AWS Identity and Access Management

사용 설명서

AWS Identity and Access Management: 사용 설명서

Table of Contents

IAM이란?

Follow us on Twitter

AWS Identity and Access Management(IAM)는 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스입니다. IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어합니다.

AWS 계정을 처음 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 SSO(Single Sign-In) ID로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업은 물론 관리 작업에도 루트 사용자를 사용하지 않는 것이 좋습니다. 대신 IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례를 준수하십시오. 그런 다음 루트 사용자 자격 증명을 안전하게 보관해 두고 몇 가지 계정 및 서비스 관리 작업을 수행할 때만 해당 자격 증명을 사용합니다.

주제

IAM 소개 동영상

AWS 교육 및 자격증 팀에서 IAM에 대한 10분 소개 동영상을 제공합니다.

AWS Identity and Access Management 소개

IAM 기능

IAM에서는 다음 기능을 제공합니다.

AWS 계정에 대한 공유 액세스

암호나 액세스 키를 공유하지 않고도 AWS 계정의 리소스를 관리하고 사용할 수 있는 권한을 다른 사람에게 부여할 수 있습니다.

세분화된 권한

리소스에 따라 여러 사람에게 다양한 권한을 부여할 수 있습니다. 예를 들어 일부 사용자에게는 Amazon Elastic Compute Cloud(Amazon EC2), Amazon Simple Storage Service(Amazon S3), Amazon DynamoDB, Amazon Redshift 및 기타 AWS 서비스에 대한 전체 액세스 권한을 허용하고 다른 사용자에게는 일부 S3 버킷에 대한 읽기 전용 권한, 일부 EC2 인스턴스를 관리할 수 있는 권한 또는 결제 정보에만 액세스할 수 있는 권한을 허용할 수 있습니다.

Amazon EC2에서 실행되는 애플리케이션을 위한 보안 AWS 리소스 액세스

EC2 인스턴스에서 실행되는 애플리케이션의 경우 IAM 기능을 사용하여 자격 증명을 안전하게 제공할 수 있습니다. 이러한 자격 증명은 애플리케이션에 다른 AWS 리소스에 액세스할 수 있는 권한을 제공합니다. 예를 들면 이러한 리소스에는 S3 버킷 및 DynamoDB 테이블이 있습니다.

멀티 팩터 인증(MFA)

보안 강화를 위해 계정과 개별 사용자에게 2팩터 인증을 추가할 수 있습니다. MFA를 사용할 경우 계정 소유자나 사용자가 계정 작업을 위해 암호나 액세스 키뿐 아니라 특별히 구성된 디바이스의 코드도 제공해야 합니다.

자격 증명 연동

기업 네트워크나 인터넷 자격 증명 공급자와 같은 다른 곳에 이미 암호가 있는 사용자에게 AWS 계정에 대한 임시 액세스 권한을 부여할 수 있습니다.

보장을 위한 자격 증명 정보

AWS CloudTrail을 사용하는 경우 계정의 리소스를 요청한 사람에 대한 정보가 포함된 로그 레코드를 받게 됩니다. 이 정보는 IAM 자격 증명을 기반으로 합니다.

PCI DSS 준수

IAM에서는 전자 상거래 웹사이트 운영자 또는 서비스 공급자에 의한 신용 카드 데이터의 처리, 저장 및 전송을 지원하며, Payment Card Industry(PCI) Data Security Standard(DSS) 준수를 검증 받았습니다. AWS PCI 규정 준수 패키지의 사본을 요청하는 방법 등 PCI DSS에 대해 자세히 알아보려면 PCI DSS 레벨 1을 참조하십시오.

많은 AWS 서비스와의 통합

IAM과 함께 사용할 수 있는 AWS 서비스의 목록은 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하십시오.

최종 일관성

IAM은 다른 많은 AWS 서비스처럼eventually consistent에 해당됩니다. IAM에서는 전 세계의 Amazon 데이터 센터 내의 여러 서버로 데이터를 복제함으로써 고가용성을 구현합니다. 일부 데이터를 변경하겠다는 요청이 성공하면 변경이 실행되고 그 결과는 안전하게 저장됩니다. 그러나 변경 사항은 IAM에 두루 복제되어야 하고, 여기에는 일정한 시간이 걸립니다. 그러한 변경 사항에는 사용자, 그룹, 역할 또는 정책을 만들거나 업데이트한 것이 포함됩니다. 그러한 IAM 변경 사항을 애플리케이션의 중요한 고가용성 코드 경로에 포함시키지 않는 것이 좋습니다. 대신 자주 실행하지 않는 별도의 초기화 루틴이나 설정 루틴에서 IAM을 변경하십시오. 또한 프로덕션 워크플로우에서 변경 사항을 적용하기 전에 변경 사항이 전파되었는지 확인하십시오. 자세한 내용은 변경 사항이 매번 즉시 표시되는 것은 아닙니다 (p. 536) 단원을 참조하십시오.

무료 사용

AWS Identity and Access Management(IAM) 및 AWS Security Token Service(AWS STS)은 추가 비용 없이 AWS 계정에 제공되는 기능입니다. IAM 사용자 또는 AWS STS 임시 보안 자격 증명을 사용하여 다른 AWS 서비스에 액세스하는 경우에만 요금이 부과됩니다. 다른 AWS 제품 요금에 대한 자세한 내용은 Amazon Web Services 요금 페이지를 참조하십시오.

IAM에 액세스

다음 방법 중 하나를 사용하여 AWS Identity and Access Management(으)로 작업할 수 있습니다.

AWS Management 콘솔

콘솔은 IAM 및 AWS 리소스를 관리하기 위한 브라우저 기반 인터페이스입니다. 콘솔을 통한 IAM 액세스에 대한 자세한 내용은 IAM 콘솔 및 로그인 페이지 (p. 71) 단원을 참조하십시오. 콘솔 사용법을 안내하는 자습서는 첫 번째 IAM 관리자 및 그룹 생성 (p. 20)을 참조하십시오.

AWS 명령줄 도구

AWS 명령줄 도구를 통해 시스템 명령줄에서 명령을 실행하여 IAM 및 AWS 작업을 수행할 수 있습니다. 명령줄을 사용하는 것이 콘솔을 사용하는 것보다 더 빠르고 편리할 수 있습니다. AWS 작업을 수행하는 스크립트를 작성할 때도 명령줄 도구가 유용합니다.

AWS에서는 AWS Command Line Interface(AWS CLI) 및 Windows PowerShell용 AWS 도구라는 두 가지 명령줄 도구 세트를 제공합니다. AWS CLI 설치 및 사용에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서 단원을 참조하십시오. Windows PowerShell용 도구 설치 및 사용에 대한 자세한 내용은 Windows PowerShell용 AWS 도구 사용 설명서 단원을 참조하십시오.

AWS SDK

AWS에서는 다양한 프로그래밍 언어 및 플랫폼(Java, Python, Ruby, .NET, iOS, Android 등)을 위한 라이브러리와 샘플 코드로 구성된 소프트웨어 개발 키트(SDK)를 제공합니다. SDK를 사용하면 편리하게 IAM 및 AWS에 프로그래밍 방식으로 액세스할 수 있습니다. 예를 들어 SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. 다운로드 및 설치 방법을 비롯하여 AWS SDK에 대한 자세한 내용은 Amazon Web Services용 도구 페이지를 참조하십시오.

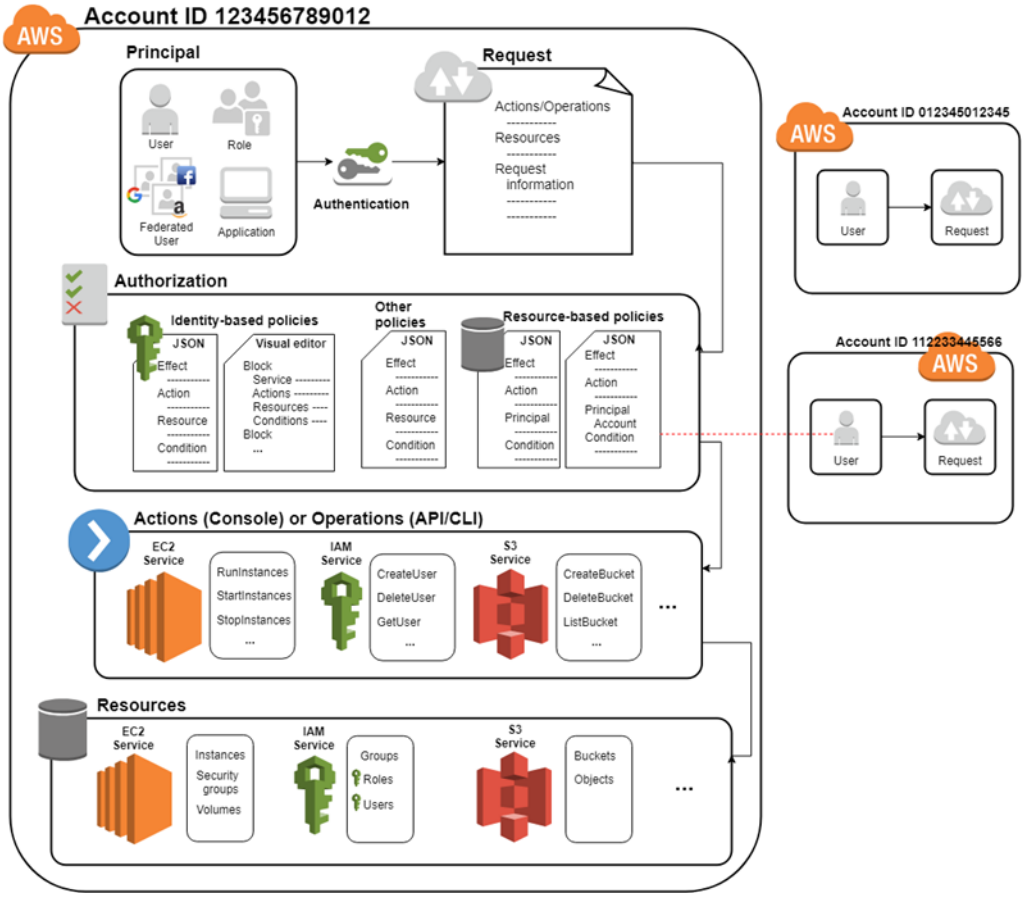
IAM HTTPS API

서비스로 직접 HTTPS 요청을 실행할 수 있는 IAM HTTPS API를 사용하여 프로그래밍 방식으로 IAM 및 AWS에 액세스할 수 있습니다. HTTPS API를 사용할 때는 자격 증명을 사용하여 요청에 디지털 방식으로 서명하는 코드를 포함해야 합니다. 자세한 내용은 HTTP 쿼리 요청을 통한 API 호출 (p. 1748) 및 IAM API Reference 단원을 참조하십시오.

IAM 작동 방식 이해

사용자를 생성하기 전에 IAM 작동 방식을 이해해야 합니다. IAM은 계정에 대한 인증 및 권한 부여를 제어하는 데 필요한 인프라를 제공합니다. IAM 인프라에는 다음 요소가 포함되어 있습니다.

주제



약관

IAM 용어에 대해 자세히 알아봅니다.

리소스

IAM에 저장된 사용자, 그룹, 정책 및 자격 증명 공급자 객체. 다른 AWS 서비스와 마찬가지로 IAM에서 리소스를 추가, 편집 및 제거할 수 있습니다.

ID

식별 및 그룹화에 사용되는 IAM 리소스 객체입니다. 정책을 IAM 자격 증명에 연결할 수 있습니다. 여기에는 사용자, 그룹 및 역할이 포함됩니다.

엔터티

AWS가 인증에 사용하는 IAM 리소스 객체입니다. 여기에는 IAM 사용자, 연합된 사용자 및 수임된 IAM 역할이 포함됩니다.

보안 주체

AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 사용하여 로그인하고 AWS에 요청하는 사람 또는 애플리케이션입니다.

보안 주체

보안 주체란 AWS 리소스에 대한 작업을 요청할 수 있는 사람 또는 애플리케이션입니다. 보안 주체는 AWS 계정 루트 사용자 또는 IAM 엔터티로 인증되어 AWS에 요청합니다. 일별 작업에 대한 루트 사용자 자격 증명은 사용하지 않는 것이 가장 좋습니다. 대신 IAM 엔터티(사용자 및 역할)를 생성합니다. 애플리케이션이 AWS 계정에 액세스할 수 있도록 연동 사용자 또는 프로그래밍 방식의 액세스를 지원할 수 있습니다.

요청

보안 주체가 AWS Management 콘솔, AWS API 또는 AWS CLI를 사용하려고 시도하면 해당 보안 주체가 요청을 AWS에 전송합니다. 이 요청에는 다음 정보가 포함되어 있습니다.

- 작업 또는 작동 – 보안 주체가 수행하고자 하는 작업 또는 작동입니다. AWS CLI 또는 AWS API를 사용하여 AWS Management 콘솔 또는 작동의 작업을 수행할 수 있습니다.
- 리소스 – 수행된 작업 또는 작동에 따른 AWS 리소스 객체입니다.
- 보안 주체 – 엔터티(사용자 또는 역할)를 사용하여 요청을 보내는 사람 또는 애플리케이션입니다. 보안 주체에 대한 정보에는 보안 주체가 로그인하는 데 사용된 엔터티와 관련된 정책이 포함됩니다.
- 환경 데이터 – IP 주소, 사용자 에이전트, SSL 사용 상태 또는 시간대와 같은 정보입니다.
- 리소스 데이터 – 요청되는 리소스와 관련된 데이터. 여기에는 DynamoDB 테이블 이름 또는 Amazon EC2 인스턴스 태그와 같은 정보가 포함될 수 있습니다.

AWS에서 요청을 평가하고 승인하는 데 사용되는 요청 콘텍스트로 이 요청 정보를 수집합니다.

인증

보안 주체는 AWS에게 요청을 보내려면 자격 증명을 사용하여 인증을 받아야 합니다(AWS에 로그인). Amazon S3 및 AWS STS 등과 같은 일부 서비스는 익명 사용자의 몇 가지 요청을 허용합니다. 하지만 이는 규칙 예외입니다.

루트 사용자로서 콘솔에서 인증하려면 이메일 주소 및 암호로 로그인해야 합니다. IAM 사용자로서 계정 ID 또는 별칭을 입력한 다음 사용자 이름과 암호를 입력합니다. API 또는 AWS CLI에서 인증하려면 액세스 키 및 보안 키를 제공해야 합니다. 추가 보안 정보도 제공해야 할 수 있습니다. 예를 들어, AWS는 멀티 팩터 인증(MFA)을 사용하여 계정의 보안을 강화하는 것을 권장합니다. AWS가 인증할 수 있는 IAM 엔터티에 대한 자세한 정보는 IAM 사용자 (p. 85) 및 IAM역할 (p. 174) 단원을 참조하십시오.

권한 부여

또한 요청을 완료할 수 있는 권한이 있어야 합니다. AWS는 권한 부여 동안 요청 콘텍스트의 값을 사용하여 요청을 허용할지 거부할지 여부에 적용되는 정책을 점검합니다. 그런 다음 이것은 정책을 사용하여 요청을 허용하거나 거부할지 여부를 결정합니다. 대부분의 정책은 AWS에 JSON 문서 (p. 354)로 저장되며 보안 주체 엔터티에 대한 권한을 지정합니다. 요청이 권한 부여될지 여부에 영향을 미치는 정책의 몇 가지 유형 (p. 349)이 있습니다. 계정에서 AWS 리소스로의 액세스 권한을 사용자에게 제공하려면 자격 기반 정책만 필요합니다. 리소스 기반 정책은 교차 계정 액세스 (p. 509)를 허용하는 데 좋습니다. 다른 정책 유형은 고급 기능이며 조심스럽게 사용해야 합니다.

AWS은 요청 컨텍스트에 적용되는 각 정책을 확인합니다. 단일 권한 정책에 거부된 작업이 포함된 경우 AWS는 전체 요청을 거부하고 평가를 중지합니다. 이를 명시적 거부라고 합니다. 요청은 기본적으로 거부되므로 AWS는 적용 가능한 권한 정책이 요청의 모든 부분을 허용하는 경우에만 요청에 권한을 부여합니다. 단일 계정 내 요청 평가 로직은 다음 일반 규칙을 따릅니다.

- 기본적으로 모든 요청을 거부합니다. (일반적으로, AWS 계정 루트 사용자 증명을 사용하여 해당 계정의 리소스를 요청하는 경우는 항상 허용됩니다.)
- 권한 정책(자격 증명 기반 또는 리소스 기반)에 포함된 명시적 허용은 이 기본 작동을 재정의합니다.

- 조직 SCP, IAM 권한 경계 또는 세션 정책이 있는 경우 허용이 재정의됩니다. 하나 이상의 이러한 정책 유형이 존재하는 경우 이들 정책 유형 모두가 해당 요청을 허용해야 합니다. 그렇지 않은 경우 이 값은 묵시적으로 거부됩니다.
- 어떠한 정책의 명시적 거부도 허용을 무시합니다.

모든 유형의 정책 평가 방법에 대한 자세한 내용은 정책 평가 로직 (p. 622) 단원을 참조하십시오. 사용자가 다른 계정에서 요청해야 하는 경우 다른 계정의 정책에서 해당 사용자가 해당 리소스를 액세스하도록 허용해야 하며, 또한 요청하는 데 사용하는 IAM 엔터티에도 해당 요청을 허용하는 자격 증명 기반 정책이 있어야 합니다.

작업 또는 연산

요청이 인증 및 권한 부여된 후 AWS가 요청의 작업 또는 작동을 승인합니다. 작업은 서비스로 정의되며 리소스 보기, 생성, 편집 및 삭제와 같이 리소스에 대해 수행할 수 있는 사항입니다. 예를 들어, IAM은 사용자 리소스에 대해 다음 작업을 비롯하여 약 40개의 작업을 수행할 수 있도록 지원합니다.

- `CreateUser`
- `DeleteUser`
- `GetUser`
- `UpdateUser`

보안 주체가 작업을 수행할 수 있도록 허용하려면 보안 주체 또는 영향을 받은 리소스에 적용되는 필요한 작업을 정책에 포함해야 합니다. 각 서비스가 지원하는 작업, 리소스 유형, 조건 키 목록은 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

리소스

AWS가 요청의 작업을 승인하면 계정 내의 관련 리소스에서 해당 작업을 수행할 수 있습니다. 리소스는 서비스 내에 존재하는 객체입니다. 예를 들어 Amazon EC2 인스턴스, IAM 사용자 및 Amazon S3 버킷이 있습니다. 서비스는 각 리소스에서 수행할 수 있는 일련의 작업을 정의합니다. 리소스에서 관련되지 않은 작업을 수행하도록 요청을 생성하면 해당 요청이 거부됩니다. 예를 들어 IAM 역할을 삭제하도록 요청하지만 IAM 그룹 리소스를 제공하지 않는 경우 요청이 실패합니다. 작업에 의해 영향을 받는 리소스를 식별하는 AWS 서비스 테이블을 보려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

자격 증명 관리 개요: 사용자

보안 및 조직을 강화하기 위해 사용자 지정 권한으로 생성한 특정 사용자 자격 증명에 AWS 계정에 대한 액세스 권한을 부여할 수 있습니다. 기존 자격 증명을 AWS에 연동하여 그러한 사용자를 위해 액세스를 더욱 간소화할 수 있습니다.

주제

첫 액세스에만 해당: 루트 사용자 자격 증명

AWS 계정을 생성할 때 AWS로 로그인하는 데 사용하는 AWS 계정 루트 사용자 자격 증명을 생성합니다. 이 루트 사용자 자격 증명, 즉 계정을 생성할 때 입력한 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 로그인할 수 있습니다. 이러한 이메일 주소 및 암호의 조합을 루트 사용자 자격 증명이라고도 합니다.

루트 사용자 자격 증명을 사용하면 AWS 계정의 모든 리소스에 완전히 무제한으로 액세스할 수 있습니다. 여기에는 결제 정보에 대한 액세스 및 암호 변경 권한이 포함됩니다. 이러한 수준의 액세스는 계정을 처음 설정했을 때 필요합니다. 그러나 일상적인 액세스에는 루트 사용자 자격 증명을 사용하지 않는 것이 좋습니다. 특히 루트 사용자 자격 증명을 타인과 공유하면 타인이 내 계정에 무제한으로 액세스할 수 있으므로 공유하지 않는 것이 좋습니다. 루트 사용자에 부여된 권한을 제한할 수는 없습니다.

다음 단원에서는 본인 및 AWS 리소스를 사용하는 사람들에게 AWS 리소스에 대한 안전하고 제한된 액세스를 제공하기 위해 IAM을 사용하여 사용자 자격 증명 및 권한을 생성하고 관리하는 방법을 설명합니다.

IAM 사용자

AWS Identity and Access Management(IAM)의 '자격 증명'을 통해 '사용자의 정체'를 확인할 수 있습니다. 이를 흔히 인증이라고 합니다. 루트 사용자 자격 증명을 타인과 공유하는 대신, 조직의 사용자에 해당되는 계정 내에 개별 IAM 사용자를 생성할 수 있습니다. IAM 사용자는 별개의 계정이 아니라 해당 계정 내의 사용자입니다. 각 사용자는 고유의 AWS Management 콘솔 액세스 암호를 가질 수 있습니다. 또한 사용자가 계정의 리소스를 사용하기 위한 프로그래밍 방식의 요청을 할 수 있도록 각 사용자에 대한 개별 액세스 키를 생성할 수 있습니다. 다음 그림에서는 AWS 계정 하나에 Li, Mateo, DevApp1, DevApp2, TestApp1 및 TestApp2라는 사용자가 추가되었습니다. 각 사용자는 고유의 자격 증명을 가집니다.


Account
Li
Mateo
DevApp1
DevApp2

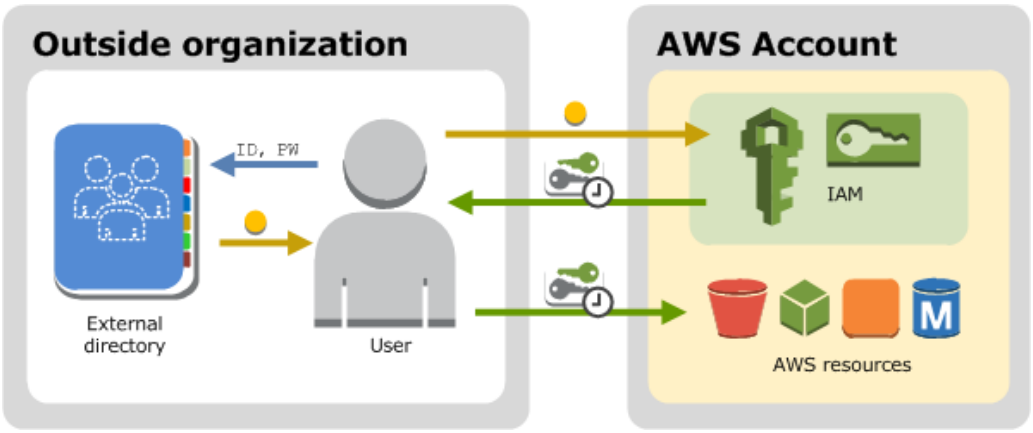
일부 사용자는 사실 애플리케이션입니다(예: DevApp1). IAM 사용자가 실제 사람일 필요는 없습니다. 회사 네트워크에서 실행하며 AWS 액세스를 필요로 하는 애플리케이션에 대한 액세스 키를 생성하기 위해 IAM 사용자를 생성할 수 있습니다.

본인을 위한 IAM 사용자를 생성한 다음, 본인에게 계정에 대한 관리 권한을 할당하는 것이 좋습니다. 그런 다음 해당 사용자로 로그인하여 필요에 따라 사용자를 추가할 수 있습니다.

기존 사용자 연동

조직 내 사용자에게 이미 인증 방법이 있는 경우(예: 회사 네트워크에 로그인) 해당 사용자를 위해 별도의 IAM 사용자를 생성할 필요가 없습니다. 대신 이러한 사용자 자격 증명을 AWS에 연동할 수 있습니다.

다음 다이어그램은 사용자가 IAM을 사용하여 AWS 계정의 리소스에 액세스하기 위한 임시 AWS 보안 자격 증명을 얻는 방법을 보여 줍니다.



연동은 다음과 같은 경우에 특히 유용합니다.

- 사용자가 이미 기업 디렉토리에 자격 증명을 보유한 경우

  기업 디렉토리가 SAML 2.0(Security Assertion Markup Language 2.0)과 호환되는 경우, 기업 디렉토리를 구성하여 사용자에게 AWS Management 콘솔에 대한 Single-Sign On(SSO) 액세스를 제공할 수 있습니다. 자세한 내용은 임시 자격 증명과 관련된 일반적인 시나리오 (p. 302) 단원을 참조하십시오.

  기업 디렉토리가 SAML 2.0과 호환되지 않는 경우, 자격 증명 브로커 애플리케이션을 생성하여 사용자에게 AWS Management 콘솔에 대한 Single-Sign On(SSO) 액세스를 제공할 수 있습니다. 자세한 내용은 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.

  기업 디렉토리가 Microsoft Active Directory인 경우, AWS Directory Service를 사용하여 기업 디렉토리와 AWS 계정 간의 신뢰를 설정할 수 있습니다.
- 사용자가 이미 인터넷 자격 증명을 보유한 경우

  사용자가 Login with Amazon, Facebook, Google 또는 OpenID Connect(OIDC) 호환 자격 증명 공급자 등의 인터넷 자격 증명 공급자를 통해 자신을 식별할 수 있도록 모바일 앱 또는 웹 기반 앱을 만들면, 해당 앱에서 연동을 통해 AWS에 액세스할 수 있습니다. 자세한 내용은 웹 자격 증명 연동에 대하여 (p. 183) 단원을 참조하십시오.

  도움말

  인터넷 자격 증명 공급자를 통해 자격 증명 연동을 사용하려면 Amazon Cognito를 사용하는 것이 좋습니다.

액세스 관리 개요: 권한 및 정책

AWS Identity and Access Management(IAM)의 액세스 관리를 통해 계정에서 보안 주체 엔터티에 허용된 권한을 정의할 수 있습니다. 보안 주체 엔터티란 IAM 엔터티(사용자 또는 역할)을 사용하여 인증된 사람 또는 애플리케이션입니다. 액세스 관리를 흔히 권한 부여라고 합니다. 정책을 생성하고 IAM 자격 증명(사용자, 사용자 그룹 또는 역할) 또는 AWS 리소스에 연결하여 AWS에서 액세스를 관리합니다. 정책은 자격 증명이나 리소스와 연결될 때 해당 권한을 정의하는 AWS의 객체입니다. AWS는 IAM 엔터티(사용자 또는 역할)가 요청을 보낼 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지 여부를 결정합니다. 대부분의 정책은 AWS에 JSON 문서로서 저장됩니다. 정책 유형 및 활용에 대한 자세한 정보는 정책 및 권한 (p. 349) 단원을 참조하십시오.

