속도	초당 10회, 초당 15회로 버스트
호출자 계정당 GetPrimaryEmail 요청 속도	초당 3회, 초당 3회로 버스트
계정당 GetRegionOptStatus 요청 속도	초당 5회, 초당 5회로 버스트

리소스	할당량
계정당 ListRegions 요청 속도	초당 5회, 초당 5회로 버스트
호출자 계정당 PutAccountName 요청 속도	초당 1회, 초당 1회로 버스트
계정당 PutAlternateContact 요청 속도	초당 5회, 초당 8회로 버스트
계정당 PutContactInformation 요청 속도	초당 5회, 초당 8회로 버스트
호출자 계정당 StartPrimaryEmailUpdate 요청 속도	초당 1회, 초당 1회로 버스트

인도의 계정 관리

신규에 가입 AWS 계정 하고 연락처 및 결제 주소로 인도를 선택하는 경우 사용자 계약은 인도의 현지 AWS 판매자인 Amazon Web Services India Private Limited(AWS 인도)와 체결됩니다. AWS 인도는 결제를 관리하며 인보이스 총액은 미국 달러(USD)가 아닌 인도 루피(INR)로 표시됩니다. 관리 방법에 대한 자세한 내용은 단원을 AWS 계정참조하십시오구성 AWS 계정.

계정이 AWS 인도에 있는 경우이 주제의 절차에 따라 계정을 관리합니다. 이 주제에서는 AWS India 계정에 가입하고, AWS India 계정에 대한 정보를 편집하고, 고객 확인을 관리하고, 영구 계정 번호(PAN)를 추가하거나 편집하는 방법을 설명합니다.

가입 중 신용 카드 확인의 일환으로 AWS India는 신용 카드에 2INR을 청구합니다. AWS India는 확인이 완료된 후 2INR을 환불합니다. 확인 프로세스의 한 부분으로 AISPL은 신용 카드 2INR을 부과합니다.

주제

AWS 인도를 AWS 계정 사용하여 생성

AWS India는 인도 AWS 에 있는의 현지 판매자입니다. 연락처 및 결제 주소가 인도에 있고 계정을 생성하려는 경우 다음 절차에 따라 AWS India 계정에 가입합니다.

AWS India 계정에 가입하려면

1. Amazon Web Services 홈 페이지를 엽니다.
2. 생성을 AWS 계정 선택합니다.

> **Note**
>
> AWS 최근에에 로그인한 경우 해당 옵션이 없을 수 있습니다. 대신 콘솔에 로그인을 선택합니다. 새 AWS 계정생성 옵션이 여전히 보이지 않는 경우 다른 계정으로 로그인을 선택한 다음 새 AWS 계정생성을 선택합니다.

3. 계정 정보를 입력하고 이메일 주소를 확인한 다음 계정의 강력한 비밀번호를 선택합니다.

4. 비즈니스 또는 개인을 선택합니다. 개인 계정과 비즈니스 계정의 특성과 기능은 동일합니다.
5. 회사 또는 개인 연락처 정보를 입력합니다. 연락처 또는 청구 주소가 인도에 있는 경우 인도 컴퓨터 비상 대응 팀(CERT-In) 규정에 따라 AWS 는 AWS 서비스에 대한 액세스 권한을 부여하기 전에 자격 증명 정보를 수집하고 검증해야 합니다.

   연락처 또는 청구 정보 중에서 선택한 이름이 고객 확인에 사용할 문서에 표시된 이름과 반드시 정확히 일치해야 합니다. 예를 들어 법인 설립 인증서를 사용하여 비즈니스 계정을 확인하려면 문서에 표시되는 비즈니스 이름을 제공해야 합니다. 수락되는 문서 유형 목록은 the section called “고객 확인에 수락되는 인도 문서”의 섹션을 참조하세요.
6. 고객 계약을 읽은 후 이용 약관 확인란을 선택한 다음에 계속을 선택합니다.
7. 사용할 결제 방법을 청구 정보 페이지에서 입력합니다. 확인 과정의 일환으로 CVV를 제공해야 합니다.
8. PAN이 있습니까?에서 세금 인보이스에 표시할 소득세 번호(PAN)가 있는 경우 예를 선택한 다음 PAN을 입력합니다. PAN이 없거나 가입 후 추가하려는 경우 아니요를 선택합니다.
9. 확인 및 계속을 선택합니다. AWS 인도는 확인 프로세스의 일부로 카드에 2INR을 청구합니다. AWS 인도는 확인이 완료된 후 2INR을 환불합니다.
10. 신원 확인 페이지에서 계정 등록의 기본 목적을 선택합니다.
11. 계정 소유자를 가장 잘 나타내는 소유권 유형을 선택합니다. 소유권 유형으로 회사, 조직 또는 파트너십을 선택하는 경우 주요 관리자의 이름을 입력합니다. 주요 관리 담당자는 이사, 운영 책임자 또는 비즈니스 운영 담당자일 수 있습니다.
12. 선택한 소유권 유형에 따라 확인에 사용할 수락된 인도 문서 유형을 선택하고 본인의 정보를 입력합니다.

    > **Note**
    >
    > 개인 계정이 있고 인도 정부에서 발급하지 않은 운전면허증을 사용할 계획인 경우 확인을 위해 다른 유형의 개인 문서를 사용할 것을 권장합니다.

13. 고객 확인에 사용할 이름을 선택합니다.

    청구지 및 연락처 정보에 있는 이름이 인도 주소와 연결된 경우 선택 항목에 표시됩니다. 선택한 이름이 고객 확인에 사용할 문서 유형의 이름과 일치하는지 확인합니다. 청구지 또는 연락처 주소와 연결된 이름을 변경해야 하는 경우 계정 등록을 완료한 후에 변경할 수 있습니다.
14. 확인용 정보 제출에 동의한 다음에 계속을 선택합니다.

계정 등록을 완료하면 고객 확인 결과에 대한 알림을 이메일로 받게 됩니다. 계정 설정의 고객 확인 페이지 또는 나중에 AWS 상태 대시보드에서 상태를 확인할 수도 있습니다. AWS 서비스에 액세스하려면 고객 확인을 통과해야 합니다.

15. 휴대폰 번호를 문자 메시지(SMS)로 인증할지, 음성 통화로 인증할지를 선택합니다.
16. 국가 또는 지역 코드를 선택한 다음에 휴대폰 번호를 입력합니다.
17. 보안 검사를 완료하세요.
18. SMS 보내기 또는 지금 전화하기를 선택합니다. 잠시 후에 휴대폰으로 SMS 또는 자동 통화를 통해 네 자리 PIN을 받게 됩니다.
19. 신원 확인 페이지에서 받은 PIN을 입력하고 계속를 선택합니다.
20. 지원 요금제 선택 페이지에서 지원 요금제을 선택한 다음에 등록 완료를 선택합니다. 결제 방법과 고객 확인이 확인된 후 계정이 활성화되고 계정 활성화에 대한 확인 이메일을 받게 됩니다.

> **Note**
>
> 고객 확인을 완료하고 이전에 신원 확인에 사용했던 이름, 주소 또는 문서 유형을 편집한 경우 고객 확인을 다시 업데이트하고 완료해야 할 수 있습니다. 자세한 내용은 the section called “고객 확인 정보 편집” 단원을 참조하십시오.

고객 확인 정보 관리

인도 컴퓨터 비상 대응 팀(CERT-In) 규정에 따라 AWS 는 AWS 서비스에 대한 신규 또는 지속적인 액세스 권한을 부여하기 전에 자격 증명 정보를 수집하고 검증해야 합니다. 제공한 인도 청구지 또는 연락처 주소의 이름을 통해 자격 증명이 확인되어야 합니다. 확인 중에 AWS 는 문서 번호가 유효한지, 제공한 이름이 고객 확인에 사용하는 문서와 연결된 이름과 일치하는지 확인합니다. 연락처 또는 결제 정보 중에서 선택한 이름은 문서에 표시되는 이름과 정확히 일치해야 합니다.