정책 및 계정

AWS에서 하나의 계정을 관리하려면 정책을 사용하여 해당 계정 내 권한을 정의합니다. 여러 계정 전반의 권한을 관리하고자 한다면 사용자에 대한 권한을 관리하기가 더 어렵습니다. 교차 계정 권한에 대해 IAM 역할, 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 사용할 수 있습니다. 하지만 여러 계정을 소유하는 경우에는 이러한 권한을 쉽게 관리할 수 있도록 ACL 대신에 AWS Organizations 서비스를 사용하는 것이 좋습니다. 자세한 정보는 조직 사용 설명서의 AWS Organizations(이)란 무엇입니까? 단원을 참조하십시오.

정책 및 사용자

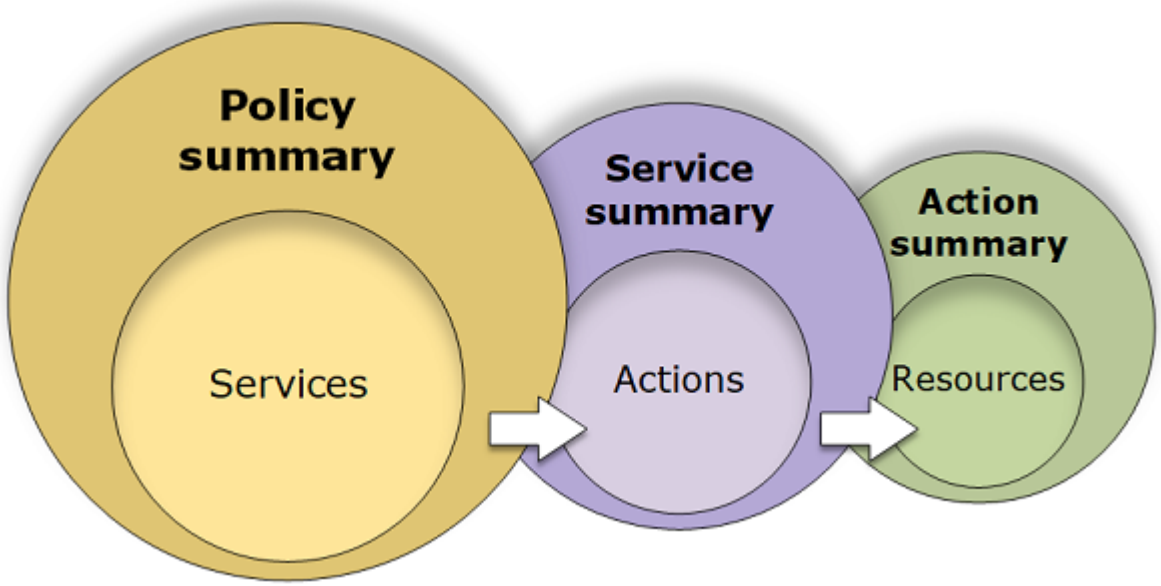
IAM 사용자는 서비스의 자격 증명입니다. IAM 사용자를 생성할 경우, 권한을 부여하지 않는 한 사용자는 계정 내에서 어떠한 것으로도 액세스할 수 없습니다. 사용자 또는 사용자가 속한 그룹에 연결된 정책인 자격 증명 기반 정책을 생성하여 사용자에게 권한을 부여합니다. 다음 예는 사용자가 `us-east-2` 리전 내의 `123456789012` 계정에서 `Books` 테이블의 모든 Amazon DynamoDB 작업(`dynamodb:*`)을 수행할 수 있도록 허용하는 JSON 정책을 보여 줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-2:123456789012:table/Books"
  }
}
```

이 정책을 IAM 사용자에게 연결한 후에는 해당 사용자가 이러한 DynamoDB 권한만 부여받습니다. 대부분의 사용자는 해당 사용자의 권한을 함께 나타내는 여러 정책을 부여받습니다.

명시적으로 허용되지 않은 작업 또는 리소스는 기본적으로 모두 거부됩니다. 예를 들어 앞서 다룬 정책이 사용자에게 연결된 유일한 정책이라면 이 사용자는 `Books` 테이블에 대한 DynamoDB 작업만 수행할 수 있습니다. 다른 모든 테이블에 대한 작업은 금지됩니다. 마찬가지로 사용자는 Amazon EC2, Amazon S3 또는 기타 다른 AWS 서비스의 어떠한 작업도 수행할 수 없습니다. 그 이유는 권한 정책이 함께 작업할 이러한 서비스는 정책에 포함되지 않기 때문입니다.

IAM 콘솔에는 정책에서 각 서비스에 대해 허용되거나 거부되는 액세스 레벨, 리소스, 조건을 설명하는 정책 요약 테이블이 포함되어 있습니다. 정책은 3가지 테이블, 즉 정책 요약 (p. 484), 서비스 요약 (p. 493), 작업 요약 (p. 497)으로 요약됩니다. 정책 요약 테이블에는 서비스 목록이 포함되어 있습니다. 서비스 요약을 보려면 여기서 서비스를 선택합니다. 이 요약 테이블에는 작업 목록과 선택한 서비스에 대해 연결된 권한이 포함되어 있습니다. 해당 테이블에서 작업을 선택하여 작업 요약을 볼 수 있습니다. 이 테이블에는 리소스 목록과 선택한 작업에 대한 조건이 포함되어 있습니다.



사용자 페이지에서 해당 사용자에게 연결된 모든 정책(관리형 및 인라인)에 대한 정책 요약을 볼 수 있습니다. 정책 페이지에서 모든 관리형 정책에 대한 요약을 봅니다.

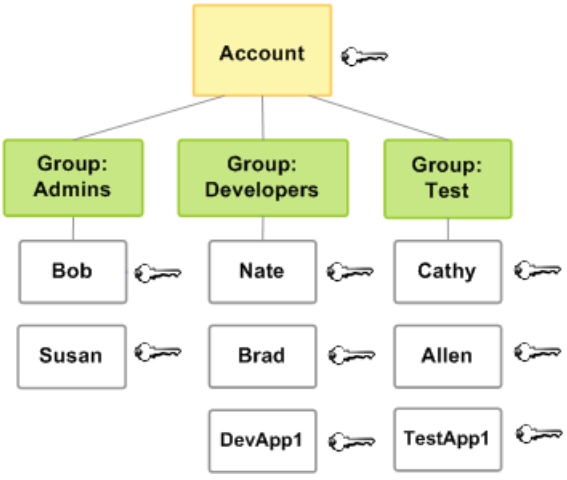
예를 들어 위 정책은 AWS Management 콘솔에 다음과 같이 요약됩니다.

Service	Access level	Resource	Request condition
Allow (1 of 102 services) Show remaining 101			
DynamoDB	Full access	TableName = Books	None

정책의 JSON 문서도 볼 수 있습니다. 요약 또는 JSON 문서를 보는 방법에 대한 자세한 정보는 정책에 의해 부여된 권한 이해 (p. 483) 단원을 참조하십시오.

정책 및 그룹

IAM 사용자를 IAM 그룹으로 구성하고 그룹에 정책을 연결할 수 있습니다. 이 경우 각 사용자는 별도의 자격 증명을 갖고 있지만 그룹에 연결된 정책에 명시된 권한이 그룹 내 모든 사용자에게 부여됩니다. 그룹을 사용하여 간편하게 권한을 관리하고 IAM 모범 사례 (p. 60)에 따를 수 있습니다.



사용자 또는 그룹에 여러 정책을 연결하여 다양한 권한을 부여할 수 있습니다. 이 경우 사용자의 권한은 각 정책의 조합으로 계산됩니다. 그러나 개별 작업 및 리소스에 대한 권한을 명시적으로 부여해야 사용자가 해당 권한을 가지게 되는 기본 원칙은 여전히 적용됩니다.

연동 사용자 및 역할

연동 사용자에게는 IAM 사용자처럼 AWS 계정에서 영구적인 ID가 부여되지 않습니다. 연동 사용자에게 권한을 부여하려면 역할이라고 하는 개체를 만들어 해당 역할의 권한을 정의할 수 있습니다. 연동 사용자가 AWS에 로그인하면 사용자가 역할과 연결되고 역할에 정의된 권한이 부여됩니다. 자세한 정보는 타사 자격 증명 공급자의 역할 만들기(연동) (p. 238) 단원을 참조하십시오.

자격 증명 기반 정책 및 리소스 기반 정책

자격 증명 기반 정책은 IAM 사용자, 그룹 또는 역할과 같은 IAM 자격 증명에 연결할 수 있는 권한 정책입니다. 리소스 기반 정책은 Amazon S3 버킷 또는 IAM 역할 신뢰 정책과 같은 리소스에 연결하는 권한 정책입니다.

자격 증명 기반 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. 자격 증명 기반 정책을 추가로 분류할 수 있습니다.

- 관리형 정책 – AWS 계정에 속한 다수의 사용자, 그룹 및 역할에게 독립적으로 연결할 수 있는 자격 증명 기반 정책입니다. 사용할 수 있는 관리형 정책은 두 가지가 있습니다.
  - AWS 관리형 정책 – AWS에서 생성 및 관리하는 관리형 정책입니다. 정책 사용이 처음이라면 AWS 관리형 정책 사용을 먼저 권장합니다.
  - 고객 관리형 정책 – 사용자가 자신의 AWS 계정에서 생성 및 관리하는 관리형 정책입니다. 고객 관리형 정책은 AWS 관리형 정책보다 정책에 대해 더욱 정밀하게 제어할 수 있습니다. 시각적 편집기에서 또는 JSON 정책 문서를 직접 생성하여 IAM 정책을 생성 및 편집할 수 있습니다. 자세한 정보는 IAM 정책 만들기 (p. 435) 및 IAM 정책 편집 (p. 460)을(를) 참조하십시오.
- 인라인 정책 – 자신이 생성 및 관리하며, 단일 사용자, 그룹 또는 역할에 직접 포함되는 정책입니다. 대부분의 경우 인라인 정책을 사용하지 않는 것이 좋습니다.

리소스 기반 정책은 지정된 보안 주체가 해당 리소스에 대해 수행할 수 있는 작업 및 이에 관한 조건을 제어합니다. 리소스 기반 정책은 인라인 정책이며, 관리형 리소스 기반 정책은 없습니다. 교차 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다.

IAM 서비스는 역할 신뢰 정책이라고 하는 리소스 기반 정책 유형 하나만 지원하며, 이 유형은 IAM 역할에 연결됩니다. IAM 역할은 리소스 기반 정책을 지원하는 자격 증명이자 리소스이므로 신뢰 정책과 자격 증명 기반 정책 모두 IAM 역할에 연결해야 합니다. 신뢰 정책은 역할을 수임할 수 있는 보안 주체 엔터티(계정, 사용자, 역할 및 연합된 사용자)를 정의합니다. IAM 역할과 다른 리소스 기반 정책 간의 차이에 대해 알아보려면 IAM 역할과 리소스 기반 정책의 차이 (p. 287) 단원을 참조하십시오.

리소스 기반 정책을 지원하는 서비스를 보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 리소스 기반 정책에 대해 자세히 알아보려면 자격 증명 기반 정책 및 리소스 기반 정책 (p. 372) 단원을 참조하십시오.

AWS용 ABAC란 무엇입니까?

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. 태그는 IAM 보안 주체(사용자 또는 역할)와 AWS 리소스에 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 작은 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계될 수 있습니다. ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

예를 들어, access-project 태그 키를 사용하여 세 개의 역할을 생성할 수 있습니다. 첫 번째 역할의 태그 값을 Heart로, 두 번째 역할의 태그 값을 Sun으로, 세 번째 역할의 태그 값을 Lightning으로 설정합니다. 그런 다음 역할과 리소스에 access-project에 대해 동일한 값으로 태그를 지정할 때 액세스를 허용하는 단일 정책을 사용할 수 있습니다. AWS에서 ABAC를 사용하는 방법을 보여 주는 자세한 자습서는 자습서: AWS에서 속성 기반 액세스 제어에 태그 사용 (p. 41) 단원을 참조하십시오.

ABAC와 기존 RBAC 모델 비교

IAM에 사용되는 기존 권한 부여 모델을 RBAC(역할 기반 액세스 제어)라고 합니다. RBAC는 AWS 외부에서 역할로 알려진 개인의 직무에 따라 권한을 정의합니다. AWS 내에서 역할은 일반적으로 IAM 역할을 말하며, 사용자가 맡을 수 있는 IAM의 자격 증명입니다. IAM에는 RBAC 모델의 직무에 대한 권한을 조정하는 직무에 대한 관리형 정책 (p. 642)이 포함되어 있습니다.

IAM에서는 다양한 직무에 대해 서로 다른 정책을 생성하여 RBAC를 구현합니다. 그런 다음 정책을 자격 증명(IAM 사용자, 사용자 그룹 또는 IAM 역할)에 연결합니다. 가장 좋은 방법은 직무에 필요한 최소 권한을 부여하는 것입니다. 이를 최소 권한 부여 (p. 61)라고 합니다. 직무가 액세스할 수 있는 특정 리소스를 나열하여 이 작업을 수행합니다. 기존 RBAC 모델을 사용하면 직원이 새 리소스를 추가할 때 해당 리소스에 액세스할 수 있도록 정책을 업데이트해야 한다는 단점이 있습니다.

예를 들어, 직원이 작업 중인 세 개의 프로젝트 Heart, Sun 및 Lightning이 있다고 가정합니다. 각 프로젝트에 대한 IAM 역할을 생성합니다. 그런 다음 각 IAM 역할에 정책을 연결하여 역할을 맡을 수 있는 모든 사람이 액세스할 수 있는 리소스를 정의합니다. 직원이 회사 내에서 직무를 변경하는 경우 다른 IAM 역할에 해당 직무를 할당합니다. 사람이나 프로그램은 둘 이상의 역할에 할당될 수 있습니다. 그러나 Sun 프로젝트에 새 Amazon S3 버킷과 같은 추가 리소스가 필요할 수 있습니다. 이 경우 Sun 역할에 연결된 정책을 업데이트하여 새 버킷 리소스를 지정해야 합니다. 그렇지 않으면 Sun 프로젝트 멤버가 새 버킷에 액세스할 수 없습니다.

ABAC는 전통적인 RBAC 모델에 비해 다음과 같은 이점을 제공합니다.

- ABAC 권한은 혁신적으로 확장됩니다. 관리자가 새 리소스에 액세스할 수 있도록 기존 정책을 업데이트할 필요가 없습니다. 예를 들어, access-project 태그로 ABAC 전략을 설계했다고 가정합니다. 개발자는 access-project = Heart 태그와 함께 역할을 사용합니다. Heart 프로젝트의 사람에게 추가 Amazon EC2 리소스가 필요한 경우 개발자는 access-project = Heart 태그를 사용하여 새 Amazon EC2 인스턴스를 생성할 수 있습니다. 그러면 Heart 프로젝트의 모든 사용자가 태그 값이 일치하기 때문에 해당 인스턴스를 시작하고 중지할 수 있습니다.
- ABAC를 사용하면 필요한 정책 수가 적어집니다. 각 직무에 대해 서로 다른 정책을 생성할 필요가 없기 때문에 생성해야 하는 정책이 더 적습니다. 그러므로 정책을 관리하기가 더 쉽습니다.
- ABAC를 사용하여 팀은 빠르게 변화하고 성장할 수 있습니다. 새 리소스에 대한 권한이 속성에 따라 자동으로 부여되기 때문입니다. 예를 들어, 회사에서 이미 ABAC를 사용하여 Heart 및 Sun 프로젝트를 지원하는 경우 새 Lightning 프로젝트를 쉽게 추가할 수 있습니다. IAM 관리자는 access-project = Lightning 태그를 사용하여 새 역할을 생성합니다. 새 프로젝트를 지원하기 위해 정책을 변경할 필요는 없습니다. 역할을 맡을 권한이 있는 모든 사용자는 access-project = Lightning 태그가 지정된 인스턴스를 생성하고 볼 수 있습니다. 또한 팀 멤버가 Heart 프로젝트에서 Lightning 프로젝트로 이동할 수 있습니다. IAM 관리자는 사용자를 다른 IAM 역할에 할당합니다. 권한 정책을 변경할 필요가 없습니다.
- ABAC를 사용하여 세분화된 권한을 사용할 수 있습니다. 정책을 생성할 때는 최소 권한을 부여 (p. 61)하는 것이 가장 좋습니다. 기존 RBAC를 사용하는 경우에는 특정 리소스에 대한 액세스만 허용하는 정책을 작성해야 합니다. 그러나 ABAC를 사용하는 경우 리소스 태그가 보안 주체의 태그와 일치하는 경우에만 모든 리소스에 대한 작업을 허용할 수 있습니다.
- ABAC를 사용하여 회사 디렉터리의 직원 속성을 사용합니다. 세션 태그를 AWS에 전달하도록 SAML 기반 또는 웹 자격 증명 공급자를 구성할 수 있습니다. 직원이 AWS에 연동되면 해당 속성이 AWS의 결과 보안 주체에 적용됩니다. 그런 다음 ABAC를 사용하여 이러한 속성에 따라 권한을 허용하거나 거부할 수 있습니다.

AWS에서 ABAC를 사용하는 방법을 보여 주는 자세한 자습서는 자습서: AWS에서 속성 기반 액세스 제어에 태그 사용 (p. 41) 단원을 참조하십시오.

IAM 외부의 보안 기능

IAM을 사용하여 AWS Management 콘솔 작업, AWS 명령줄 도구 작업 또는 AWS SDK를 통한 서비스 API 작업에 대한 액세스를 제어할 수 있습니다. 일부 AWS 제품은 리소스 보안을 위한 다른 방법도 지원합니다. 다음 목록은 전체는 아니지만 몇 가지 예에 해당합니다.

Amazon EC2

Amazon Elastic Compute Cloud에서는 키 페어를 사용하거나(Linux 인스턴스의 경우) 사용자 이름 및 암호를 사용해(Microsoft Windows 인스턴스의 경우) 인스턴스에 로그인합니다.

자세한 내용은 다음 문서를 참조하십시오.

- Linux 인스턴스용 Amazon EC2 사용 설명서의 Amazon EC2 Linux 인스턴스 시작하기
- Windows 인스턴스용 Amazon EC2 사용 설명서의 Amazon EC2 Windows 인스턴스 시작하기

Amazon RDS

Amazon Relational Database Service에서는 데이터베이스와 연결되어 있는 사용자 이름 및 암호를 사용해 데이터베이스 엔진에 로그인합니다.

자세한 내용은 Amazon RDS 사용 설명서의 Amazon RDS 시작하기를 참조하십시오.

Amazon EC2 및 Amazon RDS

Amazon EC2 및 Amazon RDS에서는 보안 그룹을 사용하여 인스턴스 또는 데이터베이스에 대한 트래픽을 제어합니다.

자세한 내용은 다음 문서를 참조하십시오.

- Linux 인스턴스용 Amazon EC2 사용 설명서의 Linux 인스턴스에 대한 Amazon EC2 보안 그룹
- Windows 인스턴스용 Amazon EC2 사용 설명서의 Windows 인스턴스에 대한 Amazon EC2 보안 그룹
- Amazon RDS 사용 설명서의 보안 그룹 Amazon RDS.

Amazon WorkSpaces

Amazon WorkSpaces에서는 사용자 이름과 암호를 사용해 데스크톱에 로그인합니다.

자세한 내용은 Amazon WorkSpaces Administration Guide의 Amazon WorkSpaces 시작하기를 참조하십시오.

Amazon WorkDocs

Amazon WorkDocs에서는 사용자 이름과 암호를 사용해 로그인하여 공유 문서에 액세스합니다.

자세한 내용은 Amazon WorkDocs 관리 안내서의 Amazon WorkDocs 시작하기를 참조하십시오.

위와 같은 액세스 제어 방법들은 IAM과 다릅니다. IAM에서는 Amazon EC2 인스턴스를 생성 또는 종료하거나 새로운 Amazon WorkSpaces 데스크톱을 설정하는 등 AWS 제품의 관리 방식을 제어할 수 있습니다. 다시 말해서, IAM은 Amazon Web Services 요청을 통한 작업을 제어하는 데 효과적일 뿐만 아니라 AWS Management 콘솔에 대한 액세스를 제어하는 데도 이상적입니다. 단, IAM은 운영 체제(Amazon EC2), 데이터베이스(Amazon RDS), 데스크톱(Amazon WorkSpaces) 또는 협업 사이트(Amazon WorkDocs)에 로그인하는 등의 작업에 대해서는 보안 관리를 지원하지 않습니다.

특정 AWS 제품을 이용해 작업할 때는 반드시 설명서를 읽고 해당 제품에 속한 모든 리소스의 보안 옵션을 살펴보시기 바랍니다.

공통 작업의 빠른 링크

다음은 IAM과 연결되어 있는 공통 작업에 대한 도움말을 살펴볼 수 있는 링크입니다.

IAM 사용자로 로그인

IAM 사용자가 AWS에 로그인하는 방법 (p. 91) 단원을 참조하십시오.

IAM 사용자 암호 관리

결제 정보에 대한 액세스를 포함하여 AWS Management 콘솔에 액세스하려면 암호가 필요합니다.

AWS 계정 루트 사용자에 대한 내용은 AWS 계정 루트 사용자 암호 변경 (p. 100) 단원을 참조하십시오.

IAM 사용자에 대한 내용은 IAM 사용자의 암호 관리 (p. 104) 단원을 참조하십시오.

IAM 사용자 권한 관리

AWS 계정에 속한 IAM 사용자들에게 권한을 부여할 때는 정책을 사용합니다. 생성 시점에서는 IAM 사용자들에게 AWS 리소스를 사용할 수 있는 권한이 없기 때문에 권한을 추가해야 합니다.

자세한 내용은 IAM 정책 관리 (p. 435) 단원을 참조하십시오.

AWS 계정에 속한 사용자 표시 및 자격 증명 정보 가져오기

AWS 계정의 자격 증명 보고서 가져오기 (p. 156) 단원을 참조하십시오.

멀티 팩터 인증(MFA) 추가

가상 MFA 디바이스를 추가하려면 다음 중 하나 단원을 참조하십시오.

- AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) (p. 123)
- IAM 사용자에 대한 가상 MFA 디바이스 활성화(콘솔) (p. 122)

U2F 보안 키를 추가하려면 다음 중 하나 단원을 참조하십시오.

- AWS 계정 루트 사용자에 대한 U2F 보안 키 활성화(콘솔) (p. 128)
- 다른 IAM 사용자에 대한 U2F 보안 키 활성화(콘솔) (p. 127)

하드웨어 MFA 디바이스를 추가하려면 다음 중 하나 단원을 참조하십시오.

- AWS 계정 루트 사용자용 하드웨어 MFA 디바이스 활성화(콘솔) (p. 133)
- 다른 IAM 사용자에 대해 하드웨어 MFA 디바이스 활성(콘솔) (p. 132)

액세스 키 가져오기

AWS SDK, AWS 명령줄 도구 또는 API 작업을 사용하여 AWS 요청을 하려면 액세스 키가 필요합니다.

> **Important**
>
> 보안 액세스 키는 액세스 키를 생성하는 시점에만 보고 다운로드할 수 있습니다. 이후로는 보안 액세스 키를 보거나 복구할 수 없습니다. 하지만 보안 액세스 키를 분실한 경우에는 새로운 액세스 키를 생성할 수 있습니다.

AWS 계정의 경우 AWS 계정을 위한 액세스 키 관리 단원을 참조하십시오.

IAM 사용자에 대한 내용은 IAM 사용자의 액세스 키 관리 (p. 111) 단원을 참조하십시오.

사용자 또는 역할 태그 지정

AWS SDK 중 하나를 통해 IAM 콘솔, AWS CLI 또는 API를 사용하여 IAM 사용자 또는 역할에 태그를 지정할 수 있습니다.

IAM 태그 지정에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.

IAM에서의 태그 관리 방법에 대한 자세한 내용은 IAM 엔터티에 대한 태그 관리(콘솔) (p. 293) 단원을 참조하십시오.

IAM 태그를 사용하여 AWS에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 IAM 리소스 태그를 사용하여 IAM 사용자 및 역할에 대한 액세스 제어 (p. 382) 단원을 참조하십시오.

AWS 시작하기

이 설명서에서는 IAM 서비스에 대해 주로 다룹니다. AWS를 시작하는 방법과 여러 서비스를 사용하여 프로젝트 구축 및 개시 등과 같은 문제를 해결하는 방법을 알아보려면 리소스 센터 시작하기 단원을 참조하십시오.

설정

AWS Identity and Access Management(IAM)는 Amazon Web Services(AWS) 및 사용자 계정 리소스에 대한 액세스를 안전하게 제어합니다. IAM은 또한 계정 자격 증명을 비밀로 유지합니다. 그 밖에 IAM은 AWS 계정에 다수의 IAM 사용자를 생성하거나, 기업 디렉터리와 자격 증명을 연동하여 임시 액세스를 허용할 수도 있습니다. 여러 AWS 계정의 리소스에 액세스할 수 있는 경우도 있습니다.

하지만 IAM을 사용하지 않을 경우에는 다수의 AWS 계정을 생성하거나(각 계정마다 AWS 제품 결제 및 구독을 따로 해야 합니다), 혹은 직원들이 단일 AWS 계정의 보안 자격 증명을 공유해야 합니다. 그 뿐만 아니라 IAM이 없으면 특정 사용자 또는 시스템의 작업이나 사용하는 AWS 리소스를 제어할 수 없습니다.

이번 안내서에서는 IAM의 개념에 대해 간략히 살펴보고, 비즈니스 사용 사례를 비롯한 AWS 권한 및 정책에 대해 설명하겠습니다.

주제

IAM을 사용하여 AWS 리소스에 대한 사용자 액세스를 허용하는 방법

IAM을 사용하여 AWS 리소스에 대한 액세스를 제어할 수 있는 몇 가지 방법이 있습니다.

액세스 유형	왜 사용해야 합니까?	자세한 정보는 어디에서 얻을 수 있습니까?
AWS 계정 내 사용자에 대한 액세스	AWS 계정에 사용자를 추가하고 싶거나, IAM을 사용하여 사용자를 생성한 후 그 권한을 관리하려고 합니다.	AWS Management 콘솔을 사용하여 사용자를 생성한 후 AWS 계정에서 사용자 권한을 관리하는 방법에 대한 자세한 내용은 시작 (p. 19) 단원을 참조하십시오. IAM API 또는 AWS Command Line Interface를 사용하여 AWS 계정에 사용자를 생성하는 방법에 대한 자세한 내용은 첫 번째 IAM 관리자 및 그룹 생성 (p. 20) 단원을 참조하십시오. IAM 사용자 작업에 대한 자세한 내용은 자격 증명(사용자, 그룹, 및 역할) (p. 83) 단원을 참조하십시오.
권한 부여 시스템과 AWS 사이의 자격 증명 연동을 통한 AWS 사용자가 아닌 사용자의 액세스	자격 증명 및 권한 부여 시스템에 AWS 사용자가 아닌 사용자가 있으며, 이 사용자들이 AWS 리소스에 액세스해야 합니다.	보안 토큰을 사용하여 회사 디렉터리와 자격 증명을 연동함으로써 AWS 계정 리소스에 대한 사용자 액세스를 허용하는 방법에 대한 자세한 내용은 임시 보안 자격 증명 (p. 302)을 참조하십시오. AWS Security Token Service API에 대한 자세한 내용은 AWS Security Token Service API Reference를 참조하십시오.
AWS 계정 간 교차 계정 액세스	일부 AWS 리소스에 대한 액세스를 AWS 계정에 속한 사용자와 공유하려고 합니다.	IAM을 사용해 다른 AWS 계정에게 권한을 부여하는 방법에 대한 자세한 내용은 역할 용어 및 개념 (p. 175) 단원을 참조하십시오.

IAM을 사용하려면 가입해야 합니까?

아직 AWS 계정이 없다면 IAM을 사용할 계정을 하나 생성해야 합니다. 하지만 IAM을 사용하려고 따로 가입할 필요는 없습니다. IAM 사용은 무료입니다.

> **Note**
>
> IAM은 IAM과 통합된 AWS 제품에서만 사용할 수 있습니다. IAM 지원 서비스 목록은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

AWS에 가입하려면

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

   등록 절차 중 전화를 받고 전화 키패드를 사용하여 확인 코드를 입력하는 과정이 있습니다.

추가 리소스

아래는 IAM 사용에 도움이 될 수 있는 몇 가지 리소스들입니다.

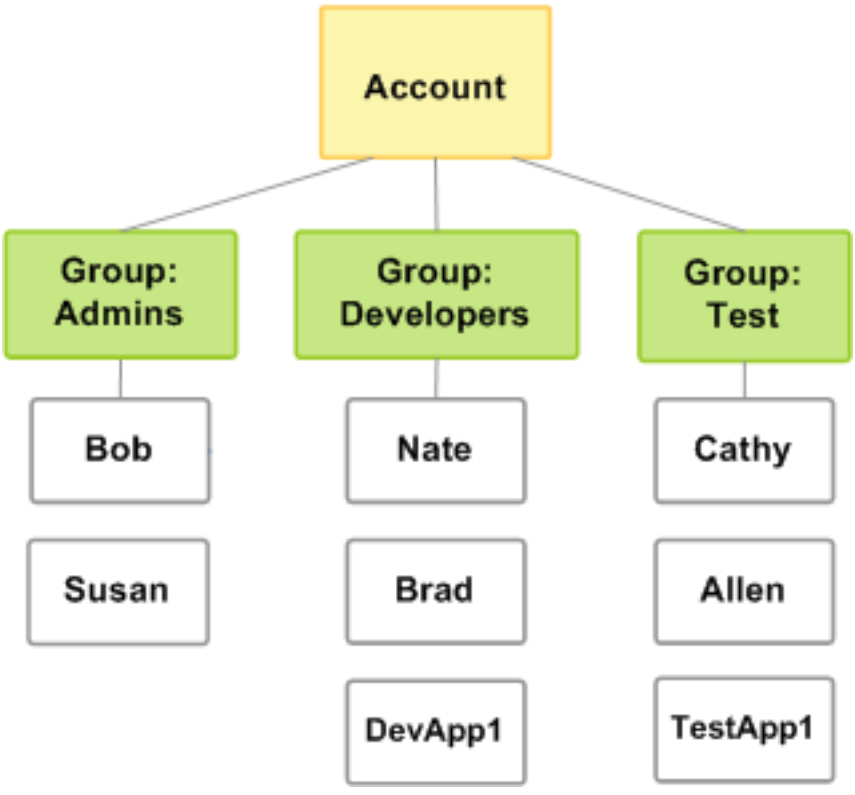
- AWS 계정 자격 증명 관리: AWS General Reference의 AWS 보안 자격 증명
- 시작하기 및 IAM이란? (p. 1)에 대해 자세히 알아보기
- IAM에 사용할 명령줄 인터페이스 설정. 교차 플랫폼 AWS CLI의 경우에는 AWS 명령줄 인터페이스 설명서 또는 IAM CLI 참조를 참조하십시오. 그 밖에 Windows PowerShell을 사용해 IAM을 관리할 수도 있습니다. 자세한 내용은 Windows PowerShell을 위한 AWS 도구 설명서 또는 IAM Windows PowerShell 참조를 참조하십시오.
- 편리한 프로그래밍 방식의 IAM 액세스를 위한 AWS SDK 다운로드: Amazon Web Services 도구
- FAQ 보기: AWS Identity and Access Management FAQ
- 기술 지원: AWS Support 센터
- 프리미엄 기술 지원: AWS Premium Support 센터
- AWS 용어 정의 찾기: Amazon Web Services 글로서리
- 커뮤니티 지원: IAM 토론 포럼
- AWS 문의: 문의처

시작

이 항목에서는 AWS 계정에서 AWS Identity and Access Management(IAM) 사용자를 생성하여 AWS 리소스에 대한 액세스 권한을 부여하는 방법을 보여 줍니다. 먼저 그룹이나 사용자를 생성하기 전에 알고 있어야 할 IAM 개념 몇 가지에 대해 학습한 후 AWS Management 콘솔을 사용해 필요한 작업을 실행하는 방법에 대해 알아볼 것입니다. 첫 번째 작업은 AWS 계정에 관리자 그룹을 구성하는 방법입니다. AWS 계정의 관리자 그룹은 필수는 아니지만 강력히 권장하는 구성입니다.

> Note
>
> 이 설명서에서는 IAM 서비스에 대해 주로 다룹니다. AWS를 시작하는 방법과 여러 서비스를 사용하여 프로젝트 구축 및 개시 등과 같은 문제를 해결하는 방법을 알아보려면 리소스 센터 시작하기 단원을 참조하십시오.

아래 그림은 AWS 계정을 3개 그룹으로 구성한 간단한 예입니다. 하나는 책임이 비슷한 사용자들을 모아놓은 그룹입니다. 이 예에서는 관리자 그룹(Admins라고 표시된 그룹)에 해당합니다. 그 밖에도 Developers 그룹과 Test 그룹이 있습니다. 각 그룹은 사용자가 다수입니다. 그리고 그림과 다르지만 각 사용자는 하나 이상의 그룹에 속할 수 있습니다. 하지만 그룹이 다른 그룹에 포함될 수는 없습니다. 이제 정책을 사용하여 권한을 그룹에게 부여합니다.



다음 절차에서는 아래 작업을 실행하게 됩니다.

- Administrators 그룹을 생성한 후 AWS 계정의 모든 리소스에 액세스할 수 있는 권한을 그룹에게 부여합니다.
- 직접 사용자를 생성하여 Administrators 그룹에 추가합니다.
- AWS Management 콘솔에 로그인할 수 있도록 사용자 암호를 생성합니다.

유효한 모든 AWS 계정 리소스에 액세스할 수 있는 권한을 Administrators 그룹에게 부여합니다. 여기에서 유효한 리소스란 사용 중이거나 등록한 모든 AWS 제품을 의미합니다. Administrators 그룹 사용자는 AWS 계정의 보안 자격 증명만 제외하고 AWS 계정 정보에 액세스할 수 있습니다.

주제

첫 번째 IAM 관리자 및 그룹 생성

> **Important**
>
> 애플리케이션이나 웹 사이트에 Amazon 광고를 설정하려다 이 페이지로 오게 된 경우, Product Advertising API 개발자로서 시작하기 단원을 참조하십시오.

AWS 계정 루트 사용자가 필요하지 않은 작업에는 루트 사용자를 사용하지 않는 것이 바람직한모범 사례 (p. 60)입니다. 그 대신에 관리자 액세스 권한이 필요한 사람마다 새 IAM 사용자를 생성하십시오. 그 다음에는 AdministratorAccess 관리형 정책을 연결하는 "관리자" 그룹에 사용자를 배치하여 그 사용자들을 관리자로 만듭니다.

그 후에 관리자 그룹에 속한 사용자들은 AWS 계정에 대한 그룹, 사용자 등을 설정해야 합니다. 향후 모든 상호작용은 루트 사용자 대신에 AWS 계정 사용자와 그들의 고유 키를 통해 이루어져야 합니다. 하지만 일부 계정 및 서비스 관리 작업을 수행하려면 루트 사용자 계정 자격 증명을 사용하여 로그인해야 합니다. 루트 사용자로 로그인해야 하는 작업을 보려면 계정 루트 사용자가 필요한 AWS 작업 단원을 참조하십시오.

관리자 IAM 사용자 및 그룹 생성(콘솔)

AWS Management 콘솔 이번 섹션에서는 IAM 사용자를 직접 생성하고 그 사용자를 연결된 관리형 정책에 따라 관리자 권한을 보유한 그룹에 추가하는 방법에 대해 살펴보겠습니다.

관리자 사용자를 직접 생성하여 관리자 그룹에 추가하려면(콘솔)

1. https://console.aws.amazon.com/iam/에서 AWS 계정 이메일 주소 및 비밀번호를 AWS 계정 루트 사용자로 사용하여 IAM 콘솔에 로그인합니다.

   > **Note**
   >
   > **`Administrator`** IAM 사용자를 사용하는 아래 모범 사례를 준수하고, 루트 사용자 자격 증명을 안전하게 보관해 두는 것이 좋습니다. 몇 가지 계정 및 서비스 관리 작업을 수행하려면 반드시 루트 사용자로 로그인해야 합니다.

2. 생성할 IAM 관리자에 대한 결제 데이터 액세스를 활성화합니다.

   a. 탐색 표시줄에서 계정 이름을 선택한 다음 내 계정을 선택합니다.
   b. 결제 정보에 대한 IAM 사용자 및 역할 액세스 옆에 있는 편집을 선택합니다.
   c. IAM 액세스 활성화 확인란을 선택하고 업데이트를 선택합니다.
   d. 탐색 표시줄에서 서비스를 선택한 다음, IAM을 선택해 IAM 대시보드로 돌아갑니다.

3. 탐색 창에서 사용자와 사용자 추가를 차례로 선택합니다.
4. [User name]에 **`Administrator`**를 입력합니다.
5. AWS Management 콘솔 access(콘솔 액세스) 옆의 확인란을 선택하고 Custom password(사용자 지정 암호)를 선택한 다음, 텍스트 상자에 새 암호를 입력합니다. 초기 상태는 AWS가 새로운 사용자가 로그인할 때 새 암호를 만들도록 요구합니다. 선택적으로 User must create a new password at next sign-in(사용자는 다음번 로그인 시 새 암호를 생성해야 합니다) 옆 확인란의 선택을 취소하여 새로운 사용자가 로그인한 후 암호를 재설정할 수 있습니다.

6. 다음: 권한을 선택합니다.
7. 권한 설정 페이지에서 그룹에 사용자 추가(Add user to group)를 선택합니다.
8. Create group을 선택합니다.
9. 그룹 생성 대화 상자의 그룹 이름에 **Administrators**를 입력합니다.
10. 정책 필터링을 선택한 다음 AWS 관리형 -job 함수를 선택하여 테이블 내용을 필터링합니다.
11. 정책 목록에서 AdministratorAccess 확인란을 선택합니다. 그런 다음 Create group을 선택합니다.
12. 그룹 목록으로 돌아가 새로 만든 그룹 옆의 확인란을 선택합니다. 목록에서 그룹을 확인하기 위해 필요한 경우 Refresh(새로 고침)를 선택합니다.
13. Next: Tags(다음: 태그)를 선택합니다.
14. (선택 사항) 태그를 키-값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서의 태그 사용에 대한 자세한 정보는 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
15. Next: Review를 선택하여 새 사용자에 추가될 그룹 멤버십의 목록을 확인합니다. 계속 진행할 준비가 되었으면 Create user를 선택합니다.

이와 동일한 절차에 따라 그룹이나 사용자를 추가 생성하여 사용자에게 AWS 계정 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 사용자 권한을 특정 AWS 리소스로 제한하는 정책을 사용하는 방법은 액세스 관리 (p. 348) 및 IAM 자격 증명 기반 정책 예제 (p. 387) 단원을 참조하십시오. 그룹을 생성한 후 추가로 사용자를 추가하려면 IAM 그룹에서 사용자 추가 및 제거 (p. 170) 단원을 참조하십시오.

IAM 사용자 및 그룹 생성(AWS CLI)

앞 단원의 절차를 따랐다면, AWS Management 콘솔을 사용하여 AWS 계정에 IAM 사용자를 생성하는 한편, 관리자 그룹을 설정했을 것입니다. 이 단원에서는 그룹을 생성하는 다른 방법을 소개합니다.

개요: 관리자 그룹 설정

1. 그룹을 생성하고 이름을 지정합니다(예: Admins). 자세한 정보는 그룹 생성(AWS CLI) (p. 21) 단원을 참조하십시오.
2. 그룹 관리 권한(모든 AWS 작업 및 리소스에 대한 액세스 권한)을 부여하는 정책을 연결합니다. 자세한 정보는 그룹에 정책 연결(AWS CLI) (p. 22) 단원을 참조하십시오.
3. 그룹에 한 명 이상의 사용자를 추가합니다. 자세한 정보는 AWS 계정의 IAM 사용자 생성 (p. 87) 단원을 참조하십시오.

그룹 생성(AWS CLI)

이 단원에서는 IAM 시스템에 그룹을 생성하는 방법을 소개합니다.

관리자 그룹을 생성하려면(AWS CLI)

1. `aws iam create-group` 명령과 선택한 그룹 이름을 입력합니다. 그룹 이름에 경로를 포함시킬 수도 있습니다. 경로에 대한 자세한 정보는 표시 이름 및 경로 (p. 563) 단원을 참조하십시오. 이름은 문자, 숫자, 그리고 다음과 같은 기호로 구성될 수 있습니다. 더하기(+), 등호(=), 쉼표(,), 마침표(.), 앳(@), 밑줄(_), 하이픈(-). 이름은 대소문자를 구분하지 않으며 최대 128자입니다.

   이 예제에서는 Admins라는 그룹을 생성합니다.