결제 이름 및 주소를 업데이트하려면 Payment preferences 페이지를 참조하세요. 연락처 이름 및 주소를 업데이트하려면 the section called “AWS 계정의 기본 연락처 업데이트”의 섹션을 참조하세요. 이름이나 청구 정보 또는 연락처 정보의 인도 주소와 같이 이전에 고객 확인에 사용한 정보를 편집하는 경우 고객 확인 정보를 업데이트하고 다시 제출해야 할 수 있습니다.

고객 확인 상태 확인

고객 확인 페이지에서 언제든지 고객 확인 상태를 볼 수 있습니다. 확인 상태가 확인 필요 또는 확인 실패인 경우 고객 확인 정보를 생성하고 업데이트한 후 확인을 위해 다시 제출합니다.

고객 인증 정보 생성

고객 확인을 완료하려면 승인된 인도 문서의 정보를 제공해야 합니다. 수락되는 문서 유형 목록은 the section called “고객 확인에 수락되는 인도 문서”의 섹션을 참조하세요.

1. AWS Management Console에 로그인합니다.
2. 상단 오른쪽 모서리의 탐색 모음에서 계정 이름(또는 별칭)을 선택한 다음 계정을 선택합니다.
3. 기타 설정에서 고객 확인을 선택합니다.

   이전에 고객 확인 정보를 아직 제공하지 않은 경우 Create customer verification 페이지가 표시됩니다.
4. 고객 확인에 사용할 문서의 이름과 정확히 일치하는 이름을 선택합니다. 예를 들어 법인 설립 인증서를 사용하여 비즈니스 계정을 확인하려면 문서에 표시되는 비즈니스 이름을 제공해야 합니다.
5. 페이지에서 요청한 나머지 정보를 작성합니다. 선택한 문서 유형에 따라 문서의 전면과 후면 모두의 사본을 업로드해야 할 수 있습니다. 이미지 파일을 업로드하는 경우 문서의 모든 정보가 표시되고 읽을 수 있는지 확인합니다.
6. 제출을 선택합니다.

   이메일 또는 AWS 상태 대시보드를 통해 고객 확인 결과와 다음 단계에 대한 알림을 받게 됩니다.

고객 확인 정보 편집

계정 등록의 기본 목적, 조직 유형, 이름, 문서 유형, 문서 업로드 또는 확인에 사용할 문서 정보와 같은 고객 확인 정보를 편집할 수 있습니다.

고객 확인에 사용할 이름 또는 문서 유형을 편집하거나 문서 정보를 업데이트하는 경우 변경 사항을 저장하여 신원을 다시 확인해야 합니다.

1. AWS Management Console에 로그인합니다.
2. 상단 오른쪽 모서리의 탐색 모음에서 계정 이름(또는 별칭)을 선택한 다음 계정을 선택합니다.
3. 기타 설정에서 고객 확인을 선택합니다.
4. 편집을 선택한 다음 변경하려는 정보를 업데이트합니다.

   정보를 업데이트할 때 다음 지침을 참고하세요.

- 다른 이름을 선택하는 경우 이름은 고객 확인에 사용할 문서의 이름과 정확히 일치해야 합니다. 예를 들어 법인 설립 인증서를 사용하여 비즈니스 계정을 확인하려면 문서에 표시되는 비즈니스 이름을 제공해야 합니다.
- 다른 문서 유형을 선택하는 경우 문서의 앞뒤(해당하는 경우) 사본을 업로드해야 합니다. 문서 업로드의 모든 정보는 표시 및 읽을 수 있어야 합니다.
- 개인 계정이 있고 인도 정부에서 발급하지 않은 운전면허증을 사용할 계획인 경우 확인을 위해 다른 유형의 개인 문서를 사용할 것을 권장합니다.