```
aws iam create-group --group-name Admins
{
    "Group": {
        "Path": "/",
        "CreateDate": "2014-06-05T20:29:53.622Z",
        "GroupId":"ABCDEFGHABCDEFGHABCDE",
```

```
        "Arn": "arn:aws:iam::123456789012:group/Admins",
        "GroupName": "Admins"
    }
}
```

2. `aws iam list-groups` 명령을 입력하여 AWS 계정의 그룹을 나열하고 해당 그룹이 생성되었는지 확인합니다.

```
aws iam list-groups
{
    "Groups": [
        {
            "Path": "/",
            "CreateDate": "2014-06-05T20:29:53.622Z",
            "GroupId":"ABCDEFGHABCDEFGHABCDE",
            "Arn": "arn:aws:iam::123456789012:group/Admins",
            "GroupName": "Admins"
        }
    ]
}
```

응답에는 새 그룹에 대한 Amazon 리소스 이름(ARN)이 포함되어 있습니다. ARN은 AWS에서 리소스를 식별하는 데 사용하는 표준 형식입니다. ARN의 12자리 숫자는 AWS 계정 ID입니다. 그룹에 할당한 표시 이름(Admins)은 그룹 ARN의 끝에 나타납니다.

그룹에 정책 연결(AWS CLI)

이 단원에서는 그룹의 사용자가 AWS 계정의 리소스에 대해 작업을 수행할 수 있도록 허용하는 정책의 연결 방법을 보여 줍니다. 방법은 Admins 그룹에 AdministratorAccess라는 AWS 관리형 정책 (p. 357)을 연결하는 것입니다. 정책에 대한 자세한 정보는 액세스 관리 (p. 348) 단원을 참조하십시오.

모든 관리자 권한을 부여하는 정책을 추가하려면(AWS CLI)

1. `aws iam attach-group-policy` 명령을 입력하여 Admins 그룹에 AdministratorAccess라는 정책을 연결합니다. 이 명령은 AdministratorAccess라는 AWS 관리형 정책의 ARN을 사용합니다.

```
aws iam attach-group-policy --group-name Admins --policy-arn arn:aws:iam::aws:policy/
AdministratorAccess
```

명령이 성공하면 응답이 없습니다.

2. `aws iam list-attached-group-policies` 명령을 입력하여 Admins 그룹에 정책이 연결되었는지 확인합니다.

```
aws iam list-attached-group-policies --group-name Admins
```

응답에는 Admins 그룹에 연결된 정책 이름이 나열됩니다. 다음과 같은 응답은 Admins 그룹에 AdministratorAccess라는 정책이 연결되었다는 것을 알려 줍니다.

```
{
    "AttachedPolicies": [
        {
            "PolicyName": "AdministratorAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
        }
    ],
    "IsTruncated": false
}
```

`aws iam get-policy` 명령을 통해 특정 정책의 콘텐츠를 확인할 수 있습니다.

Important

Administrators 그룹을 설정한 후, 한 명 이상의 사용자를 추가해야 합니다. 그룹에 사용자를 추가하는 방법에 대한 자세한 정보는 AWS 계정의 IAM 사용자 생성 (p. 87) 단원을 참조하십시오.

관련 리소스

Amazon Web Services 일반 참조에서 수록된 관련 내용은 다음 리소스 단원을 참조하십시오.

- 계정 루트 사용자가 필요한 AWS 작업

IAM 사용 설명서에 수록된 관련 내용은 다음 리소스 단원을 참조하십시오.

- 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467)
- 자습서: Billing 콘솔에 대한 액세스 권한 위임 (p. 27)

첫 번째 IAM 위임 사용자 및 그룹 생성

AWS 계정에서 여러 사용자를 지원하려면 다른 사용자가 허용된 작업만 수행할 수 있도록 권한을 위임해야 합니다. 이렇게 하려면 해당 사용자에게 필요한 권한이 있는 IAM 그룹을 생성한 다음 필요에 따라 IAM 사용자를 필요한 그룹에 추가합니다. 이 프로세스를 사용하여 전체 AWS 계정에 대한 그룹, 사용자 및 권한을 설정할 수 있습니다.

이 솔루션은 AWS 관리자가 수동으로 사용자 및 그룹을 관리할 수 있는 중소 규모 조직에서 가장 적합합니다. 대규모 조직에서는 사용자 지정 IAM 역할 (p. 210), 페더레이션 (p. 183) 또는 Single Sign-On을 사용할 수 있습니다.

위임 IAM 사용자 및 그룹 생성(콘솔)

AWS Management 콘솔을 사용하여 위임된 권한이 있는 IAM 그룹을 생성한 다음 다른 사용자에 대해 IAM 사용자를 만들어 그룹에 추가할 수 있습니다.

다른 사용자에 대해 위임 그룹 및 사용자를 생성하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.

   정책를 처음으로 선택하는 경우 Welcome to Managed Policies 페이지가 나타납니다. [Get Started]를 선택합니다.
3. [Create policy]를 선택합니다.
4. JSON 탭을 선택한 다음 창의 오른쪽에서 관리형 정책 가져오기를 선택합니다.
5. 관리형 정책 가져오기 창에 **`power`**를 입력하여 정책 목록을 줄입니다. 그런 다음 PowerUserAccess AWS 관리형 정책 옆에 있는 버튼을 선택합니다.
6. [Import]를 선택합니다.

   가져온 정책이 JSON 정책에 추가됩니다.
7. [Review policy]를 선택합니다.
8. 검토 페이지의 이름에 **`PowerUserExampleCorp`**를 입력합니다. 설명에 **`Allows full access to all services except those for user management`**을 입력합니다. 그런 다음 [Create policy]를 선택하여 작업을 저장합니다.

9. 탐색 창에서 그룹을 선택한 다음, 새 그룹 생성을 선택합니다.
10. 그룹 이름 상자에 **PowerUsers**를 입력합니다.
11. 정책 목록에서 PowerUserExampleCorp 옆의 확인란을 선택합니다. 그런 다음 [Next Step]을 선택합니다.
12. Create Group을 선택합니다.
13. 탐색 창에서 사용자와 Add user(사용자 추가)를 차례로 선택합니다.
14. [User name]에 **mary.major@examplecorp.com**를 입력합니다.
15. 다른 사용자 추가를 선택하고 두 번째 사용자에 대해 **diego.ramirez@examplecorp.com**을 입력합니다.
16. AWS Management 콘솔 액세스 옆의 확인란을 선택하고 자동 생성된 암호를 선택합니다. 초기 상태는 AWS가 새로운 사용자가 로그인할 때 새 암호를 만들도록 요구합니다. 새로운 사용자가 로그인한 후 암호를 재설정할 수 있도록 사용자가 다음에 로그인할 때 새 암호를 생성해야 합니다 확인란의 선택을 취소합니다.
17. 다음: 권한을 선택합니다.
18. 권한 설정 페이지에서 그룹에 사용자 추가를 선택한 다음 PowerUsers 옆의 확인란을 선택합니다.
19. 다음: 태그를 선택합니다.
20. (선택 사항) 태그를 키-값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서의 태그 사용에 대한 자세한 정보는 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
21. Next: Review를 선택하여 새 사용자에 추가될 그룹 멤버십의 목록을 확인합니다. 계속 진행할 준비가 되었으면 사용자 생성을 선택합니다.
22. 새 사용자의 암호를 다운로드하거나 복사하여 사용자에게 안전하게 전달합니다. 별도로 사용자에게 IAM 사용자 콘솔 페이지에 대한 링크 (p. 74)와 방금 생성한 사용자 이름을 제공합니다.

그룹 권한 줄이기

`PowerUser` 그룹의 멤버는 사용자 관리 작업(예: IAM 및 조직)을 제공하는 일부 서비스를 제외한 모든 서비스에 대해 전체 권한을 갖습니다. 사전 정의된 비활성 기간(예: 90일)이 지난 후에는 그룹 멤버가 액세스한 서비스를 검토할 수 있습니다. 그런 다음 팀에 필요한 서비스만 포함하도록 `PowerUserExampleCorp` 정책의 권한을 줄일 수 있습니다.

서비스에서 마지막으로 액세스한 데이터에 대한 자세한 정보는 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

서비스에서 마지막으로 액세스한 데이터 검토

사전 정의된 비활성 기간(예: 90일)이 끝날 때까지 기다립니다. 그런 다음 사용자 또는 그룹에 대해 서비스에서 마지막으로 액세스한 데이터를 검토하여 사용자가 `PowerUserExampleCorp` 정책에서 허용하는 서비스에 마지막으로 액세스를 시도한 시기를 확인할 수 있습니다.

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 그룹을 선택한 다음 PowerUser 그룹 이름을 선택합니다.
3. 그룹 요약 페이지에서 액세스 관리자 탭을 선택합니다.

   서비스에서 마지막으로 액세스한 데이터 테이블에는 그룹 멤버가 마지막으로 각 서비스에 액세스하려고 시도한 시간이 시간 순으로 표시됩니다. 이 테이블에는 정책에서 허용하는 서비스만 포함됩니다. 이 경우 `PowerUserExampleCorp` 정책은 모든 AWS 서비스에 대한 액세스를 허용합니다.
4. 테이블을 검토하고 그룹 멤버가 최근에 액세스한 서비스에 대한 목록을 만듭니다.

   예를 들어, 지난 달 내에 팀이 Amazon EC2 및 Amazon S3 서비스에만 액세스했다고 가정합니다. 그러나 6개월 전, 팀에서 Amazon EC2 Auto Scaling 및 IAM에 액세스했습니다. EC2 Auto Scaling을 조사했지만 필요하지 않다고 결정했습니다. 또한 IAM을 사용하여 Amazon EC2가 S3 버킷의 데이터에 액세스

할 수 있는 역할을 생성했습니다. 따라서 Amazon EC2 및 Amazon S3 서비스만 액세스할 수 있도록 사용자의 권한을 다시 축소하기로 결정했습니다.

정책을 편집하여 권한 줄이기

서비스에서 마지막으로 액세스한 데이터를 검토한 후 사용자가 필요로 하는 서비스에만 액세스할 수 있도록 정책을 편집할 수 있습니다.

필요한 서비스에만 액세스할 수 있도록 데이터를 사용하려면

1. 왼쪽 탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.
2. 정책 편집을 선택한 후 JSON 탭을 선택합니다.
3. 원하는 서비스만 허용하도록 JSON 정책 문서를 편집합니다.

   예를 들어, `Allow` 효과와 `NotAction` 요소를 포함하는 첫 번째 명령문을 편집하여 Amazon EC2 및 Amazon S3 작업만 허용하도록 합니다. 이 작업을 수행하려면 `FullAccessToSomeServices` ID가 있는 명령문으로 바꿉니다. 새 정책은 다음 예제 정책과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "FullAccessToSomeServices",
          "Effect": "Allow",
          "Action": [
              "ec2:*",
              "s3:*"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:CreateServiceLinkedRole",
              "iam:DeleteServiceLinkedRole",
              "iam:ListRoles",
              "organizations:DescribeOrganization"
          ],
          "Resource": "*"
      }
  ]
}
```

4. 특정 작업 및 리소스에 대한 정책 권한을 추가로 줄이려면 CloudTrail 이벤트 기록에서 이벤트를 확인합니다. 여기에서 사용자가 액세스한 특정 작업 및 리소스에 대한 자세한 정보를 볼 수 있습니다. 자세한 정보는 AWS CloudTrail 사용 설명서에서 CloudTrail 콘솔에서 CloudTrail 이벤트 보기 단원을 참조하십시오.

사용자의 계정 로그인 방법

암호를 사용하여 IAM 사용자를 생성하면 해당 사용자가 AWS Management 콘솔에 로그인할 수 있습니다. 로그인하려면 계정 ID 또는 별칭이 필요합니다. 또한 계정 ID가 포함된 사용자 지정 URL에서 로그인할 수도 있습니다.

Note

회사에 기존의 자격 증명 시스템이 있는 경우, Single Sign-On(SSO) 옵션을 만드는 것이 좋습니다. SSO는 IAM 사용자 자격 증명이 없어도 AWS Management 콘솔에 액세스할 수 있는 권한을 사용

자에게 제공합니다. 또한 SSO를 사용하면 사용자가 조직의 사이트와 AWS에 따로 로그인하지 않아도 됩니다. 자세한 내용은 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.

계정의 로그인 URL을 생성하기 전에 계정 별칭을 생성합니다. 그러면 URL에 계정 ID 대신 계정 이름이 포함됩니다. 자세한 내용은 AWS 계정 ID 및 별칭 (p. 77) 단원을 참조하십시오.

IAM 콘솔 대시보드에서 계정의 로그인 URL을 확인할 수 있습니다.

IAM 사용자에 대한 로그인 URL을 생성하려면 다음 패턴을 따르십시오.

```
https://account-ID-or-alias.signin.aws.amazon.com/console
```

IAM 사용자는 다음 엔드포인트에서 로그인한 다음 사용자 지정 URL을 사용하는 대신 계정 ID 또는 별칭을 수동으로 입력할 수도 있습니다.

```
https://signin.aws.amazon.com/console
```

콘솔 활동에 필요한 권한

IAM 사용자는 정책에서 지정한 AWS 리소스에만 액세스할 수 있습니다. 해당 정책은 사용자 또는 사용자가 속한 IAM 그룹에 연결되어야 합니다. 콘솔에서 작업하려면 AWS 리소스 표시 및 생성과 같은 콘솔이 실행하는 작업을 실행할 허가를 받아야 합니다. 자세한 내용은 액세스 관리 (p. 348) 및 IAM 자격 증명 기반 정책 예제 (p. 387)을(를) 참조하십시오.

계정의 사용자에게 프로그래밍 방식의 액세스가 필요한 경우 각 사용자의 액세스 키 페어(액세스 키 ID 및 보안 액세스 키)를 생성할 수 있습니다. 자세한 내용은 액세스 키 관리(콘솔) (p. 112) 단원을 참조하십시오.