  수락되는 문서 유형 목록은 the section called “고객 확인에 수락되는 인도 문서”의 섹션을 참조하세요.

5. 제출을 선택합니다.

   저장한 변경 사항의 유형으로 인해 신원을 다시 확인해야 하는 경우 고객 확인 결과와 다음 단계를 이메일로 알려드립니다. 고객 확인 페이지 또는 AWS 상태 대시보드로 돌아가서 결과를 볼 수도 있습니다.

고객 확인에 수락되는 인도 문서

인도 정부에서 발급한 다음과 같은 문서 유형이 고객 확인에 수락됩니다.

> **Note**
>
> 아래에 공유된 링크는 인도 정부에서 변경할 수 있습니다.

- PAN 카드 - 디지털 형식과 물리적 형식 모두에서 사용할 수 있는 소득세 번호(PAN) 카드에는 인도 소득세 부서에서 개인, 회사 및 법인에 발급한 고유한 영숫자 식별자가 포함되어 있습니다. PAN은 글자와 숫자를 포함하여 10자가 **AAAAA1111A** 형식으로 구성되어 있습니다. 이 문서를 검증에 사용하려면 PAN 문서에 표시되는 생년월일(개인) 또는 법인 설립일(비즈니스)도 제공하고 카드 앞면을 업로드해야 합니다. PAN의 유효성을 확인하려면 인도 국세청 공식 웹사이트를 참조하세요.
- 투표자 ID 카드/EPIC - 선거인 사진 신분증(EPIC)라고도 하는 투표자 ID 카드에는 인도의 선거관리위원회가 인도의 적격 투표자에게 발급한 고유 식별 번호가 포함되어 있습니다. 유권자 ID/EPIC 번호는 글자와 숫자를 포함하여 열 자로 구성되어 있습니다. 인도 선거관리위원회 공식 웹사이트를 참조하여 유권자 ID의 유효성을 확인할 수 있습니다. 이 문서를 확인에 사용하려면 카드의 앞면과 뒷면을 모두 업로드해야 합니다.

- 운전면허증 - 인도 정부에서 운전면허증을 발급하지 않은 경우 확인에 다른 문서 유형을 사용하는 것이 좋습니다. 운전면허증 번호는 글자, 숫자, 공백, 하이픈을 포함하여 12자~16자로 구성되어 있습니다. 확인에 이 문서를 사용하려면 생년월일을 제공하고 카드의 앞면과 뒷면을 모두 업로드해야 합니다. 운전면허증의 유효성을 확인하려면 인도 도로운송 고속도로부의 Parivahan Sewa 웹사이트를 참조하세요.
- 여권 - 여권은 인도 시민권 증명 역할을 하며 해외 여행의 신분증으로 사용할 수 있습니다. Passport Seva Kendra(PSK)에서 발급하는 여권에서 여권 파일 번호는 개인의 여권과 연결된 고유한 영숫자 식별자입니다. 여권 파일 번호는 글자와 숫자를 포함하여 열다섯 자로 구성되어 있습니다. 여권 번호와 다른 여권 파일 번호는 인도 여권의 마지막 페이지 중 하나에서 찾을 수 있습니다. 확인에 이 문서를 사용하려면 생년월일을 제공하고 여권의 첫 번째 페이지와 마지막 페이지(여권 파일 번호 포함)를 모두 업로드해야 합니다. 외교부의 Passport Seva Kendra 사이트로 이동하여 여권 파일 번호의 유효성을 확인할 수 있습니다.

  > **Note**
  >
  > 고객 확인을 위해 인도에서 발급된 인도 여권의 여권 파일 번호만 허용됩니다. 여권이 다른 국가의 인도 외교 공관에서 발급되었다면 고객 확인에 다른 인도 문서를 사용하세요.