CloudTrail에 로그인 세부 정보 기록

로그인 이벤트를 기록하도록 CloudTrail을 활성화한 경우 CloudTrail에서 이벤트를 기록하는 방법을 이해해야 합니다. CloudTrail에는 전역 및 리전 로그 항목이 포함됩니다. 로그인 이벤트가 CloudTrail에 로그인되는 위치는 사용자의 로그인 방법에 따라 다릅니다. 자세한 내용은 CloudTrail을 사용하여 IAM 이벤트 로깅을 참조하십시오.

IAM 자습서

이 섹션은 IAM에서 수행하는 일반적인 작업에 대한 처음부터 끝까지의 완전한 절차를 일별하는 내용을 담고 있습니다. 그 절차들은 랩 유형의 환경에 맞게 고안되었고 예로 사용할 회사 이름, 사용자 이름 등이 있습니다. 그 목적은 일반적인 지침을 제공하는 것입니다. 조직의 환경이 지닌 고유한 측면에 대한 주의 깊은 검토 및 적응 없이 생산 환경에 바로 사용할 수 있도록 고안된 것이 아닙니다.

주제

자습서: Billing 콘솔에 대한 액세스 권한 위임

AWS 계정 소유자는 IAM 계정의 AWS Billing and Cost Management 데이터를 보거나 관리해야 하는 특정 AWS 사용자에게 액세스 권한을 위임할 수 있습니다. 다음 지침은 사전 테스트된 시나리오를 설정하는 데 참고로 사용할 수 있습니다. 이 시나리오는 기본 AWS 프로덕션 계정에 영향을 주지 않고 결제 권한을 구성하는 실무 경험을 얻는 데 도움이 됩니다.

이 워크플로우는 네 가지 기본 단계로 이루어집니다.

1단계: AWS 테스트 계정에서 결제 데이터에 대한 액세스 권한 활성화 (p. 28)

단일 AWS 계정을 생성하는 경우 AWS 계정 소유자(AWS 계정 루트 사용자 (p. 331))만 결제 정보를 보고 관리할 수 있습니다. IAM 사용자는 계정 소유자가 IAM 액세스를 활성화하고 사용자 또는 역할에 결제 작업을 제공하는 정책을 연결해야 결제 데이터에 액세스할 수 있습니다. 루트 사용자로 로그인해야 하는 다른 작업을 보려면 계정 루트 사용자가 필요한 AWS 작업 단원을 참조하십시오.

AWS Organizations를 사용하여 멤버 계정을 생성하는 경우 이 기능이 기본적으로 활성화됩니다.

2단계: 결제 데이터에 대한 권한을 부여하는 IAM 정책 생성 (p. 28)

계정에서 결제 액세스 권한을 활성화한 후에도 특정 IAM 사용자 또는 그룹에게 명시적으로 결제 데이터 액세스 권한을 부여해야 합니다. 이 액세스 권한은 고객 관리형 정책을 사용하여 부여합니다.

3단계: 그룹에 결제 정책 연결 (p. 29)

정책을 그룹에 연결할 경우 해당 그룹의 모든 멤버가 해당 정책과 관련된 액세스 권한의 전체 집합을 부여받습니다. 이 시나리오에서는 새 결제 정책을 결제 액세스 권한이 필요한 사용자만 포함하는 그룹에 연결합니다.

4단계: Billing 콘솔에 대한 사용자 액세스 권한 테스트 (p. 29)

핵심 과제를 완료했으므로 정책을 테스트할 수 있습니다. 테스트는 정책이 의도된 대로 동작하는지 확인합니다.

사전 조건

이 자습서를 사용해 테스트 AWS 계정을 생성합니다. 다음 테이블에 요약된 대로 이 계정에서 테스트 사용자 2명과 테스트 그룹 2개를 생성합니다. 나중에 4단계에서 로그인할 수 있도록 각 사용자에게 암호를 배정하십시오.

사용자 계정 생성	그룹 계정 생성 및 구성	
FinanceManager	BillingFullAccessGroup	FinanceManager
FinanceUser	BillingViewAccessGroup	FinanceUser

1단계: AWS 테스트 계정에서 결제 데이터에 대한 액세스 권한 활성화

먼저 테스트 사용자의 결제 액세스 권한을 활성화합니다. 이 작업을 수행하려면 AWS Billing and Cost Management 사용 설명서의 결제 및 비용 관리 콘솔에 대한 액세스 활성화를 참조하십시오.

Note

AWS Organizations를 사용하여 멤버 계정을 생성하는 경우 이 기능이 기본적으로 활성화됩니다.

2단계: 결제 데이터에 대한 권한을 부여하는 IAM 정책 생성

다음 단계에서는 Billing and Cost Management 콘솔 내 페이지에 대한 보기 및 전체 액세스 권한을 모두 부여하는 사용자 지정 정책을 생성합니다. IAM 권한 정책에 대한 일반 정보는 관리형 정책 및 인라인 정책 (p. 357)을 참조하십시오.

결제 데이터에 대한 권한을 부여하는 IAM 정책을 생성하려면

1. 관리자 자격 증명을 가진 사용자로 AWS Management 콘솔에 로그인합니다. IAM 모범 사례를 준수하려면 루트 사용자 자격 증명을 사용하여 로그인하지 마십시오. 자세한 정보는 개별 IAM 사용자 만들기 (p. 61) 단원을 참조하십시오.
2. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
3. 탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.
4. Visual editor(시각적 편집기) 탭에서 Choose a service(서비스 선택)을 선택하여 시작합니다. 그런 다음 결제를 선택합니다.
5. 다음 두 단계를 사용하여 두 가지 정책을 생성합니다.

   모든 액세스

   a. 작업 선택(Select actions)을 선택한 다음 모든 작업(*)(All Actions (*)) 옆에 있는 확인란을 선택합니다. 이 정책에 대한 리소스 또는 조건을 선택할 필요가 없습니다.
   b. [Review policy]를 선택합니다.
   c. 검토 페이지에서 이름 옆에 **`BillingFullAccess`**를 입력한 다음 정책 생성을 선택하여 저장합니다.

   읽기 전용 액세스

   a. 3 및 4 (p. 28)단계를 반복합니다.
   b. Select actions(작업 선택)을 선택한 다음 읽기 옆에 있는 확인란을 선택합니다. 이 정책에 대한 리소스 또는 조건을 선택할 필요가 없습니다.
   c. [Review policy]를 선택합니다.
   d. 검토 페이지의 이름에 **`BillingViewAccess`**를 입력합니다. 그런 다음 정책 생성을 선택하여 저장합니다.

Billing and Cost Management 콘솔에 대한 사용자 액세스 권한을 부여하는 IAM 정책에서 사용 가능한 각 권한에 대한 설명을 보려면 결제 권한 설명 단원을 참조하십시오.

3단계: 그룹에 결제 정책 연결

이제 사용자 지정 결제 정책이 준비되었으므로 앞서 만든 그룹에 정책을 연결할 수 있습니다. 정책을 사용자 또는 역할에 직접 연결할 수 있지만, (IAM 모범 사례에 따라) 그룹을 대신 사용하는 것이 좋습니다. 자세한 정보는 그룹을 사용하여 IAM 사용자에게 권한 할당 (p. 61) 단원을 참조하십시오.

그룹에 결제 정책을 연결하려면

1. 탐색 창에서 정책을 선택하여 AWS 계정에 사용 가능한 정책의 전체 목록을 표시합니다. 각 정책을 적절한 그룹에 연결하려면 다음 단계를 수행합니다.

   모든 액세스

   a. 정책 검색 상자에 **`BillingFullAccess`**를 입력한 다음, 정책 이름 옆의 확인란을 선택합니다.
   b. [Policy actions]를 선택한 후 [Attach]를 선택합니다.
   c. 자격 증명(사용자, 그룹 및 역할) 검색 상자에 **`BillingFullAccessGroup`**를 입력하고 그룹 이름 옆의 확인란을 선택한 다음, 정책 연결을 선택합니다.

   읽기 전용 액세스

   a. 정책 검색 상자에 **`BillingViewAccess`**를 입력한 다음, 정책 이름 옆의 확인란을 선택합니다.
   b. [Policy actions]를 선택한 후 [Attach]를 선택합니다.
   c. 자격 증명(사용자, 그룹 및 역할) 검색 상자에 **`BillingViewAccessGroup`**를 입력하고 그룹 이름 옆의 확인란을 선택한 다음, 정책 연결을 선택합니다.
2. 콘솔에서 로그아웃하고 다음(4단계: Billing 콘솔에 대한 사용자 액세스 권한 테스트 (p. 29))을 진행합니다.

4단계: Billing 콘솔에 대한 사용자 액세스 권한 테스트

사용자가 어떤 경험을 하게 되는지 볼 수 있도록 각 테스트 사용자로 로그인하여 액세스 권한을 테스트할 것을 권장합니다. 다음 단계에 따라 두 테스트 계정으로 로그인하여 액세스 권한 차이를 확인합니다.

두 테스트 사용자 계정으로 로그인하여 결제 액세스 권한을 테스트하려면

1. AWS 계정 ID나 계정 별칭, IAM 사용자 이름 및 암호를 사용하여 IAM 콘솔에 로그인합니다.

   Note

   사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 이전에 다른 사용자로 로그인한 경우 페이지 하단 근처의 Sign in to a different account(다른 계정에 로그인)를 선택하여 기본 로그인 페이지로 돌아갑니다. 여기서 AWS 계정 ID 또는 계정 별칭을 입력하면 계정의 IAM 사용자 로그인 페이지로 리디렉션됩니다.
2. 각 사용자 환경을 비교할 수 있도록 아래 제공된 단계를 사용하여 각 계정으로 로그인합니다.

   모든 액세스

   a. 사용자 FinanceManager로 AWS 계정에 로그인합니다.
   b. 탐색 모음에서 FinanceManager@***`<account alias or ID number>`***를 선택하고 내 결제 대시보드를 선택합니다.

c. 각 페이지를 탐색하면서 다양한 버튼을 선택하여 모든 수정 권한이 있는지 확인합니다.

읽기 전용 액세스

a. 사용자 FinanceUser로 AWS 계정에 로그인합니다.
b. 탐색 모음에서 FinanceUser@*<account alias or ID number>*를 선택하고 내 결제 대시보드를 선택합니다.
c. 각 페이지를 탐색해 봅니다. 비용, 보고서 및 결제 데이터는 아무 문제 없이 표시될 것입니다. 하지만 값을 수정하는 옵션을 선택할 경우 액세스 거부됨 메시지가 표시됩니다. 예를 들어 기본 설정 페이지에서 아무 확인란이나 선택하고 기본 설정 저장을 선택합니다. 콘솔이 해당 페이지를 수정하려면 ModifyBilling 권한이 필요하다는 메시지를 표시합니다.

관련 리소스

AWS Billing and Cost Management 사용 설명서에서 수록된 관련 내용은 다음 리소스 단원을 참조하십시오.

- 대금 및 비용 관리 콘솔에 대한 액세스 권한 활성화
- 예제 4: AWS 서비스에 대한 모든 액세스 권한을 허용하되 대금 및 비용 관리 콘솔에 대한 IAM 사용자 액세스는 거부.
- 결제 권한 설명

IAM 사용 설명서에 수록된 관련 내용은 다음 리소스 단원을 참조하십시오.

- 관리형 정책과 인라인 정책 (p. 357)
- AWS Management 콘솔에 대한 사용자 액세스 제어 (p. 76)
- IAM 그룹에 정책 연결 (p. 171)

요약

이제 Billing and Cost Management 콘솔에 대한 사용자 액세스 권한을 위임하는 데 필요한 단계를 모두 성공적으로 완료했습니다. 결과적으로 사용자 결제 콘솔 환경을 직접 확인할 수 있습니다. 이제 편의에 따라 프로덕션 환경에서 이 로직을 구현할 수 있습니다.

자습서: IAM 역할을 사용한 AWS 계정 간 액세스 권한 위임

이 자습서는 소유하고 있는 다른 AWS 계정(Production 및 Development)의 리소스에 역할을 사용하여 액세스 권한을 위임하는 방법에 대해 설명합니다. 한 계정의 리소스는 다른 계정의 사용자와 공유합니다. 이러한 방식으로 교차 계정 액세스를 설정하면 각 계정에 개별 IAM 사용자를 생성할 필요가 없습니다. 또한 사용자는 다른 AWS 계정의 리소스에 액세스하기 위해 한 계정에서 로그아웃하고 다른 계정에 로그인할 필요가 없습니다. 역할을 구성한 후에는 AWS Management 콘솔, AWS CLI 및 API에서 역할을 사용하는 방법에 대해서도 알아봅니다.

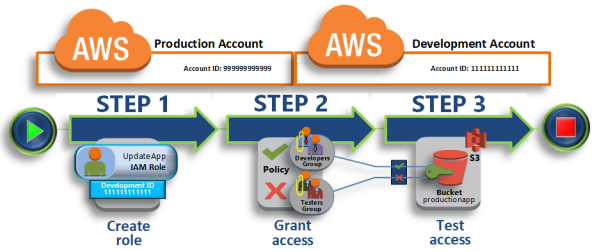
이 자습서에서는 Production 계정이 라이브 애플리케이션을 관리하는 위치라고 가정합니다. Development 계정은 개발자와 테스터가 자유롭게 애플리케이션을 테스트할 수 있는 샌드박스입니다. 각 계정의 애플리케이션 정보는 Amazon S3 버킷에 저장됩니다. Developers와 Testers, 두 IAM 그룹으로 구성된 Development 계정에서는 IAM 사용자를 관리합니다. 두 그룹의 사용자는 Development 계정에서 작업하면서 리소스에 액세스할 수 있는 권한을 갖습니다. 개발자는 종종 Production 계정의 라이브 애플리케이션을 업데이트해야 합니다. 이들 애플리케이션은 `productionapp`이라고 하는 Amazon S3 버킷에 저장되어 있습니다.

이 자습서의 마지막에서는 다음 항목을 갖게 됩니다.

- `Production` 계정의 특정 역할을 맡을 수 있는 `Development` 계정(신뢰할 수 있는 계정)의 사용자
- 특정 Amazon S3 버킷에 액세스할 수 있는 `Production` 계정(신뢰하는 계정)의 역할
- `Production` 계정의 `productionapp` 버킷

그러면 개발자들이 AWS Management 콘솔에서 이 역할을 사용하여 Production 계정의 `productionapp` 버킷에 액세스할 수 있습니다. 또한 역할을 통해 제공되는 임시 자격 증명으로 API 호출을 인증함으로써 버킷에 액세스하는 것도 가능합니다. 하지만 테스터는 이 역할을 사용하지 못합니다.

이 워크플로우는 세 가지 기본 단계로 이루어집니다.



1단계: 역할 생성 (p. 32)

먼저 AWS Management 콘솔을 사용하여 Production 계정(ID 번호 999999999999)과 Development 계정(ID 번호 111111111111) 사이에 신뢰를 구성합니다. UpdateApp이라는 IAM 역할을 생성하여 시작합니다. 역할을 생성하였으면 Development 계정을 신뢰할 수 있는 엔터티로 정의한 다음 신뢰할 수 있는 계정의 사용자가 `productionapp` 버킷을 업데이트할 수 있는 권한 정책을 지정합니다.

2단계: 역할에 대한 액세스 권한 부여 (p. 34)

이 자습서 단계에서는 테스터들이 `UpdateApp` 역할에 액세스하지 못하도록 IAM 그룹 정책을 변경합니다. Testers 그룹은 이 시나리오에서 PowerUser 액세스 권한을 갖기 때문에 역할을 사용하지 못하도록 명시적으로 거부해야 합니다.

3단계: 역할을 전환하여 액세스 테스트 (p. 35)

마지막으로, 개발자로서 `UpdateApp` 역할을 사용하여 Production 계정의 `productionapp` 버킷을 업데이트합니다. 이제 AWS 콘솔, AWS CLI 및 API를 통해 역할에 액세스할 수 있게 되었습니다.

사전 조건

이 자습서에서는 다음을 이미 완료했다고 가정합니다.

- Development 계정 및 Production 계정으로 사용할 수 있는 2개의 AWS 계정.
- Development 계정에서 다음과 같이 생성 및 구성된 사용자 및 그룹:

사용자	그룹	권한
David	개발자	두 사용자 모두 `Development` 계정에서 AWS Management 콘솔에 로그인하고 사용할 수 있습니다.
Theresa	테스터	

- Production 계정에서는 사용자 또는 그룹을 생성할 필요가 없습니다.
- Production 계정에서 생성된 Amazon S3 버킷. 이 자습서에서는 이 버킷을 `ProductionApp`이라고 부릅니다. 하지만 S3 버킷 이름은 전역에서 고유해야 하므로 다른 이름의 버킷을 사용해야 합니다.

1단계: 역할 생성

한 AWS 계정의 사용자가 다른 AWS 계정의 리소스에 액세스하도록 허용할 수 있습니다. 이렇게 하려면 액세스할 수 있는 사용자와 해당 역할로 전환한 사용자에게 부여할 권한을 정의합니다.

자습서 1단계에서는 Production 계정에서 역할을 생성하고 Development 계정을 신뢰할 수 있는 엔터티로 지정합니다. 또한 역할 권한을 `productionapp` 버킷에 대한 읽기 및 쓰기 액세스 권한으로 제한합니다. 따라서 역할을 사용할 수 있는 권한을 받은 사용자는 누구나 `productionapp` 버킷에 대해 읽기나 쓰기가 가능합니다.

역할을 생성하려면 먼저 Development AWS 계정의 ID가 필요합니다. 계정 ID는 AWS 계정에 할당된 고유 식별자입니다.

Development AWS 계정 ID를 가져오는 방법

1. Development 계정 관리자로 AWS Management 콘솔에 로그인한 후 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 모음에서 지원을 선택한 후 지원 센터를 선택합니다. 현재 로그인한 12자리 계정 번호(ID)는 지원 센터 제목 표시줄에 나타납니다. 이 시나리오에서는 Development 계정 ID가 111111111111이라고 가정합니다. 그러나 테스트 환경에서 시나리오를 재구성하는 경우에는 유효한 계정 ID를 사용해야 합니다.

Development 계정에서 사용할 수 있도록 Production 계정의 역할을 생성하는 방법

1. Production 계정 관리자로 AWS Management 콘솔에 로그인한 후 IAM 콘솔을 엽니다.
2. 역할을 만들기 전에 먼저 해당 역할에 필요한 권한을 정의하는 관리형 정책을 준비합니다. 차후 단계에서 이 정책을 해당 역할에 연결합니다.

   `productionapp` 버킷에 대한 읽기 및 쓰기 액세스 권한을 설정하려고 합니다. AWS에 이미 몇 가지 Amazon S3 관리형 정책이 있지만 단일 Amazon S3 버킷에 대한 읽기 및 쓰기 액세스가 가능한 정책은 없습니다. 대신에 사용자가 직접 정책을 생성할 수 있습니다.

   왼쪽 탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.
3. JSON 탭을 선택하고 다음 JSON 정책 문서에서 텍스트를 복사합니다. 이 텍스트를 JSON 텍스트 상자에 붙여 넣어 리소스 ARN(`arn:aws:s3:::productionapp`)을 S3 버킷에 적합한 것으로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
       ],
      "Resource": "arn:aws:s3:::productionapp"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
```

```
      "Resource": "arn:aws:s3:::productionapp/*"
    }
  ]
}
```

ListBucket은 사용자가 productionapp 버킷에 저장되어 있는 객체를 볼 수 있는 권한입니다. GetObject, PutObject 및 DeleteObject는 사용자가 productionapp 버킷에 저장되어 있는 콘텐츠를 각각 보거나, 업데이트하거나, 삭제할 수 있는 권한입니다.

4. 작업이 완료되면 [Review policy]를 선택합니다. 정책 검사기 (p. 441)가 모든 구문 오류를 보고합니다.

   Note

   언제든지 Visual editor(시각적 편집기) 탭과 JSON 탭 간을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 정책 재구성 (p. 538) 단원을 참조하십시오.

5. 검토 페이지에서 정책 이름에 **read-write-app-bucket**을 입력합니다. 정책 요약을 검토하여 정책이 부여한 권한을 확인한 다음 정책 생성을 선택하여 작업을 저장합니다.

   새로운 정책이 관리형 정책 목록에 나타납니다.

6. 왼쪽 탐색 창에서 역할을 선택한 후 역할 만들기를 선택합니다.
7. 다른 AWS 계정 역할 유형을 선택합니다.
8. 계정 ID에 Development 계정 ID를 입력합니다.

   이 자습서에서는 Development 계정 ID의 예로 **111111111111**을 사용합니다. 하지만 실제로는 유효한 계정 ID를 사용해야 합니다. **111111111111** 같이 잘못된 계정 ID를 사용할 경우, IAM에서 새로운 역할을 생성할 수 없습니다.

   이 연습에서는 외부 ID를 요구하거나, 사용자가 역할을 위임하기 위해 멀티 팩터 인증(MFA)을 요구할 필요가 없습니다. 따라서 이러한 옵션을 선택하지 않은 상태로 두십시오. 자세한 정보는 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.

9. 다음: 권한을 클릭하여 역할과 연결될 권한을 설정합니다.
10. 앞에서 생성한 정책 옆의 상자를 선택합니다.

    도움말

    필터에서 Customer managed(고객 관리형)을 선택하여 생성한 정책만 포함하도록 목록을 필터링합다. 이렇게 하면 AWS에서 생성한 정책이 표시되지 않아서 찾고자 하는 정책을 쉽게 찾을 수 있습니다.

   그런 후 다음: 태그를 선택합니다.

11. (선택 사항) 태그를 키-값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서의 태그 사용에 대한 자세한 정보는 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
12. 다음: 검토를 선택하고 역할 이름으로 **UpdateApp**을 입력합니다.
13. (선택 사항) [Role description]에 새 역할에 대한 설명을 입력합니다.
14. 역할을 검토한 후 역할 만들기를 선택합니다.

    역할 목록에 UpdateApp 역할이 표시됩니다.

이제 역할의 고유 식별자인 Amazon 리소스 이름(ARN)을 가져와야 합니다. Developers 및 Testers 그룹의 정책을 변경하면서 권한을 부여하거나 거부하려면 역할의 ARN을 지정해야 합니다.

UpdateApp 역할의 ARN을 가져오려면

1. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다.

2. 역할 목록에서 `UpdateApp` 역할을 선택합니다.
3. 세부 정보 창의 요약 섹션에서 역할 ARN 값을 복사합니다.

   Production 계정 ID는 999999999999입니다. 따라서 역할 ARN은 `arn:aws:iam::999999999999:role/UpdateApp`이 됩니다. 하지만 사용자 환경에서는 'Production' 계정에 실제 AWS 계정 ID를 입력해야 합니다.

이 시점에서 Production 계정 및 Development 계정 간에 신뢰를 설정했습니다. Production 계정에서 Development 계정을 신뢰할 수 있는 보안 주체로 식별하는 역할을 생성하여 이 작업을 수행했습니다. 그 밖에도 `UpdateApp` 역할 전환 사용자의 권한까지 정의했습니다.

다음에는 그룹 권한을 변경하는 방법에 대해 알아보겠습니다.

2단계: 역할에 대한 액세스 권한 부여

여기에서는 Testers 그룹 멤버나 Developers 그룹 멤버 모두 Development 계정의 애플리케이션을 자유롭게 테스트할 수 있는 권한을 갖습니다. 하지만 역할 전환에 필요한 권한을 추가하려면 몇 단계를 거쳐야 합니다.

UpdateApp 역할로 전환할 수 있도록 Developers 그룹을 변경하는 방법

1. Development 계정에 관리자로 로그인한 다음 IAM 콘솔을 엽니다.
2. 그룹을 선택한 후 Developers(개발자)를 선택합니다.
3. 권한 탭을 선택하고 Inline Policies(인라인 정책) 섹션을 확장한 후 Create Group Policy(그룹 정책 생성)을 선택합니다. 인라인 정책이 아직 없으면 이 버튼이 표시되지 않습니다. 이 경우 "To create one, click here" 끝의 링크를 선택합니다.
4. 사용자 지정 정책을 선택한 후 선택 버튼을 선택합니다.
5. **`allow-assume-S3-role-in-production`**과 같이 정책 이름을 입력합니다.
6. 아래 정책 문을 추가하여 Production 계정에서 `AssumeRole` 역할의 `UpdateApp` 작업을 허용합니다. 이때 `Resource` 요소에서 *`PRODUCTION-ACCOUNT-ID`*는 Production 계정의 실제 AWS 계정 ID로 변경해야 합니다.

   ```
   {
     "Version": "2012-10-17",
     "Statement": {
       "Effect": "Allow",
       "Action": "sts:AssumeRole",
       "Resource": "arn:aws:iam::PRODUCTION-ACCOUNT-ID:role/UpdateApp"
     }
   }
   ```

   `Allow`는 Production 계정에서 `UpdateApp` 역할에 대한 Developers 그룹의 액세스를 명시적으로 허용하는 값입니다. 따라서 개발자라면 누구나 이 역할에 액세스할 수 있습니다.
7. Apply Policy(정책 적용)을 선택하여 정책을 Developer 그룹에 추가합니다.

대부분 환경에서 다음과 같은 절차는 필요하지 않습니다. 하지만 Power User 권한을 사용하는 경우에는 역할 전환을 할 수 있는 그룹이 있을 수도 있습니다. 다음 절차에서는 Testers 그룹에게 역할을 위임할 수 없도록 "Deny" 권한을 추가하는 방법을 보여 줍니다. 이 절차가 필요 없는 환경인 경우 추가하지 않는 것이 좋습니다. '거부' 권한은 전체 권한 구조를 관리하고 이해하기가 더 복잡하게 만듭니다. "Deny" 권한은 더 좋은 방법이 없을 때만 사용하십시오.

UpdateApp 역할 위임 권한을 거부하도록 Testers 그룹을 변경하는 방법

1. 그룹을 선택한 후 Testers(테스터)를 선택합니다.

2. 권한 탭을 선택하고 Inline Policies(인라인 정책) 섹션을 확장한 후 Create Group Policy(그룹 정책 생성)을 선택합니다.
3. 사용자 지정 정책을 선택한 후 선택 버튼을 선택합니다.
4. **deny-assume-S3-role-in-production**과 같이 정책 이름을 입력합니다.
5. 다음 정책을 추가하여 `AssumeRole` 역할의 `UpdateApp` 작업을 거부합니다. 이때 `Resource` 요소에서 *PRODUCTION-ACCOUNT-ID*는 Production 계정의 실제 AWS 계정 ID로 변경해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::PRODUCTION-ACCOUNT-ID:role/UpdateApp"
  }
}
```

   `Deny`는 Production 계정에서 `UpdateApp` 역할에 대한 Testers 그룹의 액세스를 명시적으로 거부하는 값입니다. 따라서 이 역할에 액세스하려는 테스터에게는 모두 액세스 거부 메시지가 표시됩니다.
6. Apply Policy(정책 적용)를 선택한 후 정책을 Tester 그룹에 추가합니다.

Developers 그룹은 이제 Production 계정에서 `UpdateApp` 역할을 사용할 수 있는 권한이 생겼습니다. 그리고 Testers 그룹은 `UpdateApp` 역할을 사용하지 못합니다.

다음으로 개발자인 David가 Production 계정의 `productionapp` 버킷에 액세스하는 방법을 알아봅니다. David는 AWS Management 콘솔, AWS CLI 또는 AWS API에서 버킷에 액세스할 수 있습니다.

3단계: 역할을 전환하여 액세스 테스트

이 자습서의 첫 두 단계를 완료하면 Production 계정에 리소스에 대한 액세스 권한을 부여하는 역할이 생기게 됩니다. 또한 해당 역할을 사용할 수 있는 사용자가 속한 그룹이 하나 Development 계정에 생기게 됩니다. 이제 역할을 사용할 준비가 되었습니다. 이 단계에서는 AWS Management 콘솔, AWS CLI 및 AWS API에서 해당 역할로 전환을 테스트하는 방법을 설명합니다.

> Important
>
> IAM 사용자 또는 연합된 사용자로 로그인할 때만 역할을 전환할 수 있습니다. 또한 Amazon EC2 인스턴스를 시작하여 애플리케이션을 실행하는 경우 애플리케이션은 인스턴스 프로파일을 통해 역할을 부여할 수 있습니다. AWS 계정 루트 사용자로 로그인되어 있을 때는 역할을 바꿀 수 없습니다.

역할 전환(콘솔)

David가 AWS Management 콘솔의 Production 환경에서 작업해야 할 경우 Switch Role(역할 전환)을 사용하면 됩니다. David가 계정 ID나 별칭 및 역할 이름을 지정하면 David의 권한이 해당 역할에 허용되는 권한으로 즉시 전환됩니다. 그런 다음 David는 콘솔을 사용하여 `productionapp` 버킷으로 작업할 수 있지만 Production의 다른 리소스로는 작업할 수 없습니다. David가 이 역할을 사용하는 동안에는 Development 계정에서 파워 유저 권한도 사용할 수 없습니다. 한 번에 하나의 권한 집합만 적용할 수 있기 때문입니다.

> Important
>
> AWS Management 콘솔을 사용하여 역할을 전환하려면 계정에서 `ExternalId`를 요구하지 않아야 합니다. 예를 들어, 계정에 대한 액세스 권한을 제3자에게 부여하고 권한 정책의 `Condition` 요소에 `ExternalId`가 필요하다고 가정합니다. 이 경우 제3자는 AWS API 또는 명령줄 도구를 사용해야만 계정에 액세스할 수 있습니다. 콘솔은 `ExternalId`에 대한 값을 제공할 수 없기 때문에 사용할 수 없습니다. 이 시나리오에 대한 자세한 정보는 AWS 리소스에 대한 액세스를 타사에 부여할 때

외부 ID를 사용하는 방법 (p. 229)와 AWS Management 콘솔 보안 블로그의 AWS에 대한 교차 계정 액세스를 가능하게 하는 방법을 참조하십시오.

David는 다음과 같은 두 가지 방법으로 Switch Role(역할 전환) 페이지를 시작할 수 있습니다.

- David가 관리자로부터 미리 정의된 [Switch Role] 구성을 가리키는 링크를 받습니다. 이 링크는 역할 생성 마법사의 마지막 페이지 또는 교차 계정 역할의 Role Summary(역할 요약) 페이지에서 관리자에게 제공됩니다. 이 링크를 선택하면 계정 ID 및 역할 이름 필드에 이미 정보가 채워진 Switch Role(역할 전환) 페이지가 David에게 표시됩니다. David는 Switch Role(역할 전환) 버튼을 선택하기만 하면 됩니다.
- 관리자가 이메일로 링크를 보내는 대신 계정 ID 번호 및 역할 이름 값을 보냅니다. David는 역할을 전환하기 위해 수동으로 이 정보를 입력해야 합니다. 다음 절차에 이 내용이 잘 설명되어 있습니다.

역할을 위임하려면

1. David가 Development 그룹에 있는 일반 사용자로 AWS Management 콘솔 콘솔에 로그인합니다.
2. 그는 관리자가 이메일로 보내준 링크를 선택합니다. 계정 ID나 별칭 및 역할 이름 정보가 이미 채워진 Switch Role(역할 전환) 페이지가 David에게 표시됩니다.

   —또는—

   그는 탐색 모음에서 자신의 이름(자격 증명 메뉴)을 선택한 후 Switch Role(역할 전환)을 선택합니다.

   David가 이 방법으로 처음 Switch Role(역할 전환) 페이지 액세스를 시도하는 것이라면 첫 실행 Switch Role(역할 전환) 페이지가 표시됩니다. 이 페이지에는 역할 전환을 통해 사용자가 여러 AWS 계정의 리소스를 관리할 수 있는 방법에 대한 추가 정보가 제공됩니다. 이 절차의 나머지 부분을 완료하려면 David가 이 페이지에서 Switch Role(역할 전환) 버튼을 선택해야 합니다.
3. 다음으로, 해당 역할에 액세스하기 위해 David는 수동으로 Production 계정 ID 번호(`999999999999`)와 역할 이름(`UpdateApp`)을 입력해야 합니다.

   또한 David는 현재 활성 상태인 역할(및 관련 권한)을 모니터링하려고 합니다. 이 정보를 추적하려면 표시 이름 텍스트 상자에 `PRODUCTION`을 입력하고 빨간색 옵션을 선택한 다음 Switch Role(역할 전환)을 선택합니다.
4. 이제 David는 Amazon S3 콘솔을 사용하여 Amazon S3 버킷으로 작업하거나 `UpdateApp` 역할에 권한이 있는 다른 모든 리소스로 작업할 수 있습니다.
5. David는 해야 할 일을 마친 뒤 원래의 권한으로 돌아갈 수 있습니다. 이를 위해 그는 탐색 모음에서 프로덕션이라고 표시된 역할 이름을 선택하고 Back to David @ 111111111111(David @ 111111111111로 돌아가기)을 선택합니다.
6. 다음에 David가 역할을 전환하려고 탐색 모음에서 자격 증명 메뉴를 선택하면 지난 번에 사용한 PRODUCTION 항목이 표시되는 것을 볼 수 있습니다. 계정 ID와 역할 이름을 다시 입력할 필요 없이 해당 항목을 선택하기만 하면 즉시 역할이 전환됩니다.

역할 전환(AWS CLI)

David가 명령줄에서 프로덕션 환경으로 작업해야 할 경우 AWS CLI를 사용하면 됩니다. David는 `aws sts assume-role` 명령을 실행하고 역할 ARN을 전달하여 해당 역할에 대한 임시 보안 자격 증명을 얻습니다. 그런 다음 후속 AWS CLI 명령이 해당 역할의 권한을 사용하여 작동하도록 환경 변수에서 해당 자격 증명을 구성합니다. David가 이 역할을 사용하는 동안에는 Development 계정에서 파워 유저 권한을 사용할 수 없습니다. 한 번에 한 가지 권한 세트만 적용될 수 있기 때문입니다.

모든 액세스 키와 토큰은 예제일 뿐이며 표시된 대로 사용할 수 없습니다. 라이브 환경의 적절한 값으로 바꾸십시오.

역할을 위임하려면

1. David가 명령 프롬프트 창을 열고 다음 명령을 실행하여 AWS CLI 클라이언트가 작동하는지 확인합니다.

```
aws help
```

Note

David의 기본 환경에는 `David` 명령으로 만든 기본 프로필의 `aws configure` 사용자 자격 증명이 사용됩니다. 자세한 내용은 AWS Command Line Interface 사용 설명서의 AWS Command Line Interface 구성을 참조하십시오.

2. David가 Production 계정의 `UpdateApp` 역할로 전환하기 위해 다음 명령을 실행하여 역할 전환 프로세스를 시작합니다. David는 해당 역할을 만든 관리자에게서 역할 ARN을 받았습니다. 이 명령을 실행하려면 세션 이름도 제공해야 합니다. 원하는 아무 텍스트나 선택할 수 있습니다.

```
aws sts assume-role --role-arn "arn:aws:iam::999999999999:role/UpdateApp" --role-
session-name "David-ProdUpdate"
```

다음 내용이 출력됩니다.

```
{
    "Credentials": {
        "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
        "SessionToken": "AQoDYXdzEGcaEXAMPLE2gsYULo
+Im5ZEXAMPLEeYjs1M2FUIgIJx9tQqNMBEXAMPLE
CvSRyh0FW7jEXAMPLEW+vE/7s1HRpXviG7b+qYf4nD00EXAMPLEmj4wxS04L/
uZEXAMPLECihzFB5lTYLto9dyBgSDy
EXAMPLE9/
g7QRUhZp4bqbEXAMPLENwGPyOj59pFA4lNKCIkVgkREXAMPLEjlzxQ7y52gekeVEXAMPLEDiB9ST3Uuysg
sKdEXAMPLE1TVastU1A0SKFEXAMPLEiywCC/Cs8EXAMPLEpZgOs+6hz4AP4KEXAMPLERbASP
+4eZScEXAMPLEsnf87e
NhyDHq6ikBQ==",
        "Expiration": "2014-12-11T23:08:07Z",
        "AccessKeyId": "AKIAIOSFODNN7EXAMPLE"
    }
}
```

3. 출력의 [Credentials] 섹션에 David에게 필요한 세 가지 항목이 표시됩니다.

   - `AccessKeyId`
   - `SecretAccessKey`
   - `SessionToken`

David는 후속 호출 시 이러한 파라미터를 사용하도록 AWS CLI 환경을 구성해야 합니다. 자격 증명을 구성하는 다양한 방법에 대한 자세한 정보는 AWS Command Line Interface 구성을 참조하십시오. `aws configure` 명령은 세션 토큰 캡처를 지원하지 않기 때문에 사용할 수 없습니다. 하지만 구성 파일에 정보를 수동으로 입력할 수 있습니다. 이는 비교적 만료 시간이 짧은 임시 자격 증명이기 때문에 현재 명령 줄 세션의 환경에 추가하는 것이 가장 쉽습니다.

4. 세 값을 환경에 추가하기 위해 David는 이전 단계의 출력을 잘라내어 다음 명령에 붙여 넣습니다. 세션 토큰 출력의 줄 바꿈 문제를 해결하기 위해 간단한 텍스트 편집기에서 텍스트 출력을 잘라내어 붙여 넣을 수 있습니다. 여기서는 명확성을 위해 줄을 바꾸어 표시했지만 긴 문자열 하나로 추가해야 합니다.

Note

다음 예제는 Windows 환경에 표시된 명령을 나타내며, 여기서 "set"은 환경 변수를 생성하라는 명령입니다. Linux 또는 macOS 컴퓨터에서는 "export" 명령을 대신 사용할 수 있습니다. 예제의 나머지 부분은 세 환경에서 모두 유효합니다.

```
set AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
set AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

```
set AWS_SESSION_TOKEN=AQoDYXdzEGcaEXAMPLE2gsYULo
+Im5ZEXAMPLEeYjs1M2FUIgIJx9tQqNMBEXAMPLECvS
Ryh0FW7jEXAMPLEW+vE/7s1HRpXviG7b+qYf4nD00EXAMPLEmj4wxS04L/
uZEXAMPLECihzFB5lTYLto9dyBgSDyEXA
MPLEKEY9/
g7QRUhZp4bqbEXAMPLENwGPyOj59pFA4lNKCIkVgkREXAMPLEjlzxQ7y52gekeVEXAMPLEDiB9ST3UusKd
EXAMPLE1TVastU1A0SKFEXAMPLEiywCC/Cs8EXAMPLEpZgOs+6hz4AP4KEXAMPLERbASP
+4eZScEXAMPLENhykxiHen
DHq6ikBQ==
```

이 시점에서 모든 후속 명령은 해당 자격 증명으로 식별되는 역할의 권한에 따라 실행됩니다. David의 경우 `UpdateApp` 역할입니다.

5. 명령을 실행하여 Production 계정의 리소스에 액세스합니다. 이 예제에서 David는 단순히 다음 명령을 사용하여 S3 버킷의 콘텐츠를 나열합니다.

```
aws s3 ls s3://productionapp
```

Amazon S3 버킷 이름은 범용 고유 이름이기 때문에 해당 버킷을 소유하는 계정 ID를 지정할 필요가 없습니다. 다른 AWS 서비스의 리소스에 액세스하려면 해당 서비스의 AWS CLI 설명서에서 해당 리소스를 참조하는 데 필요한 명령과 구문을 참조하십시오.

AssumeRole(AWS API)사용

David가 코드에서 Production 계정을 업데이트해야 하는 경우 `AssumeRole`을 호출하여 `UpdateApp` 역할을 맡습니다. 이 호출로 인해 Production 계정에서 David가 `productionapp` 버킷에 액세스하기 위해 사용할 수 있는 임시 자격 증명이 반환됩니다. David는 해당 자격 증명을 사용하여 `productionapp` 버킷을 업데이트하는 API 호출을 실행할 수 있습니다. 그러나 David는 Development 계정의 파워 유저 권한이 있더라도 Production 계정의 다른 리소스에 액세스하는 API 호출을 실행할 수 없습니다.

역할을 위임하려면

1. David가 애플리케이션의 일부로 `AssumeRole`을 호출합니다. David는 `UpdateApp` ARN: `arn:aws:iam::999999999999:role/UpdateApp`를 지정해야 합니다.

   `AssumeRole` 호출의 응답에는 `AccessKeyId` 및 `SecretAccessKey`가 있는 임시 자격 증명이 포함됩니다. 또한 자격 증명이 만료되고 새 자격 증명을 요청해야 하는 시점을 나타내는 `Expiration` 시간이 포함됩니다.
2. David가 임시 자격 증명을 사용하여 `s3:PutObject` 버킷을 업데이트하는 `productionapp` 호출을 실행합니다. 이때 자격 증명을 `AuthParams` 파라미터로 API 호출에 전달합니다. 임시 역할 자격 증명에는 `productionapp` 버킷에 대한 읽기 및 쓰기 권한만 있기 때문에 Production 계정의 다른 모든 작업은 거부됩니다.

코드 샘플(Python 사용)은 IAM 역할(AWS API)로 전환하기 (p. 263) 단원을 참조하십시오.

관련 리소스

- IAM 사용자 및 그룹에 대한 자세한 정보는 자격 증명(사용자, 그룹, 및 역할) (p. 83) 단원을 참조하십시오.
- Amazon S3 버킷 생성에 대한 자세한 정보는 Amazon Simple Storage Service 시작 안내서에서 버킷 생성 단원을 참조하십시오.
- 해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

요약

교차 계정 API 액세스 자습서를 완료했습니다. 다른 계정과 신뢰 관계를 설정하기 위한 역할을 만들고 신뢰할 수 있는 주체가 수행할 수 있는 작업을 정의했습니다. 그런 다음 해당 역할에 액세스할 수 있는 IAM 사용자를 제어하는 그룹 정책을 수정했습니다. 그 결과 Development 계정의 개발자가 임시 자격 증명을 사용하여 Production 계정에서 `productionapp` 버킷을 업데이트할 수 있습니다.

자습서: 첫 번째 고객 관리형 정책 만들기 및 연결

이 자습서에서는 AWS Management 콘솔을 사용하여 고객 관리형 정책 (p. 359)을 만든 다음 이 정책을 IAM 계정의 AWS 사용자에게 연결합니다. 여기서 생성하는 정책은 IAM 테스트 사용자가 읽기 전용 권한으로 AWS Management 콘솔에 직접 로그인할 수 있도록 허용합니다.

이 워크플로우는 세 가지 기본 단계로 이루어집니다.

1단계: 정책 만들기 (p. 39)

기본적으로 IAM 사용자에게는 아무런 권한이 없습니다. 관리자가 허용하지 않는 한, 이들 사용자가 AWS Management Console에 액세스하거나 그 안에서 데이터를 관리할 수 없습니다. 이 단계에서는 연결된 사용자가 콘솔에 로그인할 수 있도록 허용하는 고객 관리형 정책을 생성합니다.

2단계: 정책 연결 (p. 40)

정책을 사용자에 연결할 경우 이 사용자는 해당 정책과 관련된 액세스 권한을 모두 상속받습니다. 이 단계에서는 새 정책을 테스트 사용자 계정에 연결합니다.

3단계: 사용자 액세스 테스트 (p. 40)

정책을 연결하고 나면 해당 사용자로 로그인하여 정책을 테스트할 수 있습니다.

사전 조건

이 자습서의 단계를 수행하려면 다음이 준비되어 있어야 합니다.

- 관리 권한을 가진 IAM 사용자로 로그인할 수 있는 AWS 계정.
- 다음과 같이 할당된 권한 또는 그룹 멤버십이 없는 테스트 IAM 사용자.

사용자 이름	그룹	권한
PolicyUser	<없음>	<없음>

1단계: 정책 만들기

이 단계에서는 연결된 사용자가 IAM 데이터에 대한 읽기 전용 권한으로 AWS Management 콘솔에 로그인할 수 있도록 허용하는 고객 관리형 정책을 생성합니다.

테스트 사용자에 대한 정책을 생성하려면

1. https://console.aws.amazon.com/iam/에서 관리자 권한을 가진 사용자로 IAM 콘솔에 로그인합니다.
2. 탐색 창에서 정책을 선택합니다.
3. 콘텐츠 창에서 정책 생성을 선택합니다.
4. JSON 탭을 선택하고 다음 JSON 정책 문서에서 텍스트를 복사합니다. 이 텍스트를 JSON 텍스트 상자에 붙여 넣습니다.

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

5. 작업이 완료되면 [Review policy]를 선택합니다. 정책 검사기 (p. 441)가 모든 구문 오류를 보고합니다.

   Note

   언제든지 Visual editor(시각적 편집기) 탭과 JSON 탭 간을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 정책 재구성 (p. 538) 단원을 참조하십시오.
6. 검토 페이지에서 정책 이름에 **`UsersReadOnlyAccessToIAMConsole`**을 입력합니다. 정책 요약을 검토하여 정책이 부여한 권한을 확인한 다음 정책 생성을 선택하여 작업을 저장합니다.

   새로운 정책이 관리형 정책 목록에 나타나며 연결 준비가 완료됩니다.

2단계: 정책 연결

다음에는 방금 생성한 테스트 IAM 사용자에 정책을 연결합니다.

테스트 사용자에 정책을 연결하려면

1. IAM 콘솔의 탐색 창에서 정책을 선택합니다.
2. 정책 목록의 맨 위에 있는 검색 상자에서 해당 정책이 표시될 때까지 **`UsersReadOnlyAccesstoIAMConsole`** 입력을 시작합니다. 그런 다음 목록에서 UsersReadOnlyAccessToIAMConsole 옆에 있는 확인란을 선택합니다.
3. Policy actions(정책 작업) 버튼을 선택한 후 연결을 선택합니다.
4. 필터에서 사용자를 선택합니다.
5. 검색 상자에서 해당 사용자가 목록에 표시될 때까지 **`PolicyUser`** 입력을 시작합니다. 그런 다음 목록에서 해당 사용자 옆의 확인란을 선택합니다.
6. Attach Policy(정책 연결)를 선택합니다.

이제 IAM 테스트 사용자에 정책을 연결했습니다. 즉, 이 사용자가 IAM 콘솔에 읽기 전용으로 액세스할 수 있습니다.

3단계: 사용자 액세스 테스트

이 자습서에서는 사용자가 어떤 경험을 하게 되는지 볼 수 있도록 테스트 사용자로 로그인하여 액세스를 테스트할 것을 권장합니다.

테스트 사용자 계정으로 로그인하여 액세스 권한을 테스트하려면

1. `PolicyUser` 테스트 사용자로 https://console.aws.amazon.com/에 있는 IAM 콘솔에 로그인합니다.
2. 콘솔에서 각 페이지를 탐색하고 새 사용자 또는 그룹을 생성해 봅니다. `PolicyUser`는 데이터를 표시할 수는 있지만 IAM 데이터를 생성하거나 수정할 수는 없습니다.

관련 리소스

IAM 사용 설명서에 수록된 관련 내용은 다음 리소스를 참조하십시오.

- 관리형 정책과 인라인 정책 (p. 357)
- AWS Management 콘솔에 대한 사용자 액세스 제어 (p. 76)
- 개별 IAM 사용자 만들기 (p. 61)

요약

이제 고객 관리형 정책을 생성 및 연결하는 데 필요한 모든 단계를 성공적으로 완료했습니다. 테스트 계정으로 IAM 콘솔에 로그인하여 사용자의 환경을 확인할 수 있습니다.

자습서: AWS에서 속성 기반 액세스 제어에 태그 사용

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 보안 주체 (사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. 그런 다음 태그 조건 키를 사용하여 해당 태그를 기반으로 보안 주체에 권한을 부여하는 정책을 정의할 수 있습니다. 태그를 사용하여 AWS 리소스에 대한 액세스를 제어하면 AWS 정책에 대한 변경 사항이 줄어들면서 팀과 리소스가 성장할 수 있습니다. ABAC 정책은 각 개별 리소스를 나열해야 하는 기존 AWS 정책보다 유연합니다. ABAC에 대한 자세한 내용 및 기존 정책과 비교할 때의 이점은 AWS용 ABAC란 무엇입니까? (p. 12) 단원을 참조하십시오.

주제

- 자습서 개요 (p. 41)
- 사전 조건 (p. 42)
- 1단계: 테스트 사용자 생성 (p. 43)
- 2단계: ABAC 정책 생성 (p. 44)
- 3단계: 역할 생성 (p. 46)
- 4단계: 비밀 생성 테스트 (p. 47)
- 5단계: 비밀 확인 테스트 (p. 49)
- 6단계: 테스트 확장성 (p. 50)
- 7단계: 비밀 업데이트 및 삭제 테스트 (p. 51)
- 요약 (p. 52)
- 관련 리소스 (p. 52)
- ABAC에 SAML 세션 태그 사용 (p. 53)

자습서 개요

이 자습서에서는 보안 주체 태그가 있는 IAM 역할이 일치하는 태그가 있는 리소스에 액세스할 수 있도록 허용하는 정책을 생성하고 테스트하는 방법을 보여 줍니다. 보안 주체가 AWS에 요청하면 보안 주체와 리소스 태그가 일치하는지 여부에 따라 권한이 부여됩니다. 이 전략을 통해 개인이 자신의 작업에 필요한 AWS 리소스만 보거나 편집할 수 있습니다.

시나리오

Example Corporation이라는 대기업의 수석 개발자이자 숙련된 IAM 관리자가 있다고 가정해 보겠습니다. 이 관리자는 IAM 사용자, 역할 및 정책을 생성하고 관리하는 데 익숙합니다. 개발 엔지니어와 품질 보증 팀 멤버가 필요한 리소스에 액세스할 수 있도록 해야 하며 기업의 성장에 따라 확장 가능한 전략도 준비해야 합니다.

AWS 리소스 태그와 IAM 역할 보안 주체 태그를 사용하여 이를 지원하는 서비스에 대한 ABAC 전략을 구현하도록 선택합니다(AWS Secrets Manager로 시작). 태그를 기반으로 권한 부여를 지원하는 서비스에 대한 자세한 내용은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 각 서비스의 작업 및 리소스와 함께 정책에서 사용할 수 있는 태그 지정 조건 키에 대한 자세한 내용은 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오. 세션 태그 (p. 294)를 AWS에 전달하도록 SAML 기반 또는 웹 자격 증명 공급자를 구성할 수 있습니다. 직원이 AWS에 연동되면 해당 속성이 AWS의 결과 보안 주체에 적용됩니다. 그런 다음 ABAC를 사용하여 이러한 속성에 따라 권한을 허용하거나 거부할 수 있습니다. SAML 연동 자격 증명과 함께 세션 태그를 사용하는 것이 이 자습서와 어떻게 다른지 알아보려면 ABAC에 SAML 세션 태그 사용 (p. 53) 단원을 참조하십시오.

엔지니어링 및 품질 보증 팀 멤버는 Pegasus 또는 Unicorn 프로젝트에 참여하고 있습니다. 다음 세 글자로 된 프로젝트 및 팀 태그 값을 선택합니다.

- Pegasus 프로젝트에 대해 `access-project` = `peg`
- Unicorn 프로젝트에 대해 `access-project` = `uni`
- 엔지니어링 팀에 대해 `access-team` = `eng`
- 품질 보증 팀에 대해 `access-team` = `qas`

또한 사용자 지정 AWS 결제 보고서를 활성화할 때 `cost-center` 비용 할당 태그가 필요하도록 선택할 수 있습니다. 자세한 내용은 AWS Billing and Cost Management 사용 설명서의 비용 할당 태그 사용을 참조하십시오.

주요 의사 결정 요약

- 직원은 IAM 사용자 자격 증명으로 로그인한 다음 팀 및 프로젝트의 IAM 역할을 맡습니다. 회사에 자체 자격 증명 시스템이 있는 경우 직원이 IAM 사용자 없이 역할을 맡을 수 있도록 연동을 설정할 수 있습니다. 자세한 내용은 ABAC에 SAML 세션 태그 사용 (p. 53) 단원을 참조하십시오.
- 동일한 정책이 모든 역할에 연결됩니다. 작업은 태그에 따라 허용되거나 거부됩니다.
- 직원은 자신의 역할에 적용되는 리소스에 동일한 태그를 연결하는 경우에만 새 리소스를 생성할 수 있습니다. 이렇게 하면 직원이 리소스를 생성한 후 해당 리소스를 볼 수 있습니다. 관리자는 더 이상 새 리소스의 ARN으로 정책을 업데이트할 필요가 없습니다.
- 직원은 프로젝트에 관계없이 자신의 팀이 소유한 리소스를 읽을 수 있습니다.
- 직원은 자신의 팀과 프로젝트가 소유한 리소스를 업데이트하고 삭제할 수 있습니다.
- IAM 관리자는 새 프로젝트에 대한 새 역할을 추가할 수 있습니다. 해당 역할에 대한 액세스를 허용하도록 새 IAM 사용자를 생성하고 태그를 지정할 수 있습니다. 관리자는 새 프로젝트 또는 팀 멤버를 지원하기 위해 정책을 편집할 필요가 없습니다.

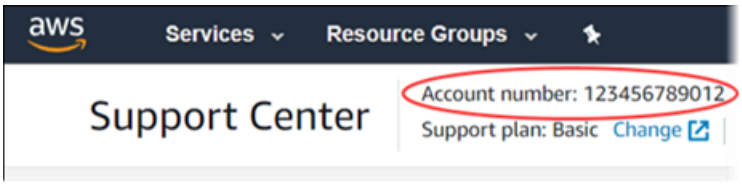
이 자습서에서는 각 리소스에 태그를 지정하고 프로젝트 역할에 태그를 지정하고 역할에 정책을 추가하여 앞에서 설명한 동작을 허용합니다. 결과 정책은 동일한 프로젝트 및 팀 태그로 태그가 지정된 리소스에 대한 역할 `Create`, `Read`, `Update` 및 `Delete` 액세스를 허용합니다. 또한 이 정책은 동일한 팀으로 태그가 지정된 리소스에 대해 프로젝트 간 `Read` 액세스를 허용합니다.

사전 조건

이 자습서의 단계를 수행하려면 다음이 준비되어 있어야 합니다.

- 관리 권한을 가진 IAM 사용자로 로그인할 수 있는 AWS 계정. 새 계정이 있고 AWS 계정 루트 사용자로 로그인하는 경우 IAM 관리자 사용자를 생성합니다 (p. 20).
- 3단계에서 역할을 생성하는 데 사용한 12자리 계정 ID입니다.

AWS Management 콘솔에서 AWS 계정 ID 번호를 검색하려면 오른쪽 상단에 있는 탐색 모음에서 지원을 선택한 후 지원 센터를 선택합니다. 현재 로그인한 계정 번호(ID)는 지원 센터 제목 표시줄에 나타납니다.



- AWS Management 콘솔에서 IAM 사용자, 역할 및 정책을 생성 및 편집해 본 경험. 그러나 IAM 관리 프로세스를 기억해야 하는 경우를 위해 이 자습서에서는 단계별 지침을 볼 수 있는 링크를 제공합니다.

1단계: 테스트 사용자 생성

테스트를 위해 동일한 태그를 사용하여 역할을 맡을 권한이 있는 IAM 사용자 4명을 생성합니다. 이렇게 하면 팀에 사용자를 더 쉽게 추가할 수 있습니다. 사용자에게 태그를 지정하면 올바른 역할을 맡을 수 있는 액세스 권한이 자동으로 부여됩니다. 사용자가 하나의 프로젝트와 팀에서만 작업하는 경우 역할의 신뢰 정책에 사용자를 추가할 필요가 없습니다.

1. 다음과 같이 `access-assume-role`이라는 고객 관리형 정책을 생성합니다. JSON 정책 생성에 대한 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 단원을 참조하십시오.

   ABAC 정책: 사용자 및 역할 태그가 일치하는 경우에만 모든 ABAC 역할 수임

   다음 정책은 사용자가 `access-` 이름 접두사가 있는 계정의 모든 역할을 맡을 수 있도록 허용합니다. 역할에는 사용자와 동일한 프로젝트, 팀 및 비용 센터 태그가 지정되어 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TutorialAssumeRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::123456789012:role/access-*",
            "Condition": {
                "StringEquals": {
                    "iam:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "iam:ResourceTag/access-team": "${aws:PrincipalTag/access-team}",
                    "iam:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"
                }
            }
        }
    ]
}
```

   이 자습서를 많은 사용자로 확장하기 위해 정책을 그룹에 연결하고 각 사용자를 그룹에 추가할 수 있습니다. 자세한 내용은 IAM 그룹 생성 (p. 168) 및 IAM 그룹에서 사용자 추가 및 제거 (p. 170) 단원을 참조하십시오.