- 법인 설립 증명서 - 법인 설립 증명서는 법인으로 사업체를 등록한 날짜를 기재한 법인업무부(MCA)에서 발행한 문서입니다. 인증서는 인도에 등록된 회사를 고유하게 식별하고 추적하는 데 사용됩니다. 각 인증서에는 문자와 숫자를 포함하여 21자로 구성된 고유한 영숫자 식별자인 기업 식별 번호(CIN)가 포함되어 있습니다. 이 문서를 확인에 사용하려면 인증서의 통합 문서를 업로드해야 합니다. 법인업무부 포털로 이동하여 CIN의 유효성을 확인할 수 있습니다.

다양한 인도 문서 유형이 개인 및 기업 계정용으로 수락됩니다.

- 개인 계정의 경우 - PAN 카드, 유권자 ID 카드/EPIC, 운전면허증, 여권.
- 비즈니스 계정의 경우 - PAN 카드 및 법인 설립 증명서.

AWS 인도 계정 관리

다음 작업을 제외하고 계정 관리 절차는 인도 이외의 국가에서 생성된 계정과 동일합니다. 계정 관리에 대한 일반적인 정보는 계정 구성 섹션을 참조하세요.

AWS Management Console 를 사용하여 다음 작업을 수행합니다.

- 소득세 번호 추가 또는 편집

- 여러 소득세 번호 편집
- the section called “고객 확인 정보 관리”
- 여러 납세자 식별 번호(GST) 편집
- 세금 계산서 보기

계정 관리 사용 설명서의 문서 이력

다음 표에서는 AWS 계정 관리에 대한 설명서 릴리스를 설명합니다.

변경 사항	설명	날짜
새 계정 이름 APIs	계정 이름을 보거나 수정할 수 있는 새 GetAccountInformation, 및 PutAccountName APIs를 지원합니다.	2025년 4월 22일
보안 챌린지 질문 편집 지원 종료	지원이 종료되었으므로 가이드에서 보안 챌린지 질문 편집 주제를 제거했습니다.	2025년 1월 6일
새 기본 이메일 API	의 모든 멤버 계정에 대한 루트 사용자 이메일 주소 중앙에서 업데이트하는 새로운 GetPrimaryEmail StartPrimaryEmailUpdate, 및 AcceptPrimaryEmailUpdate APIs를 지원합니다 AWS Organizations. 자세한 내용은 AWS Organizations 사용 설명서의 멤버 계정의 루트 사용자 이메일 주소A 업데이트를 참조하세요.	2024년 6월 6일
계정 해지 주제 다시 쓰기	멤버 및 관리 계정을 해지하는 방법에 대한 단계를 추가하는 등 전체 계정 해지 주제를 완전히 점검했습니다.	2024년 2월 1일
새 보안 챌린지 질문 추가에 대한 지원 종료	계정 페이지에서 새 챌린지 질문을 추가하는 옵션이 제거되	2024년 1월 5일

	었음을 알리는 새 콘텐츠가 추가되었습니다.	
aws-portal 네임스페이스에 대한 지원 종료	AWS Identity and Access Management 이전에 계정을 관리하는 데 사용된 (IAM) 작업 (예: aws-portal:ModifyAccount 및 aws-portal:ViewAccount)이 표준 지원이 종료되었습니다.	2024년 1월 1일
리전 주제 다시 쓰기	확장 및 축소 제어 추가를 포함하여 전체 리전 주제를 완전히 점검했습니다.	2023년 10월 8일
루트 사용자 주제를 IAM 사용 설명서로 재배치	루트 사용자에 대한 토론을 하나의 주제로 통합하고 IAM 사용 설명서로 이동된 루트 사용자 주제에 상호 참조 링크를 추가했습니다.	2023년 9월 18일
기본 계정 연락처 주제에 새 섹션 추가	새 전화번호 및 이메일 주소 요구 사항 섹션이 추가되었습니다.	2023년 9월 12일
새 연락처 정보 API	신규 GetContactInformation 및 PutContactInformation API를 지원합니다.	2022년 7월 22일
AWS 계정 관리는 이제 콘솔을 AWS Organizations 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	AWS 계정 관리 참조 가이드의 최초 릴리스	2021년 9월 30일

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