2. 다음 IAM 사용자를 생성하고 `access-assume-role` 권한 정책을 연결하고 다음 태그를 추가합니다. 새 사용자 생성 및 태그 지정에 대한 자세한 내용은 IAM 사용자 생성(콘솔) (p. 88) 단원을 참조하십시오.

ABAC 사용자

사용자 이름	사용자 태그
access-Arnav-peg-eng	access-project = peg access-team = eng cost-center = 987654
access-Mary-peg-qas	access-project = peg access-team = qas cost-center = 987654
access-Saanvi-uni-eng	access-project = uni access-team = eng cost-center = 123456
access-Carlos-uni-qas	access-project = uni access-team = qas cost-center = 123456

2단계: ABAC 정책 생성

다음과 같이 **access-same-project-team**이라는 정책을 생성합니다. 이후 단계에서 이 정책을 역할에 추가합니다. JSON 정책 생성에 대한 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 단원을 참조하십시오.

이 자습서에 적용할 수 있는 추가 정책은 다음 페이지를 참조하십시오.

- IAM 보안 주체에 대한 액세스 제어 (p. 383)
- Amazon EC2: 프로그래밍 방식으로 콘솔에서 사용자가 태그를 지정한 EC2 인스턴스를 시작 또는 중지할 수 있도록 허용 (p. 407)
- EC2: 일치하는 보안 주체 및 리소스 태그를 기반으로 인스턴스 시작 또는 중지 (p. 408)
- EC2: 태그를 기반으로 인스턴스 시작 또는 중지 (p. 408)
- IAM: 특정 태그가 있는 역할 수임 (p. 413)

ABAC 정책: 보안 주체 및 리소스 태그가 일치하는 경우에만 Secrets Manager 리소스 액세스

다음 정책은 보안 주체와 동일한 키-값 페어로 리소스에 태그가 지정된 경우에만 보안 주체가 리소스를 생성, 읽기, 편집 및 삭제할 수 있도록 허용합니다. 보안 주체가 리소스를 생성할 때 보안 주체의 태그와 일치하는 값을 가진 `access-project`, `access-team` 및 `cost-center` 태그를 추가해야 합니다. 이 정책에서는 선택 사항인 `Name` 또는 `OwnedBy` 태그를 추가할 수도 있습니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Sid": "AllActionsSecretsManagerSameProjectSameTeam",
         "Effect": "Allow",
```

```
        "Action": "secretsmanager:*",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
                "aws:ResourceTag/access-team": "${aws:PrincipalTag/access-team}",
                "aws:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"
            },
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "access-project",
                    "access-team",
                    "cost-center",
                    "Name",
                    "OwnedBy"
                ]
            },
            "StringEqualsIfExists": {
                "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
                "aws:RequestTag/access-team": "${aws:PrincipalTag/access-team}",
                "aws:RequestTag/cost-center": "${aws:PrincipalTag/cost-center}"
            }
        }
    },
    {
        "Sid": "AllResourcesSecretsManagerNoTags",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetRandomPassword",
            "secretsmanager:ListSecrets"
        ],
        "Resource": "*"
    },
    {
        "Sid": "ReadSecretsManagerSameTeam",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:Describe*",
            "secretsmanager:Get*",
            "secretsmanager:List*"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/access-team": "${aws:PrincipalTag/access-team}"
            }
        }
    },
    {
        "Sid": "DenyUntagSecretsManagerReservedTags",
        "Effect": "Deny",
        "Action": "secretsmanager:UntagResource",
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "aws:TagKeys": "access-*"
            }
        }
    },
    {
        "Sid": "DenyPermissionsManagement",
        "Effect": "Deny",
        "Action": "secretsmanager:*Policy",
        "Resource": "*"
    }
]
```

```
}
```

이 정책이 하는 일은 무엇입니까?

- `AllActionsSecretsManagerSameProjectSameTeam` 문은 리소스 태그가 보안 주체 태그와 일치하는 경우에만 모든 관련 리소스에 대해 이 서비스의 모든 작업을 허용합니다. 정책에 `"Action": "secretsmanager:*"`를 추가하면 Secrets Manager이 커질수록 정책도 커집니다. Secrets Manager에서 새 API 작업을 추가하는 경우 문에 해당 작업을 추가할 필요가 없습니다. 이 문은 세 가지 조건 블록을 사용하여 ABAC를 구현합니다. 세 블록 모두 true를 반환하는 경우에만 요청이 허용됩니다.
  - 지정된 태그 키가 리소스에 있고 해당 값이 보안 주체의 태그와 일치하는 경우 이 문의 첫 번째 조건 블록은 true를 반환합니다. 이 블록은 일치하지 않는 태그 또는 리소스 태그 지정을 지원하지 않는 작업에 대해 false를 반환합니다. 이 블록에서 허용되지 않는 작업에 대한 자세한 내용은 AWS Secrets Manager에 대한 작업, 리소스 및 조건 키를 참조하십시오 . 이 페이지에서는 비밀 리소스 유형에 대해 수행된 작업이 `secretsmanager:ResourceTag/tag-key` 조건 키를 지원한다는 것을 보여 줍니다. 일부 Secrets Manager 작업에서는 `GetRandomPassword` 및 `ListSecrets`를 포함하여 해당 해당 리소스 유형을 지원하지 않습니다. 이러한 작업을 허용하려면 추가 문을 생성해야 합니다.
  - 두 번째 조건 블록은 요청에 전달된 모든 태그 키가 지정된 목록에 포함된 경우 true를 반환합니다. 이 작업은 `StringEquals` 조건 연산자와 함께 `ForAllValues`를 사용하여 수행됩니다. 키 또는 키 세트의 일부가 전달되지 않으면 조건이 true를 반환합니다. 이 경우 요청에서 태그 전달을 허용하지 않는 `Get*` 작업을 사용할 수 있습니다. 요청자가 목록에 없는 태그 키를 포함하는 경우 조건은 false를 반환합니다. 요청에 전달되는 모든 태그 키가 이 목록의 멤버와 일치해야 합니다. 자세한 내용은 다수의 키와 값 사용 (p. 610) 단원을 참조하십시오.
  - 세 번째 조건 블록은 요청이 태그 전달을 지원하고, 세 개의 태그가 모두 존재하고, 보안 주체 태그 값과 일치하는 경우 true를 반환합니다. 요청이 태그 전달을 지원하지 않는 경우에도 이 블록은 true를 반환합니다. 그 이유는 조건 연산자의 `...IfExists` (p. 607) 때문입니다. 지원하는 작업 중에 전달된 태그가 없거나 태그 키 및 값이 일치하지 않으면 블록이 false를 반환합니다.
- `AllResourcesSecretsManagerNoTags` 문은 첫 번째 문에서 허용되지 않는 `GetRandomPassword` 및 `ListSecrets` 작업을 허용합니다.
- `ReadSecretsManagerSameTeam` 문은 보안 주체가 리소스와 동일한 액세스 팀 태그로 태그가 지정된 경우 읽기 전용 작업을 허용합니다. 이는 프로젝트 또는 비용 센터 태그에 관계없이 허용됩니다.
- `DenyUntagSecretsManagerReservedTags` 문은 Secrets Manager에서 “access-”로 시작하는 키가 있는 태그를 제거하라는 요청을 거부합니다. 이러한 태그는 리소스에 대한 액세스를 제어하는 데 사용되므로 태그를 제거하면 권한이 제거될 수 있습니다.
- `DenyPermissionsManagement` 문은 Secrets Manager 리소스 기반 정책을 생성, 편집 또는 삭제할 수 있는 권한을 거부합니다. 이러한 정책을 사용하여 비밀의 권한을 변경할 수 있습니다.

  Important

  이 정책은 전략을 사용하여 서비스에 대한 모든 작업을 허용하지만 권한 변경 작업을 명시적으로 거부합니다. 작업을 거부하면 보안 주체가 해당 작업을 수행할 수 있도록 허용하는 다른 정책을 재정의합니다. 이로 인해 의도하지 않은 결과가 발생할 수 있습니다. 명시적 거부는 해당 작업을 허용해야 하는 상황이 없는 경우에만 사용하는 것이 가장 좋습니다. 그렇지 않은 경우 개별 작업 목록을 허용하고 원치 않는 작업이 기본적으로 거부됩니다.

3단계: 역할 생성

다음 IAM 역할을 생성하고 이전 단계에서 생성한 **`access-same-project-team`** 정책을 연결합니다. IAM 역할 생성에 대한 자세한 내용은 역할을 만들어 IAM 사용자에게 권한 위임 (p. 226) 단원을 참조하십시오. IAM 사용자 및 역할 대신 연동을 사용하도록 선택한 경우 ABAC에 SAML 세션 태그 사용 (p. 53) 단원을 참조하십시오.

ABAC 역할

직무	역할 태그	역할 이름	역할 설명

프로젝트 Pegasus 엔지니어링	`access-project = peg`
	`access-team = eng`
	`cost-center = 987654`
		`access-peg-engineering`	엔지니어는 모든 엔지니어링 리소스를 읽고 Pegasus 엔지니어링 리소스를 생성 및 관리할 수 있습니다.

프로젝트 Pegasus 품질 보증	`access-project = peg`
	`access-team = qas`
	`cost-center = 987654`
		`access-peg-quality-assurance`	QA 팀은 모든 QA 리소스를 읽고 모든 Pegasus QA 리소스를 생성 및 관리할 수 있습니다.

프로젝트 Unicorn 엔지니어링	`access-project = uni`
	`access-team = eng`
	`cost-center = 123456`
		`access-uni-engineering`	엔지니어는 모든 엔지니어링 리소스를 읽고 Unicorn 엔지니어링 리소스를 생성 및 관리할 수 있습니다.

프로젝트 Unicorn 품질 보증	`access-project = uni`
	`access-team = qas`
	`cost-center = 123456`
		`access-uni-quality-assurance`	QA 팀은 모든 QA 리소스를 읽고 모든 Unicorn QA 리소스를 생성 및 관리할 수 있습니다.

4단계: 비밀 생성 테스트

역할에 연결된 권한 정책을 통해 직원이 비밀을 생성할 수 있습니다. 이 작업은 비밀에 프로젝트, 팀 및 비용 센터 태그가 지정된 경우에만 허용됩니다. Secrets Manager에서 사용자로 로그인하고, 올바른 역할을 맡고, 활동을 테스트하여 권한이 예상대로 작동하는지 확인합니다.

필수 태그를 사용하거나 사용하지 않고 비밀 생성을 테스트하려면

1. 기본 브라우저 창에서 관리자 사용자로 로그인한 상태로 유지되므로 IAM에서 사용자, 역할 및 정책을 검토할 수 있습니다. 테스트를 위해 브라우저 익명 창 또는 별도의 브라우저를 사용하십시오. `access-Arnav-peg-eng`IAM 사용자로 로그인하고 https://console.aws.amazon.com/secretsmanager/에서 Secrets Manager 콘솔을 엽니다.
2. `access-uni-engineering` 역할로의 전환을 시도합니다. AWS Management 콘솔에서의 역할 전환에 대한 자세한 내용은 역할 전환(콘솔) (p. 256) 단원을 참조하십시오.

   사용자와 역할의 `access-team` 태그 값이 일치하지 않기 때문에 이 작업은 실패합니다.
3. `access-peg-engineering` 역할로 전환합니다. AWS Management 콘솔에서의 역할 전환에 대한 자세한 내용은 역할 전환(콘솔) (p. 256) 단원을 참조하십시오.
4. 다음 정보를 사용하여 새 비밀을 저장합니다. 비밀을 저장하는 방법에 대한 자세한 내용은 AWS Secrets Manager 사용 설명서의 기본 비밀 생성을 참조하십시오.

   1. 비밀 유형 선택 섹션에서 다른 유형의 비밀을 선택합니다. 두 텍스트 상자에 `test-access-key` 및 `test-access-secret`를 입력합니다.

      특정 AWS 서비스에 대한 자격 증명을 저장하려면 추가 권한이 있어야 합니다. 예를 들어, Amazon RDS 데이터베이스에 대한 자격 증명을 생성하려면 RDS 인스턴스, RDS 클러스터 및 Amazon Redshift 클러스터를 설명할 수 있는 권한이 있어야 합니다.
   2. 비밀 이름 필드에 `test-access-peg-eng`를 입력합니다.
   3. 다음 표에서 다양한 태그 조합을 추가하고 예상되는 동작을 확인합니다.

4. Store(저장)를 선택하여 비밀을 생성합니다. 스토리지에 장애가 발생하면 이전 Secrets Manager 콘솔 페이지로 돌아가서 아래 표에 있는 다음 태그 세트를 사용합니다. 마지막 태그 세트가 허용되고 비밀이 성공적으로 생성됩니다.

`test-access-peg-eng` 역할에 대한 ABAC 태그 조합

`access-project` 태그 값	**`access-team`** 태그 값	**`cost-center`** 태그 값	추가 태그	예상되는 동작
(none)	(none)	(none)	(none)	`access-project` 태그 값이 역할의 `peg` 값과 일치하지 않아 거부됩니다.
`uni`	`eng`	`987654`	(none)	`access-project` 태그 값이 역할의 `peg` 값과 일치하지 않아 거부됩니다.
`peg`	`qas`	`987654`	(none)	`access-team` 태그 값이 역할의 `eng` 값과 일치하지 않아 거부됩니다.
`peg`	`eng`	`123456`	(none)	`cost-center` 태그 값이 역할의 `987654` 값과 일치하지 않아 거부됩니다.
`peg`	`eng`	`987654`	`owner = Jane`	세 개의 필수 태그가 모두 있고 해당 값이 역할 값과 일치하지만 추가 태그 `owner`가 정책에서 허용되지 않아 거부됩니다.
`peg`	`eng`	`987654`	`Name = Jane`	세 개의 필수 태그가 모두 있고 해당 값이 역할 값과 일치하기 때문에 허용됩니다. 선택적으로 `Name` 태그를 포함할 수도 있습니다.

5. 로그아웃하고 다음 역할 및 태그 값 각각에 대해 이 절차의 처음 세 단계를 반복합니다. 이 절차의 네 번째 단계에서는 선택한 누락된 태그, 선택적 태그, 허용되지 않는 태그 및 잘못된 태그 값 세트를 테스트합니다. 그런 다음 필수 태그를 사용하여 다음 태그와 이름으로 비밀을 생성합니다.

ABAC 역할 및 태그

사용자 이름	역할 이름	비밀 이름	비밀 태그

`access-Mary-peg-qas`	`access-peg-quality-assurance`	`test-access-peg-qas`	`access-project = peg`
			`access-team = qas`
			`cost-center = 987654`

`access-Saanvi-uni-eng`	`access-uni-engineering`	`test-access-uni-eng`	`access-project = uni`
			`access-team = eng`
			`cost-center = 123456`

`access-Carlos-uni-qas`	`access-uni-quality-assurance`	`test-access-uni-qas`	`access-project = uni`

사용자 이름	역할 이름	비밀 이름	비밀 태그

			`access-team` = `qas`
			
			`cost-center` = `123456`

5단계: 비밀 확인 테스트

각 역할에 연결된 정책을 통해 직원은 프로젝트에 관계없이 팀 이름으로 태그가 지정된 모든 비밀을 볼 수 있습니다. Secrets Manager에서 역할을 테스트하여 권한이 예상대로 작동하는지 확인합니다.

필수 태그를 사용하거나 사용하지 않고 비밀 보기를 테스트하려면

1. 다음 IAM 사용자 중 한 명으로 로그인합니다.
   - `access-Arnav-peg-eng`
   - `access-Mary-peg-qas`
   - `access-Saanvi-uni-eng`
   - `access-Carlos-peg-qas`
2. 일치하는 역할로 전환합니다.
   - `access-peg-engineering`
   - `access-peg-quality-assurance`
   - `access-uni-engineering`
   - `access-peg-quality-assurance`

   AWS Management 콘솔에서의 역할 전환에 대한 자세한 내용은 역할 전환(콘솔) (p. 256) 단원을 참조하십시오.
3. 왼쪽의 탐색 창에서 메뉴 아이콘을 선택하여 메뉴를 확장한 다음 비밀을 선택합니다.
4. 현재 역할에 관계없이 표에 네 가지 비밀이 모두 표시됩니다. 이는 `access-same-project-team`이라는 정책이 모든 리소스에 대해 `secretsmanager:ListSecrets` 작업을 허용하기 때문입니다.
5. 비밀 중 하나의 이름을 선택합니다.
6. 비밀에 대한 세부 정보 페이지에서 역할의 태그에 따라 페이지 콘텐츠를 볼 수 있는지 여부가 결정됩니다. 역할의 이름을 비밀의 이름과 비교합니다. 동일한 팀 이름을 공유하는 경우 `access-team` 태그가 일치합니다. 일치하지 않으면 액세스가 거부됩니다.

   각 역할에 대한 ABAC 비밀 보기 동작

역할 이름	비밀 이름	예상되는 동작
`access-peg-engineering`	`test-access-peg-eng`	허용됨
	`test-access-peg-qas`	거부됨
	`test-access-uni-eng`	허용됨
	`test-access-uni-qas`	거부됨
`access-peg-quality-assurance`	`test-access-peg-eng`	거부됨
	`test-access-peg-qas`	허용됨

역할 이름	비밀 이름	예상되는 동작
	test-access-uni-eng	거부됨
	test-access-uni-qas	허용됨
access-uni-engineering	test-access-peg-eng	허용됨
	test-access-peg-qas	거부됨
	test-access-uni-eng	허용됨
	test-access-uni-qas	거부됨
access-peg-quality-assurance	test-access-peg-eng	거부됨
	test-access-peg-qas	허용됨
	test-access-uni-eng	거부됨
	test-access-uni-qas	허용됨

7. 페이지 상단의 이동 경로에서 비밀을 선택하여 비밀 목록으로 돌아갑니다. 다른 역할을 사용하여 이 절차의 단계를 반복하여 각 암호를 볼 수 있는지 여부를 테스트합니다.

6단계: 테스트 확장성

RBAC(역할 기반 액세스 제어)를 통해 ABAC(속성 기반 액세스 제어)를 사용하는 중요한 이유는 확장성입니다. 회사에서 새 프로젝트, 팀 또는 인력을 AWS에 추가할 때 ABAC 기반 정책을 업데이트할 필요가 없습니다. 예를 들어, Example Company가 코드명이 Centaur인 새로운 프로젝트에 자금을 조달하고 있다고 가정합니다. Saanvi Sarkar라는 엔지니어는 Unicorn 프로젝트에서 계속 작업하면서 Centaur의 수석 엔지니어도 겸할 예정입니다. 또한 Nikhil Jayashankar를 포함하여 Centaur 프로젝트에서만 작업하기 위해 몇 명의 엔지니어가 새로 고용되었습니다.

새 프로젝트를 AWS에 추가하려면

1. IAM 관리자 사용자로 로그인하고 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 역할을 선택한 후 `access-cen-engineering`이라는 IAM 역할을 추가합니다. 역할에 **`access-same-project-team`** 권한 정책을 연결하고 다음 태그를 추가합니다.
   - `access-project` = `cen`
   - `access-team` = `eng`
   - `cost-center` = `101010`
3. 왼쪽에 있는 탐색 창에서 Users(사용자)를 선택합니다.
4. `access-Nikhil-cen-eng`라는 새 사용자를 추가하고 `access-assume-role` 정책을 연결합니다.
5. 4단계: 비밀 생성 테스트 (p. 47) 및 5단계: 비밀 확인 테스트 (p. 49)의 절차를 사용합니다. 다른 브라우저 창에서 Nikhil이 Centaur 엔지니어링 비밀만 만들 수 있는지와 모든 엔지니어링 비밀을 볼 수 있는지를 테스트합니다.
6. 관리자로 로그인한 기본 브라우저 창에서 `access-Saanvi-uni-eng`를 선택합니다.
7. 권한 탭에서 access-assume-role 권한 정책을 제거합니다.
8. `access-assume-specific-roles`라는 다음 인라인 정책을 추가합니다. 인라인 정책을 사용자에게 추가하는 방법에 대한 자세한 내용은 사용자 또는 역할의 인라인 정책을 포함하려면(콘솔) (p. 452) 단원을 참조하십시오.

   ABAC 정책: 특정 역할만 수임

이 정책을 통해 Saanvi는 Pegasus 또는 Centaur 프로젝트의 엔지니어링 역할을 맡을 수 있습니다. IAM에서는 다중 값 태그를 지원하지 않으므로 이 사용자 지정 정책을 생성해야 합니다. Saanvi의 사용자에게 `access-project = peg` 및 `access-project = cen` 태그를 지정할 수 없습니다. 또한 AWS 권한 부여 모델은 두 값과 모두 일치할 수 없습니다. 자세한 내용은 IAM 및 AWS STS의 태그 지정 규칙 (p. 290) 단원을 참조하십시오. 대신 Saanvi가 맡을 수 있는 두 역할을 수동으로 지정해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TutorialAssumeSpecificRoles",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::123456789012:role/access-peg-engineering",
                "arn:aws:iam::123456789012:role/access-cen-engineering"
            ]
        }
    ]
}
```

9. 4단계: 비밀 생성 테스트 (p. 47) 및 5단계: 비밀 확인 테스트 (p. 49)의 절차를 사용합니다. 다른 브라우저 창에서 Saanvi가 두 역할을 모두 맡을 수 있는지 확인합니다. 역할의 태그에 따라 프로젝트, 팀 및 비용 센터에 대해서만 비밀을 생성할 수 있는지 확인합니다. 또한 Saanvi가 방금 생성한 비밀을 포함하여 엔지니어링 팀이 소유한 비밀에 대한 세부 정보를 볼 수 있는지 확인합니다.

7단계: 비밀 업데이트 및 삭제 테스트

역할에 연결된 `access-same-project-team` 정책을 통해 직원은 프로젝트, 팀 및 비용 센터로 태그가 지정된 모든 비밀을 업데이트하고 삭제할 수 있습니다. Secrets Manager에서 역할을 테스트하여 권한이 예상대로 작동하는지 확인합니다.

필수 태그를 사용하거나 사용하지 않고 비밀 업데이트 및 삭제를 테스트하려면

1. 다음 IAM 사용자 중 한 명으로 로그인합니다.
   - `access-Arnav-peg-eng`
   - `access-Mary-peg-qas`
   - `access-Saanvi-uni-eng`
   - `access-Carlos-peg-qas`
   - `access-Nikhil-cen-eng`
2. 일치하는 역할로 전환합니다.
   - `access-peg-engineering`
   - `access-peg-quality-assurance`
   - `access-uni-engineering`
   - `access-peg-quality-assurance`
   - `access-cen-engineering`

   AWS Management 콘솔에서의 역할 전환에 대한 자세한 내용은 역할 전환(콘솔) (p. 256) 단원을 참조하십시오.
3. 각 역할에 대해 비밀 설명을 업데이트하고 다음 비밀을 삭제해봅니다. 자세한 내용은 AWS Secrets Manager 사용 설명서의 비밀 수정 및 비밀 삭제 및 복원을 참조하십시오.

각 역할에 대한 ABAC 비밀 업데이트 및 삭제 동작

역할 이름	비밀 이름	예상되는 동작
access-peg-engineering	test-access-peg-eng	허용됨
	test-access-uni-eng	거부됨
	test-access-uni-qas	거부됨
access-peg-quality-assurance	test-access-peg-qas	허용됨
	test-access-uni-eng	거부됨
access-uni-engineering	test-access-uni-eng	허용됨
	test-access-uni-qas	거부됨
access-peg-quality-assurance	test-access-uni-qas	허용됨

요약

이제 속성 기반 액세스 제어(ABAC)에 태그를 사용하는 데 필요한 모든 단계를 성공적으로 완료했습니다. 태그 지정 전략을 정의하는 방법을 배웠습니다. 보안 주체와 리소스에 해당 전략을 적용했습니다. Secrets Manager에 대한 전략을 적용하는 정책을 생성하고 적용했습니다. 또한 새 프로젝트 및 팀 멤버를 추가할 때 ABAC가 쉽게 확장된다는 사실을 알게 되었습니다. 따라서 테스트 역할을 사용하여 IAM 콘솔에 로그인하고 AWS에서 ABAC에 대한 태그를 사용하는 방법을 경험할 수 있습니다.

Note

특정 조건에서만 작업을 허용하는 정책을 추가했습니다. 더 광범위한 권한을 가진 사용자 또는 역할에 다른 정책을 적용하는 경우, 작업에서 태그 지정이 필요하도록 제한을 받지 않을 수 있습니다. 예를 들어 `AdministratorAccess` AWS 관리형 정책을 사용하여 사용자에게 전체 관리 권한을 부여하는 경우, 이러한 정책은 해당 액세스를 제한하지 않습니다. 여러 정책이 적용될 때 권한이 결정되는 방법에 대한 자세한 내용은 계정 내에서 요청 허용 여부 결정 (p. 625) 단원을 참조하십시오.

관련 리소스

IAM 사용 설명서에 수록된 관련 내용은 다음 리소스를 참조하십시오.

- AWS용 ABAC란 무엇입니까? (p. 12)
- AWS 전역 조건 컨텍스트 키 (p. 650)
- 첫 번째 IAM 관리자 및 그룹 생성 (p. 20)
- IAM 사용자 생성(콘솔) (p. 88)
- 역할을 만들어 IAM 사용자에게 권한 위임 (p. 226)
- IAM 사용자 및 역할 태그 지정 (p. 290)
- 리소스 태그를 사용하여 AWS 리소스에 대한 액세스 제어 (p. 384)
- 역할 전환(콘솔) (p. 256)
- ABAC에 SAML 세션 태그 사용 (p. 53)

계정의 태그를 모니터링하는 방법을 알아보려면 서버리스 워크플로 및 Amazon CloudWatch Events를 사용하여 AWS에서 리소스 태그 변경 모니터링을 참조하십시오.

ABAC에 SAML 세션 태그 사용

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결 (p. 290)할 수 있습니다. 엔터티를 사용하여 AWS에 요청하면 해당 엔터티가 보안 주체가 되고 해당 보안 주체에 태그가 포함됩니다.

역할을 맡거나 사용자를 연동할 때 세션 태그 (p. 294)를 전달할 수도 있습니다. 그런 다음 태그 조건 키를 사용하여 해당 태그를 기반으로 보안 주체에 권한을 부여하는 정책을 정의할 수 있습니다. 태그를 사용하여 AWS 리소스에 대한 액세스를 제어하면 AWS 정책에 대한 변경 사항이 줄어들면서 팀과 리소스가 성장할 수 있습니다. ABAC 정책은 각 개별 리소스를 나열해야 하는 기존 AWS 정책보다 유연합니다. ABAC에 대한 자세한 내용 및 기존 정책과 비교할 때의 이점은 AWS용 ABAC란 무엇입니까? (p. 12) 단원을 참조하십시오.

회사에서 SAML 기반 자격 증명 공급자(IdP)를 사용하여 회사 사용자 자격 증명을 관리하는 경우 AWS에서 SAML 속성을 사용하여 세밀한 액세스 제어를 수행할 수 있습니다. 속성에는 비용 센터 식별자, 사용자 이메일 주소, 부서 분류 및 프로젝트 할당이 포함될 수 있습니다. 이러한 속성을 세션 태그로 전달하면 이러한 세션 태그를 기반으로 AWS에 대한 액세스를 제어할 수 있습니다.

세션 보안 주체에 SAML 속성을 전달하여 ABAC 자습서 (p. 41)를 완료하려면 이 주제에 포함된 변경 사항을 사용하여 자습서: AWS에서 속성 기반 액세스 제어에 태그 사용 (p. 41)의 작업을 완료합니다.

사전 조건

ABAC에 대해 SAML 세션 태그를 사용하는 단계를 수행하려면 다음 사항이 이미 있어야 합니다.

- 특정 속성을 가진 테스트 사용자를 생성할 수 있는 SAML 기반 IdP에 대한 액세스
- 관리 권한을 가진 IAM 사용자로 로그인할 수 있는 AWS 계정. 새 계정이 있고 AWS 계정 루트 사용자로 로그인하는 경우 IAM 관리자 사용자를 생성합니다 (p. 20).
- AWS Management 콘솔에서 IAM 사용자, 역할 및 정책을 생성 및 편집해 본 경험. 그러나 IAM 관리 프로세스를 기억해야 하는 경우를 위해 ABAC 자습서에서는 단계별 지침을 볼 수 있는 링크를 제공합니다.
- IAM에서 SAML 기반 IdP를 설정해 본 경험. 자세한 내용과 자세한 IAM 설명서에 대한 링크를 보려면 AssumeRoleWithSAML을 사용하여 세션 태그 전달 (p. 298) 단원을 참조하십시오.

1단계: 테스트 IAM 사용자 생성

1단계: 테스트 사용자 생성 (p. 43)의 지침을 건너뜁니다. 자격 증명은 공급자에 정의되어 있으므로 직원에 대한 IAM 사용자를 추가할 필요는 없습니다.

2단계: ABAC 정책 생성

2단계: ABAC 정책 생성 (p. 44)의 지침에 따라 IAM에서 지정된 관리형 정책을 생성합니다.

3단계: SAML 역할 생성 및 구성

SAML용 ABAC 자습서를 사용하는 경우 역할을 생성하고, SAML IdP를 구성하고, AWS Management 콘솔 액세스를 활성화하기 위한 추가 단계를 수행해야 합니다. 자세한 내용은 3단계: 역할 생성 (p. 46) 단원을 참조하십시오.

3A단계: SAML 역할 생성

SAML 자격 증명 공급자 및 1단계에서 생성한 `test-session-tags` 사용자를 신뢰하는 단일 역할을 생성합니다. ABAC 자습서에서는 역할 태그가 서로 다른 별도의 역할을 사용합니다. SAML IdP에서 세션 태그를

전달하기 때문에 역할은 하나만 필요합니다. SAML 기반 역할을 생성하는 방법은 SAML 2.0 연동을 위한 역할 생성(콘솔) (p. 244) 단원을 참조하십시오.

역할 이름을 `access-session-tags`로 지정합니다. 역할에 `access-same-project-team` 권한 정책을 연결합니다. 다음 정책을 사용하도록 역할 신뢰 정책을 편집합니다. 역할의 신뢰 관계를 편집하는 방법에 대한 자세한 지침은 역할 수정(콘솔) (p. 275) 단원을 참조하십시오.

다음 역할 신뢰 정책은 SAML 자격 증명 공급자 및 `test-session-tags` 사용자가 역할을 맡을 수 있도록 허용합니다. 역할을 맡을 때는 세 개의 지정된 세션 태그를 전달해야 합니다. 이 `sts:TagSession` 작업은 세션 태그 전달을 허용하는 데 필요합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSamlIdentityAssumeRole",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRoleWithSAML",
                "sts:TagSession"
            ],
            "Principal": {"Federated":"arn:aws:iam::123456789012:saml-
provider/ExampleCorpProvider"},
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/cost-center": "*",
                    "aws:RequestTag/access-project": "*",
                    "aws:RequestTag/access-team": [
                        "eng",
                        "qas"
                    ]
                },
                "StringEquals": {"SAML:aud": "https://signin.aws.amazon.com/saml"}
            }
        }
    ]
}
```

이 `AllowSamlIdentityAssumeRole` 문을 사용하면 엔지니어링 및 품질 보증 팀의 멤버가 Example Corporation IdP에서 AWS로 연동될 때 이 역할을 맡을 수 있습니다. `ExampleCorpProvider` SAML 공급자는 IAM에 정의되어 있습니다. 관리자가 세 개의 필수 세션 태그를 전달하도록 SAML 어설션을 이미 설정했습니다. 어설션에서 추가 태그를 전달할 수 있지만 이 세 가지 태그는 반드시 있어야 합니다. 자격 증명의 속성은 `cost-center` 및 `access-project` 태그에 대한 값을 가질 수 있습니다. 그러나 자격 증명이 엔지니어링 또는 품질 보증 팀에 속한다는 것을 나타내려면 `access-team` 속성 값이 `eng` 또는 `qas`와 일치해야 합니다.

3B단계: SAML IdP 구성

`cost-center`, `access-project` 및 `access-team` 속성을 세션 태그로 전달하도록 SAML IdP를 구성합니다. 자세한 내용은 AssumeRoleWithSAML을 사용하여 세션 태그 전달 (p. 298) 단원을 참조하십시오.

이러한 속성을 세션 태그로 전달하려면 SAML 어설션에 다음 요소를 포함합니다.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:cost-center">
  <AttributeValue>987654</AttributeValue>
</Attribute>
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:access-project">
  <AttributeValue>peg</AttributeValue>
</Attribute>
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:access-team">
  <AttributeValue>eng</AttributeValue>
</Attribute>
```

3B단계: 콘솔 액세스 활성화

연동 SAML 사용자에 대해 콘솔 액세스를 활성화합니다. 자세한 내용은 SAML 2.0 연동 사용자가 AWS Management 콘솔에 액세스할 수 있게 하기 (p. 208) 단원을 참조하십시오.

4단계: 비밀 생성 테스트

`access-session-tags` 역할을 사용하여 AWS Management 콘솔에 연동합니다. 자세한 내용은 SAML 2.0 연동 사용자가 AWS Management 콘솔에 액세스할 수 있게 하기 (p. 208) 단원을 참조하십시오. 그런 다음 4단계: 비밀 생성 테스트 (p. 47)의 지침에 따라 비밀을 생성합니다. 다양한 SAML 자격 증명을 속성과 함께 사용하여 ABAC 자습서에 표시된 태그와 일치시킵니다. 자세한 내용은 4단계: 비밀 생성 테스트 (p. 47) 단원을 참조하십시오.

5단계: 비밀 확인 테스트

5단계: 비밀 확인 테스트 (p. 49) 단원의 지침에 따라 이전 단계에서 생성한 비밀을 확인합니다. 다양한 SAML 자격 증명을 속성과 함께 사용하여 ABAC 자습서에 표시된 태그와 일치시킵니다.

6단계: 테스트 확장성

6단계: 테스트 확장성 (p. 50) 단원의 지침에 따라 확장성을 테스트합니다. 다음 속성을 사용하여 SAML 기반 IdP에 새 자격 증명을 추가하면 됩니다.

- `cost-center = 101010`
- `access-project = cen`
- `access-team = eng`

7단계: 비밀 업데이트 및 삭제 테스트

7단계: 비밀 업데이트 및 삭제 테스트 (p. 51) 단원의 지침에 따라 비밀을 업데이트 및 삭제합니다. 다양한 SAML 자격 증명을 속성과 함께 사용하여 ABAC 자습서에 표시된 태그와 일치시킵니다.

> **Important**
>
> 요금이 청구되지 않도록 생성한 모든 비밀을 삭제합니다. Secrets Manager의 요금에 대한 자세한 내용은 AWS Secrets Manager 요금을 참조하십시오.

요약

이제 권한 관리를 위해 SAML 세션 태그 및 리소스 태그를 사용하는 데 필요한 모든 단계를 성공적으로 완료했습니다.

> **Note**
>
> 특정 조건에서만 작업을 허용하는 정책을 추가했습니다. 더 광범위한 권한을 가진 사용자 또는 역할에 다른 정책을 적용하는 경우, 작업에서 태그 지정이 필요하도록 제한을 받지 않을 수 있습니다. 예를 들어 `AdministratorAccess` AWS 관리형 정책을 사용하여 사용자에게 전체 관리 권한을 부여하는 경우, 이러한 정책은 해당 액세스를 제한하지 않습니다. 여러 정책이 적용될 때 권한이 결정되는 방법에 대한 자세한 내용은 계정 내에서 요청 허용 여부 결정 (p. 625) 단원을 참조하십시오.

자습서: 사용자들이 자신의 자격 증명 및 MFA 설정을 구성할 수 있도록 하기

사용자가 내 보안 자격 증명 페이지에서 자신의 멀티 팩터 인증(MFA) 디바이스와 자격 증명을 스스로 관리하도록 할 수 있습니다. 사용자에 대해 AWS Management 콘솔을 사용해 이들에 대한 자격 증명(액세스 키,

암호, 서명 인증서 및 SSH 퍼블릭 키)과 MFA 디바이스를 구성할 수 있지만, 이는 사용자 수가 적을 때 유용합니다. 하지만 사용자 수가 증가함에 따라 이 작업은 곧 많은 시간이 소모되는 작업이 될 수 있습니다. 보안 모범 사례에 따라 사용자는 정기적으로 암호를 변경하고 액세스 키를 교체해야 합니다. 또한 사용자는 필요 없는 자격 증명을 삭제하거나 비활성화해야 합니다. 중요한 작업에는 MFA를 사용하는 것이 좋습니다. 이 자습서에서는 관리자에게 부담을 주지 않으면서 이러한 모범 사례를 활성화하는 방법을 보여 줍니다.

이 자습서에서는 사용자가 MFA를 사용하여 로그인하는 경우에만 AWS 서비스에 액세스할 수 있도록 허용하는 방법을 보여 줍니다. MFA 디바이스에 로그인하지 않으면 사용자가 다른 서비스에 액세스할 수 없습니다.

이 워크플로우는 세 가지 기본 단계로 이루어집니다.

1단계: MFA 로그인을 강제할 정책 생성 (p. 56)

사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 변경하고 MFA 디바이스를 관리할 수 있도록 허용하는 몇 가지 IAM 작업을 제외하고 모든 작업을 금지하는 고객 관리형 정책을 생성합니다. 해당 페이지에 액세스하는 방법에 대한 자세한 내용은 IAM 사용자가 자신의 암호를 변경하는 방법(콘솔) (p. 110) 단원을 참조하십시오.

2단계: 테스트 그룹에 정책 연결하기 (p. 57)

멤버가 MFA로 로그인한 경우 해당 멤버에게 모든 Amazon EC2 작업의 전체 액세스 권한을 부여한 그룹을 생성합니다. 이러한 그룹을 생성하려면 `AmazonEC2FullAccess`라는 AWS 관리형 정책과 1단계에서 생성한 고객 관리형 정책을 모두 연결합니다.

3단계: 사용자 액세스 테스트 (p. 57)

테스트 사용자로 로그인하여 사용자가 MFA 디바이스를 생성할 때까지 Amazon EC2에 대한 액세스가 차단되는지 확인합니다. 그런 다음 사용자는 해당 디바이스를 사용하여 로그인할 수 있습니다.

사전 조건

이 자습서의 단계를 수행하려면 다음이 준비되어 있어야 합니다.

- 관리 권한을 가진 IAM 사용자로 로그인할 수 있는 AWS 계정.
- 1단계에서 정책에 입력한 계정 ID 번호.

  계정 ID 번호를 찾으려면 페이지 상단의 탐색 표시줄에서 지원을 선택한 후 지원 센터를 선택합니다. 이 페이지의 지원 메뉴에서 계정 ID를 찾을 수 있습니다.
- 가상(소프트웨어 기반) MFA 디바이스 (p. 122), U2F 보안 키 (p. 125), 또는 하드웨어 기반 MFA 디바이스 (p. 130).
- 다음과 같은 그룹의 구성원인 테스트 IAM 사용자:

사용자 계정 생성		그룹 계정 생성 및 구성		
MFAUser	AWS Management 콘솔 액세스에 대한 옵션만 선택하고 암호를 지정합니다.	EC2MFA	MFAUser	정책을 연결하거나 이 그룹에 권한을 부여하지 마십시오.

1단계: MFA 로그인을 강제할 정책 생성

IAM 사용자가 자신의 자격 증명과 MFA 디바이스를 관리하는 데 필요한 권한을 제외한 모든 권한을 거부하는 IAM 고객 관리형 정책을 만드는 것부터 시작합니다.

1. 관리자 자격 증명을 지닌 사용자로 AWS Management Console에 로그인합니다. IAM 모범 사례를 준수하려면 AWS 계정 루트 사용자 자격 증명을 사용하여 로그인하지 마십시오. 자세한 내용은 개별 IAM 사용자 만들기 단원을 참조하십시오.
2. https://console.aws.amazon.com/iam에서 IAM 콘솔을 엽니다.
3. 탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.
4. JSON 탭을 선택하고 다음 JSON 정책 문서에서 텍스트를 복사합니다. AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391)
5. 정책 텍스트를 JSON 텍스트 상자에 붙여 넣은 다음 Review policy(정책 검토)를 선택합니다. 정책 검사기 (p. 441)가 모든 구문 오류를 보고합니다.

   Note

   언제든지 Visual editor(시각적 편집기) 탭과 JSON 탭 간을 전환할 수 있습니다. 그러나 위의 정책에는 시각적 편집기에서 사용할 수 없는 `NotAction` 요소가 포함되어 있습니다. Visual editor(시각적 편집기) 탭에 이 정책에 대한 알림 메시지가 표시됩니다. 이 정책으로 작업을 계속하려면 JSON 탭으로 돌아가십시오.
6. 검토 페이지에서 정책 이름에 **`Force_MFA`**을 입력합니다. 정책 설명에 다음을 입력합니다. **`This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.`** 정책 요약을 검토하여 정책이 부여한 권한을 확인한 다음 정책 생성을 선택하여 작업을 저장합니다.

   새로운 정책이 관리형 정책 목록에 나타나며 연결 준비가 완료됩니다.

2단계: 테스트 그룹에 정책 연결하기

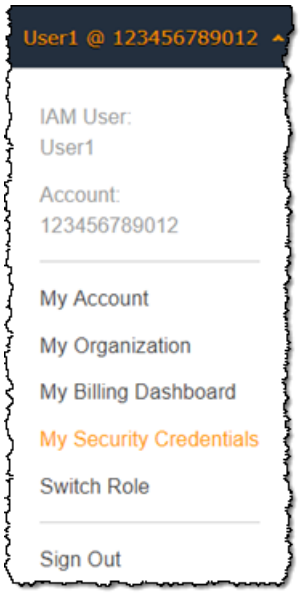
그 다음에는 MFA 보호 권한을 부여하는 데 사용할 테스트 IAM 그룹에 두 개의 정책을 연결합니다.

1. 탐색 창에서 [Groups]를 선택합니다.
2. 검색 상자에 **`EC2MFA`**를 입력한 다음 목록에서 그룹 이름(확인란 아님)을 선택합니다.
3. 권한 탭에서 정책 연결을 클릭합니다.
4. 정책 연결 페이지의 검색 상자에 **`EC2Full`**을 입력한 다음, 목록에서 AmazonEC2FullAccess 옆에 있는 확인란을 선택합니다. 변경 내용을 저장하지 마십시오.
5. 검색 상자에 **`Force`**를 입력한 다음, 목록에서 Force_MFA 옆에 있는 확인란을 선택합니다.
6. Attach Policy(정책 연결)를 선택합니다.

3단계: 사용자 액세스 테스트

자습서의 이 부분에서는 테스트 사용자로 로그인하여 정책이 의도한 대로 작동하는지 검증합니다.

1. 이전 섹션에서 할당한 암호를 사용해 **`MFAUser`**로 AWS 계정에 로그인합니다. URL은 `https://<alias or account ID number>.signin.aws.amazon.com/console`을 사용합니다.
2. EC2를 선택해 Amazon EC2 콘솔을 열고 사용자에게 어떤 권한도 없는지 확인합니다.
3. 오른쪽 상단의 탐색 모음에서 `MFAUser` 사용자 이름을 선택한 다음 내 보안 자격 증명를 선택합니다.



4. 이제 MFA 디바이스를 추가합니다. Multi-Factor Authentication (MFA) 섹션에서 MFA 디바이스 할당을 선택합니다.

   Note

   `iam:DeleteVirtualMFADevice` 수행 권한이 없다는 오류가 표시될 수 있습니다. 이는 이전에 다른 누군가가 가상 MFA 디바이스를 사용자에게 할당하기 시작했다가 프로세스를 취소한 경우 발생할 수 있습니다. 계속 진행하려면 사용자 또는 다른 관리자가 사용자의 기존 MFA 디바이스를 삭제해야 합니다. 자세한 내용은 iam:DeleteVirtualMFADevice를 수행할 권한이 없음 (p. 536) 단원을 참조하십시오.

5. 이 자습서의 경우 휴대폰의 Google Authenticator 앱과 같은 가상(소프트웨어 기반) MFA 디바이스를 사용합니다. Virtual MFA device(가상 MFA 디바이스)를 선택한 다음 다음 단계를 클릭합니다.

   IAM은 QR 코드 그래픽을 포함하여 가상 MFA 디바이스의 구성 정보를 생성 및 표시합니다. 그래픽은 QR 코드를 지원하지 않는 디바이스 상에서 수동 입력할 수 있는 보안 구성 키를 표시한 것입니다.

6. 가상 MFA 앱을 엽니다. (가상 MFA 디바이스의 호스팅에 사용되는 앱 목록은 가상 MFA 애플리케이션을 참조하십시오) 가상 MFA 앱이 다수의 계정(다수의 가상 MFA 디바이스)을 지원하는 경우 옵션을 선택하여 새로운 계정(새로운 가상 MFA 디바이스)을 생성합니다.

7. MFA 앱의 QR 코드 지원 여부를 결정한 후 다음 중 한 가지를 실행합니다.

   - 마법사에서 Show QR code(QR 코드 표시)를 선택합니다. 그런 다음 앱을 사용하여 QR 코드를 스캔합니다. 예를 들어 카메라 모양의 아이콘을 선택하거나 코드 스캔(Scan code)과 비슷한 옵션을 선택한 다음, 디바이스의 카메라를 사용하여 코드를 스캔합니다.
   - Manage MFA Device(MFA 디바이스 관리) 마법사에서 Show secret key(보안 키 표시)을 선택한 다음 MFA 앱에 보안 키를 입력합니다.

   모든 작업을 마치면 가상 MFA 디바이스가 일회용 암호 생성을 시작합니다.

8. MFA 디바이스 관리 마법사의 MFA Code 1(MFA 코드 1) 상자에 현재 가상 MFA 디바이스에 표시된 일회용 암호를 입력합니다. 디바이스가 새로운 일회용 암호를 생성할 때까지 최대 30초 기다립니다. 그런 다음 두 번째 일회용 암호를 MFA Code 2(MFA 코드 2) 상자에 입력합니다. Assign MFA(MFA 할당)을 선택합니다.

   Important

   코드를 생성한 후 즉시 요청을 제출하십시오. 코드를 생성하고 너무 오래 시간이 지난 후 요청을 제출하면 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다.

이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화 (p. 138)할 수 있습니다.

이제 AWS에서 가상 MFA 디바이스를 사용할 준비를 마쳤습니다.

9. 콘솔에서 로그아웃한 다음, **`MFAUser`**로 다시 로그인합니다. 이번에는 AWS가 휴대전화로 받은 MFA 코드를 입력하도록 요청합니다. 코드를 받아 상자에 입력한 후 전송을 선택합니다.
10. EC2를 선택하여 Amazon EC2 콘솔을 다시 엽니다. 이번에는 모든 정보를 볼 수 있으며 원하는 작업은 모두 수행할 수 있습니다. 이 사용자로 다른 콘솔로 이동하면 액세스 거부 메시지가 표시됩니다. 그 이유는 이 자습서의 정책에서 Amazon EC2에 대해서만 액세스 권한을 부여하기 때문입니다.

관련 리소스

IAM 사용 설명서에서 수록된 관련 내용은 다음 리소스 단원을 참조하십시오.

- AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119)
- MFA 디바이스 활성화 (p. 120)
- IAM 로그인 페이지에 MFA 디바이스 사용 (p. 79)

IAM 모범 사례 및 사용 사례

IAM의 이점을 극대화하기 위해 권장 모범 사례에 대해 알아보시기 바랍니다. 이를 위한 한 가지 방법은 실제 시나리오에서 다른 AWS 서비스와 함께 IAM을 어떻게 사용하는지 알아보는 것입니다.

주제

IAM 모범 사례

Follow us on Twitter

AWS 리소스를 안전하게 보호하기 위해 AWS Identity and Access Management(IAM) 서비스에 대한 다음 권장 사항을 따르십시오.

주제

AWS 계정 루트 사용자 액세스 키 잠금

액세스 키(액세스 키 ID 및 보안 액세스 키)를 사용하여 프로그래밍 방식으로 AWS에 요청을 할 수 있습니다. 그러나 AWS 계정 루트 사용자 액세스 키는 사용하지 마십시오. AWS 계정 루트 사용자에 대한 액세스 키는 결제 정보를 포함하여 모든 AWS 서비스의 전체 리소스에 대해 전체 액세스 권한을 부여합니다. AWS 계정 루트 사용자 액세스 키에 연결된 권한은 줄일 수 없습니다.

따라서 신용카드 번호 또는 다른 중요한 기밀 정보와 같이 루트 사용자 액세스 키를 보호해야 합니다. 이를 위한 몇 가지 방법은 다음과 같습니다.

- AWS 계정 루트 사용자에 대한 액세스 키가 아직 없다면 필요할 때까지 만들지 마십시오. 대신 계정 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 로그인한 후 IAM 사용자를 만들어 (p. 20) 관리 권한을 부여합니다.
- AWS 계정 루트 사용자에 대한 액세스 키가 있다면 삭제하고, 계속 유지해야 할 경우 주기적으로 액세스 키를 교체(변경)하십시오. 루트 사용자 액세스 키를 삭제 또는 교체하려면 AWS Management 콘솔의 내 보안 자격 증명 페이지에서 계정의 이메일 주소와 암호를 사용하여 로그인합니다. 액세스 키 섹션에서 액세스 키를 관리할 수 있습니다. 액세스 키 교체에 대한 자세한 내용은 액세스 키 교체 (p. 115) 단원을 참조하십시오.
- 다른 사람과 AWS 계정 루트 사용자 암호 또는 액세스 키를 공유하지 마십시오. 이 설명서의 나머지 섹션에서 AWS 계정 루트 사용자 자격 증명을 다른 사용자와 공유하거나 애플리케이션에 포함하는 것을 피할 수 있는 여러 가지 방법을 참조할 수 있습니다.
- 강력한 암호를 사용하여 AWS Management 콘솔에 대한 계정 수준의 액세스를 보호하십시오. AWS 계정 루트 사용자 암호 관리에 대한 자세한 정보는 AWS 계정 루트 사용자 암호 변경 (p. 100) 단원을 참조하십시오.
- AWS 계정 루트 사용자 계정에서 AWS 멀티 팩터 인증(MFA)을 활성화합니다. 자세한 정보는 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.

개별 IAM 사용자 만들기

AWS 계정 루트 사용자 자격 증명을 사용하여 AWS에 액세스하거나 다른 사용자와 공유하지 마십시오. 대신 AWS 계정에 액세스해야 하는 사용자에 대해 별도의 사용자 계정을 만들어주십시오. 관리자에 대해서도 IAM 사용자를 만들어 관리 권한을 부여한 후 모든 관리 작업에 대해 이 IAM 사용자를 사용하십시오. 이를 위한 자세한 방법은 첫 번째 IAM 관리자 및 그룹 생성 (p. 20) 단원을 참조하십시오.

계정에 액세스하는 사용자에 대해 개별 IAM 사용자를 만들면 각 IAM 사용자에 따라 서로 다른 보안 자격 증명 조합을 부여할 수 있습니다. 또한 각 IAM 사용자에게 다양한 권한을 부여하고, 필요할 경우 언제든지 IAM 사용자의 권한을 변경 또는 취소할 수 있습니다. (루트 사용자 자격 증명을 제공한 후에는 다시 취소하기가 쉽지 않으며 권한을 제한할 수 없습니다.)

> Note
>
> 그러나 개별 IAM 사용자에게 권한을 설정하기 전에 다음과 같은 그룹 관련 참고 사항을 고려해 보십시오.

그룹을 사용하여 IAM 사용자에게 권한을 할당합니다.

개별 IAM 사용자에 대해 권한을 정의하는 대신, 업무(관리자, 개발자, 회계 등)에 관련된 그룹을 만드는 것이 더 편리할 수 있습니다. 그런 다음 각 그룹별로 관련 권한을 정의합니다. 끝으로 해당 그룹에 IAM 사용자를 할당합니다. 그룹에 할당된 권한은 IAM 그룹에 속한 모든 사용자에게 상속됩니다. 따라서 한번에 그룹 내 모든 사용자에 대해 변경 사항을 적용할 수 있습니다. 사내에서 직원의 부서가 변경되면 해당 IAM 사용자가 속한 IAM 그룹만 변경하면 됩니다.

자세한 정보는 다음을 참조하십시오.

- 첫 번째 IAM 관리자 및 그룹 생성 (p. 20)
- IAM 그룹 관리 (p. 169)

최소 권한 부여

IAM 정책을 만들 때는 최소 권한 부여의 표준 보안 조언을 따르거나, 작업 수행에 필요한 최소한의 권한만 부여합니다. 사용자(역할)가 수행해야 하는 작업을 파악한 후 사용자들이 해당 작업만 수행하도록 사용자에 대한 정책을 작성합니다.

최소한의 권한 조합으로 시작하여 필요에 따라 추가 권한을 부여합니다. 처음부터 권한을 많이 부여한 후 나중에 줄이는 방법보다 이 방법이 안전합니다.

액세스 레벨 그룹화를 사용하면 정책이 부여하는 액세스 레벨을 이해할 수 있습니다. 정책 작업 (p. 594)은 `List`, `Read`, `Write`, `Permissions management` 또는 `Tagging`으로 분류됩니다. 예를 들어 `List` 및 `Read` 액세스 레벨에서 작업을 선택하여 사용자에게 읽기 전용 액세스 권한을 부여할 수 있습니다. 정책 요약을 사용하여 액세스 레벨 권한을 이해하는 방법에 대해 알아보려면 액세스 레벨을 이용한 IAM 권한 검토 (p. 63) 단원을 참조하십시오.

이 경우 서비스에서 마지막으로 액세스한 데이터가 유용할 수 있습니다. IAM 사용자, 그룹, 역할 또는 정책에 대한 IAM 콘솔 세부 정보 페이지의 액세스 관리자 탭에서 이 데이터를 확인합니다. AWS Organizations 마스터 계정 자격 증명을 사용하여 로그인한 경우 IAM 콘솔의 AWS Organizations 섹션에서 이 데이터를 볼 수 있습니다. 또한 AWS CLI 또는 AWS API를 사용하여 IAM 또는 조직의 엔터티 또는 정책에 대해 서비스에서 마지막으로 액세스한 데이터 보고서를 검색할 수 있습니다. 이 정보를 사용하여 불필요한 권한을 확인할 수 있으므로 IAM 또는 Organizations 정책을 미세 조정함으로써 최소 권한의 원칙을 보다 잘 준수할 수 있습니다. 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

권한을 추가로 줄이려면 AWS CloudTrail 이벤트 이력에서 계정의 이벤트를 확인합니다. CloudTrail 이벤트 로그에는 정책의 권한을 변경하는 데 사용할 수 있는 자세한 이벤트 정보가 포함되어 있습니다. 로그에는 IAM 엔터티에 필요한 작업 및 리소스만 포함되어 있습니다. 자세한 정보는 AWS CloudTrail 사용 설명서에서 CloudTrail 콘솔에서 CloudTrail 이벤트 보기 단원을 참조하십시오.

자세한 정보는 다음을 참조하십시오.

- 액세스 관리 (p. 348)
- 각 서비스의 정책 주제에서는 서비스별 리소스에 대해 정책을 작성하는 방법의 예제를 제공합니다. 예제:
  - Amazon DynamoDB 개발자 안내서의 Amazon DynamoDB 인증 및 액세스 제어
  - Amazon Simple Storage Service 개발자 가이드의 버킷 정책 및 사용자 정책 사용
  - Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요

AWS 관리형 정책으로 권한 사용 시작

직원에게 필요한 권한만 제공하려면 IAM 정책에 대한 시간과 자세한 지식이 필요합니다. 직원들은 필요하거나 사용해야 하는 AWS 서비스를 익힐 시간이 필요합니다. 관리자는 IAM에 대해 배우고 테스트할 시간이 필요합니다.

신속하게 시작하려면 AWS 관리형 정책을 사용하여 직원에게 시작해야 하는 권한을 부여합니다. 이 정책은 이미 계정에서 사용할 수 있으며 AWS에 의해 유지 관리 및 업데이트됩니다. AWS 관리형 정책에 대한 자세한 정보는 AWS 관리형 정책 (p. 357) 단원을 참조하십시오.

AWS 관리형 정책은 여러 가지 일반 사용 사례에서 권한을 제공할 목적으로 설계되었습니다. AmazonDynamoDBFullAccess 및 IAMFullAccess와 같은 전체 액세스 AWS 관리형 정책은 서비스에 대한 전체 액세스 권한을 부여하여 서비스 관리자에 대한 권한을 정의합니다. AWSCodeCommitPowerUser 및 AWSKeyManagementServicePowerUser와 같은 파워 사용자 AWS 관리형 정책은 권한 관리 권한을 허용하지 않고 AWS 서비스에 대한 여러 수준의 액세스를 제공합니다. AmazonMobileAnalyticsWriteOnlyAccess 및 AmazonEC2ReadOnlyAccess와 같은 부분 액세스 AWS 관리형 정책은 AWS 서비스에 대한 특정 액세스 수준을 제공합니다. AWS 관리형 정책을 사용하면 정책을 직접 작성하는 것보다 쉽게 사용자, 그룹 및 역할에 적절한 권한을 할당할 수 있습니다.

직무 기능에 관한 AWS 관리형 정책은 다양한 서비스에 적용할 수 있으며 IT 업계의 일반적인 직무 기능과 연계됩니다. 직무 정책의 목록과 설명은 직무 기능에 대한 AWS 관리형 정책 (p. 642) 단원을 참조하십시오.

인라인 정책 대신 고객 관리형 정책 사용

사용자 지정 정책의 경우 인라인 정책보다는 관리형 정책의 사용을 권장합니다. 이 정책을 사용하면 콘솔의 한 위치에서 모든 관리형 정책을 볼 수 있다는 이점이 있습니다. 또한 단일 AWS CLI 또는 AWS API 작업으로 이 정보를 볼 수도 있습니다. 인라인 정책은 IAM ID(사용자, 그룹 또는 역할)에만 존재하는 정책입니다. 관

리형 정책은 여러 자격 증명에 연결할 수 있는 별도의 IAM 리소스입니다. 자세한 정보는 관리형 정책과 인라인 정책 (p. 357) 단원을 참조하십시오.

계정에 인라인 정책이 있는 경우 이를 관리형 정책으로 변환할 수 있습니다. 이렇게 하려면 정책을 새로운 관리형 정책에 복사하고 새 정책을 인라인 정책이 있는 자격 증명에 연결합니다. 그런 다음 인라인 정책을 삭제합니다. 아래 지침을 사용하여 이 작업을 수행할 수 있습니다.

인라인 정책을 관리형 정책으로 변환하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 그룹, 사용자 또는 역할을 선택합니다.
3. 목록에서 제거할 정책이 있는 그룹, 사용자 또는 역할 이름을 선택합니다.
4. Permissions 탭을 선택합니다. 그룹을 선택한 경우 필요에 따라 Inline Policies(인라인 정책) 섹션을 확장합니다.
5. 그룹의 경우 제거할 인라인 정책 옆의 정책 표시를 선택합니다. 사용자 및 역할에 대해 필요한 경우 Show ***n*** more(n개 더 표시)를 선택한 다음 제거할 인라인 정책 옆에 있는 화살표를 선택합니다.
6. 정책에 대한 JSON 정책 문서를 복사합니다.
7. 탐색 창에서 정책을 선택합니다.
8. 정책 생성을 선택한 후 JSON 탭을 선택합니다.
9. 기존 텍스트를 JSON 정책 텍스트로 바꾸고 정책 검토를 선택합니다.
10. 정책 이름을 입력하고 정책 생성을 선택합니다.
11. 탐색 창에서 그룹, 사용자 또는 역할을 선택한 다음 제거하려는 정책이 있는 그룹, 사용자 또는 역할의 이름을 다시 선택합니다.
12. 그룹의 경우 정책 연결을 선택합니다. 사용자 및 역할의 경우 권한 추가를 선택합니다.
13. 그룹에 대해 새 정책 이름 옆의 확인란을 선택한 다음 정책 연결을 선택합니다. 사용자 또는 역할의 경우 권한 추가를 선택합니다. 다음 페이지에서 기존 정책 직접 연결을 선택하고 새 정책 이름 옆의 확인란을 선택한 다음 다음: 검토를 선택하고 권한 추가를 선택합니다.

    그룹, 사용자 또는 역할에 대한 요약 페이지로 돌아갑니다.
14. 그룹의 경우 제거할 인라인 정책 옆의 정책 제거를 선택합니다. 사용자 또는 역할의 경우 제거할 인라인 정책 옆의 X를 선택합니다.

경우에 따라 관리형 정책에 대한 인라인 정책을 선택하는 것이 좋습니다. 자세한 정보는 관리형 정책과 인라인 정책의 선택 (p. 361) 단원을 참조하십시오.

액세스 레벨을 이용한 IAM 권한 검토

AWS 계정의 보안을 개선하려면 모든 IAM 정책을 정기적으로 검토하고 모니터링해야 합니다. 정책은 필요한 작업을 수행하는 데 필요한 최소 권한 (p. 61)만 부여해야 합니다.

정책을 보면 그 정책 안에서 각 서비스에 대한 액세스 레벨의 요약이 들어 있는 정책 요약 (p. 483)을 확인할 수 있습니다. AWS은 작업 내용에 따라 각 서비스 작업을 다섯 개의 액세스 레벨, 즉 `List`, `Read`, `Write`, `Permissions management`, `Tagging` 중 하나로 분류합니다. 이러한 액세스 레벨을 사용하여 어떤 작업을 정책에 포함할지 결정할 수 있습니다.

예를 들어 Amazon S3 서비스의 경우, 다수의 사용자가 `List` 및 `Read` 작업에 액세스하도록 허용할 수 있습니다. 이러한 작업은 사용자가 Amazon S3에 버킷을 나열하고 객체를 가져오도록 허용합니다. 하지만 소수의 사용자만 Amazon S3 `Write` 작업에 액세스하여 버킷을 삭제하거나 S3 버킷에 객체를 넣도록 허용해야 합니다. 또한 관리자만 Amazon S3 `Permissions management` 작업에 액세스할 수 있도록 권한을 줄여야 합니다. 그래야 제한된 수의 사람만 Amazon S3에서 버킷 정책을 관리할 수 있습니다. IAM 및 AWS Organizations 서비스의 `Permissions management` 작업에서는 이 점이 특히 중요합니다.

`Tagging` 작업을 허용하면 리소스에 대한 태그만을 수정하는 작업을 수행할 사용자 권한을 부여합니다. 하지만 `CreateRole` 등과 같은 일부 `Write` 작업은 리소스를 생성하거나 리소스에 대한 다른 속성을 수정할 때 리소스 태그 지정을 허용합니다. 따라서 `Tagging` 작업에 대한 액세스를 거부하면 사용자가 리소스 태그 지정을 수행할 수 없습니다. 액세스 레벨 분류에 대한 세부 정보와 예제는 정책 요약에서 액세스 레벨 요약 이해하기 (p. 491) 단원을 참조하십시오.

서비스의 각 작업에 할당된 액세스 레벨 분류를 보려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

정책의 액세스 레벨을 보려면 먼저 정책 요약을 찾아야 합니다. 정책 요약에서 관리형 정책에 관한 부분은 정책 페이지에, 사용자에게 연결되는 정책 부분은 사용자 페이지에 수록됩니다. 자세한 정보는 정책 요약(서비스 목록) (p. 484) 단원을 참조하십시오.

정책 요약의 액세스 레벨 열에는 정책이 서비스의 네 가지 AWS 액세스 레벨 중 하나 이상에 대해 전체 또는 제한 액세스 권한을 제공한다고 표시되어 있습니다. 또는 정책이 서비스 내 모든 작업에 모든 액세스를 제공한다고 표시되어 있을 수도 있습니다. 이 액세스 레벨 열에 수록된 정보를 통해 정책이 제공하는 액세스 레벨을 알 수 있습니다. 그런 다음 AWS 계정을 더 안전하게 사용하기 위한 조치를 취할 수 있습니다. 액세스 레벨 분류에 대한 세부 정보와 예제는 정책 요약에서 액세스 레벨 요약 이해하기 (p. 491) 단원을 참조하십시오.

사용자에 대한 강력한 암호 정책 구성

사용자가 직접 암호를 변경하도록 허용할 경우 강력한 암호를 만들고 주기적으로 암호를 변경하도록 해야 합니다. IAM 콘솔의 계정 설정 페이지에서 계정 암호 정책을 만들 수 있습니다. 암호 정책을 사용하여 최소 길이, 비 알파벳 문자 포함 여부, 교체 주기 등의 암호 요구 사항을 정의할 수 있습니다.

자세한 내용은 IAM 사용자의 계정 암호 정책 설정 (p. 101) 단원을 참조하십시오.

MFA 활성화

보안 강화를 위해 계정에 속한 모든 사용자에게 Multi-Factor Authentication(MFA)을 요구하는 것이 좋습니다. MFA에는 인증 문제에 응답을 생성하는 디바이스가 있습니다. 로그인 과정을 완료하려면 사용자의 자격 증명과 디바이스에서 생성한 응답 두 가지가 모두 필요합니다. 사용자의 암호 또는 액세스 키가 손상된 경우에도 추가 인증 요건 때문에 계정 리소스가 계속해서 안전합니다.

응답은 다음 중 한 가지 방법으로 생성합니다.

- 가상 및 하드웨어 MFA 디바이스가 코드를 생성하여 앱 또는 디바이스에 보여준 후 로그인 화면에 입력합니다.
- 사용자가 디바이스를 터치하면 U2F 보안 키가 응답을 생성합니다. 로그인 화면에 사용자가 직접 코드를 입력할 필요가 없습니다.

민감한 리소스 또는 API 작업에 액세스할 수 있도록 권한이 부여된 IAM 사용자라면 U2F 또는 하드웨어 MFA 디바이스를 사용하는 것이 좋습니다.

MFA에 대한 자세한 내용은 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.

MFA를 사용해 액세스 키에 대한 보안 API 액세스를 구성하는 방법에 대한 자세한 내용은 MFA 보호 API 액세스 구성 (p. 146) 단원을 참조하십시오.

Amazon EC2 인스턴스에서 실행되는 애플리케이션에 역할 사용

Amazon EC2 인스턴스에서 실행되는 애플리케이션이 다른 AWS 서비스에 액세스하려면 자격 증명이 필요하며, 이 애플리케이션에 안전하게 자격 증명을 제공하려면 IAM 역할을 사용합니다. 역할에는 특정 사용자

나 그룹이 아닌 권한의 조합이 설정됩니다. 또한 역할에는 IAM 사용자와 달리 영구적인 자격 증명 조합이 부여되지 않습니다. Amazon EC2의 경우 IAM은 EC2 인스턴스에 동적으로 생성되는 임시 자격 증명을 제공하며 이 자격 증명은 자동 교체됩니다.

EC2 인스턴스 실행 시 실행 파라미터로 인스턴스에 대한 역할을 지정할 수 있습니다. EC2 인스턴스에서 실행되는 애플리케이션은 AWS 리소스에 액세스할 때 역할의 자격 증명을 사용할 수 있습니다. 역할의 권한에 따라 애플리케이션에서 수행할 수 있는 작업이 결정됩니다.

자세한 정보는 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265) 단원을 참조하십시오.

역할을 사용하여 권한 위임

다른 AWS 계정의 사용자가 내 AWS 계정의 리소스에 액세스하도록 허용하려면 계정 간에 보안 자격 증명을 공유하지 마십시오. 대신 IAM 역할을 사용하십시오. 다른 계정의 IAM 사용자에게 어떤 권한이 허용되는지 지정하는 역할을 정의할 수 있습니다. 어떤 AWS 계정에 해당 역할을 수임하도록 허용된 IAM 사용자가 있는지를 지정할 수도 있습니다. 해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

자세한 내용은 역할 용어 및 개념 (p. 175) 단원을 참조하십시오.

액세스 키를 공유하지 마십시오

액세스 키는 AWS으로의 프로그래밍 방식 액세스를 제공합니다. 액세스 키를 암호화되지 않은 코드에 삽입하거나 AWS 계정 사용자 간에 이들 보안 자격 증명을 공유하지 마십시오. AWS로 액세스가 필요한 애플리케이션은 IAM 역할을 사용하여 임시 보안 자격 증명 검색하도록 프로그램을 구성합니다. 사용자별 프로그래밍 액세스를 허용하고자 한다면 개인 액세스 키가 있는 IAM 사용자를 만듭니다.

자세한 정보는 IAM 역할(AWS API)로 전환하기 (p. 263) 및 IAM 사용자의 액세스 키 관리 (p. 111)을(를) 참조하십시오.

자격 증명을 정기적으로 교체

암호와 액세스 키를 정기적으로 교체하고, 계정의 모든 IAM 사용자도 이와 같이 하도록 해야 합니다. 그러면 자신도 모르게 암호 또는 액세스 키가 손상되어도 이 손상된 자격 증명이 리소스 액세스에 사용되는 기간을 줄일 수 있습니다. 계정에 모든 IAM 사용자가 주기적으로 암호를 교체하도록 요구하는 암호 정책을 적용할 수 있습니다. 또한 얼마나 자주 교체하도록 할지 선택할 수 있습니다.

계정의 암호 정책 설정에 대한 자세한 정보는 IAM 사용자의 계정 암호 정책 설정 (p. 101) 단원을 참조하십시오.

IAM 사용자의 액세스 키 교체에 대한 자세한 정보는 액세스 키 교체 (p. 115) 단원을 참조하십시오.

불필요한 자격 증명 삭제

필요 없는 IAM 사용자 자격 증명(암호 및 액세스 키)은 삭제합니다. 예를 들어 콘솔을 사용하지 않는 애플리케이션에 대해 IAM 사용자를 생성한 경우 IAM 사용자는 암호가 필요하지 않습니다. 마찬가지로 사용자가 콘솔만 사용하는 경우 액세스 키를 제거하십시오. 최근에 사용된 적이 없는 암호와 액세스 키는 삭제해야 할 자격 증명을 식별하기 위한 좋은 기준이 될 수 있습니다. 콘솔, CLI, API를 사용하여 또는 자격 증명 보고서를 다운로드하여 미사용 암호나 액세스 키를 확인할 수 있습니다.

최근 사용되지 않은 IAM 사용자 자격 증명 확인에 대한 자세한 정보는 미사용 자격 증명 찾기 (p. 154) 단원을 참조하십시오.

IAM 사용자의 암호 삭제에 대한 자세한 정보는 IAM 사용자의 암호 관리 (p. 104) 단원을 참조하십시오.

IAM 사용자의 액세스 키 비활성화 또는 삭제에 대한 자세한 정보는 IAM 사용자의 액세스 키 관리 (p. 111) 단원을 참조하십시오.

IAM 자격 증명 보고서에 대한 자세한 정보는 AWS 계정의 자격 증명 보고서 가져오기 (p. 156) 단원을 참조하십시오.

보안 강화를 위해 정책 조건 사용

필요할 경우 IAM 정책에서 리소스에 대한 액세스 허용 조건을 정의할 수 있습니다. 예를 들어 요청을 할 수 있는 IP 주소의 범위를 지정하도록 조건을 작성할 수 있습니다. 특정 기간이나 시간 범위 내에서만 요청이 가능하도록 조건을 작성할 수도 있습니다. 또한 SSL 또는 MFA(멀티 팩터 인증)를 사용하도록 조건을 설정할 수 있습니다. 예를 들어 MFA 디바이스를 사용하여 인증된 사용자만 Amazon EC2 인스턴스를 종료할 수 있도록 조건을 지정할 수 있습니다.

자세한 정보는 IAM 정책 요소 참조에서 IAM JSON 정책 요소: Condition (p. 598) 단원을 참조하십시오.

AWS 계정의 활동 모니터링

AWS의 로깅 기능을 사용하여 사용자가 계정에서 수행한 작업과 사용한 리소스를 확인할 수 있습니다. 로그 파일에는 작업 시간 및 날짜, 작업의 소스 IP, 부족한 권한으로 인해 실패한 작업 등이 나와 있습니다.

로깅 기능은 다음과 같은 AWS 서비스에서 제공됩니다.

- Amazon CloudFront – CloudFront에서 받는 사용자 요청을 기록합니다. 자세한 정보는 Amazon CloudFront 개발자 안내서의 액세스 로그 단원을 참조하십시오.
- AWS CloudTrail – AWS 계정에서 또는 이를 대신하여 수행된 AWS API 호출 및 관련 이벤트를 기록합니다. 자세한 정보는 AWS CloudTrail User Guide 단원을 참조하십시오.
- Amazon CloudWatch – AWS 클라우드 리소스 및 AWS에서 실행되는 애플리케이션을 모니터링합니다. 정의한 지표에 기반하여 CloudWatch에서 경보를 설정할 수 있습니다. 자세한 정보는 Amazon CloudWatch 사용 설명서 단원을 참조하십시오.
- AWS Config – IAM 사용자, 그룹, 역할 및 정책 등 AWS 리소스의 구성에 대한 세부적인 기록 정보를 제공합니다. 예를 들어, AWS Config를 사용하여 특정 시점에 사용자 또는 그룹에 속한 권한을 확인할 수 있습니다. 자세한 정보는 AWS Config Developer Guide 단원을 참조하십시오.
- Amazon Simple Storage Service(Amazon S3) – Amazon S3 버킷에 대한 액세스 요청을 기록합니다. 자세한 정보는 Amazon Simple Storage Service 개발자 가이드에서 서버 액세스 로깅 단원을 참조하십시오.

IAM 모범 사례에 대한 동영상 프레젠테이션

다음 동영상에는 이러한 모범 사례 및 여기서 논의한 기능을 사용하여 작업을 수행하는 방법에 대한 상세 정보를 보여주는 컨퍼런스 프레젠테이션이 포함되어 있습니다.

AWS re:Invent 2015 - IAM 모범 사례

기업 사용 사례

IAM의 간단한 기업 사용 사례를 통해 사용자의 AWS 액세스 권한을 제어하기 위한 서비스 구현의 기본적인 방법을 이해할 수 있습니다. 사용 사례는 일반적인 용어로 서술되며 원하는 결과를 달성하기 위해 IAM API를 사용하는 방법에 대한 기술적인 내용을 다루지 않습니다.

이 사용 사례에서는 Example Corp라는 가상의 회사가 IAM를 사용하는 2가지 일반적인 방법에 대해 살펴보겠습니다. 첫 번째 시나리오는 Amazon Elastic Compute Cloud(Amazon EC2)를 가정합니다. 두 번째는 Amazon Simple Storage Service(Amazon S3)를 가정합니다.

다른 AWS 서비스와 함께 IAM를 사용하는 방법에 대한 자세한 정보는 IAM로 작업하는 AWS 서비스 (p. 573) 섹션 단원을 참조하십시오.

주제

Example Corp의 초기 설정

Example Corp의 창립자인 John은 회사 초창기에는 자신이 직접 AWS 계정을 만들어 AWS 제품을 관리했으며, 이후 개발자와 관리자, 테스트 담당자, 관리자 및 시스템 관리자로 일할 직원들을 고용했습니다.

John은 AWS Management 콘솔을 사용하여 AWS 계정 루트 사용자 자격 증명으로 자신이 사용할 John이라는 계정과 Admins라는 그룹을 생성했습니다. 그는 AWS 관리형 정책 AdministratorAccess를 사용하여 Admins 그룹에 AWS 계정의 리소스에서 모든 작업을 수행할 수 있는 권한을 부여합니다. 그런 다음 John 사용자를 Admins 그룹에 추가했습니다. 이처럼 관리자 그룹과 IAM 사용자를 만든 후 이 사용자를 관리자 그룹에 추가하기 위한 단계별 지침은 첫 번째 IAM 관리자 및 그룹 생성 (p. 20) 단원을 참조하십시오.

이제 John은 AWS와 상호 작용하는 데 루트 사용자의 자격 증명을 사용하는 대신 개인 사용자 계정의 자격 증명만 사용합니다.

John은 또한 AWS 계정 내 모든 사용자에게 계정 수준의 권한을 간편하게 적용할 수 있도록 AllUsers라는 그룹을 생성합니다. 그리고 자신도 이 그룹에 추가했습니다. 그런 다음 Developers, Testers, Managers, SysAdmins라고 하는 그룹을 각각 만들었습니다. 그리고 각 직원들에 대해 사용자 계정을 만들어 해당 그룹에 추가했습니다. 또한 모든 사용자를 AllUsers 그룹에도 추가했습니다. 그룹 생성에 대한 자세한 정보는 IAM 그룹 생성 (p. 168) 섹션을, 사용자 생성에 대한 자세한 정보는 AWS 계정의 IAM 사용자 생성 (p. 87) 단원을 참조하고, 사용자를 그룹에 추가하는 방법은 IAM 그룹 관리 (p. 169) 단원을 참조하십시오.

Amazon EC2의 IAM 사용 사례

Example Corp와 같은 회사는 일반적으로 IAM를 사용하여 Amazon EC2와 같은 서비스와 상호 작용합니다. 이 부분의 사용 사례를 이해하기 위해서는 Amazon EC2에 대한 기본적인 지식이 필요합니다. Amazon EC2에 대한 자세한 정보는 Linux 인스턴스용 Amazon EC2 사용 설명서 단원을 참조하십시오.

그룹에 대한 Amazon EC2 권한

"경계" 제어를 제공하기 위해 John은 정책을 AllUsers 그룹에 연결합니다. 이 정책은 Example Corp 회사 네트워크의 IP 주소가 아닌 주소에서 시작된 모든 사용자의 AWS 요청을 거부합니다.

Example Corp는 다음과 같이 그룹에 따라 서로 다른 권한을 부여했습니다.

- 시스템 관리자 – AMI, 인스턴스, 스냅샷, 볼륨, 보안 그룹 등을 생성하고 관리하기 위한 권한이 필요합니다. John은 그룹 구성원에게 모든 Amazon EC2 작업을 사용할 수 있는 권한을 부여하는 `AmazonEC2FullAccess` AWS 관리형 정책을 SysAdmins 그룹에 연결합니다.
- 개발자 – 인스턴스를 사용한 작업 권한만 필요합니다. 따라서 John은 개발자가 `DescribeInstances`, `RunInstances`, `StopInstances`, `StartInstances`, `TerminateInstances`를 호출할 수 있는 권한을 부여하는 정책을 생성하고 Developers 그룹에 연결합니다.

  Note

  Amazon EC2는 SSH 키, Windows 암호 및 보안 그룹을 사용하여 특정 Amazon EC2 인스턴스의 운영 체제에 액세스할 사용자를 제어합니다. IAM 시스템에서는 특정 인스턴스의 운영 체제 액세스를 허용 또는 거부할 방법을 제공하지 않습니다.
- 관리자 – 현재 제공되고 있는 Amazon EC2 리소스를 나열하는 것 외, 어떤 Amazon EC2 작업도 수행할 필요가 없습니다. 따라서 John은 Amazon EC2 "Describe" API 작업만 호출할 수 있는 권한을 부여하는 정책을 생성하고 Managers 그룹에 연결합니다.

이러한 각 정책의 예를 보려면 Linux 인스턴스용 Amazon EC2 사용 설명서에서 IAM 자격 증명 기반 정책 예제 (p. 387) 및 AWS Identity and Access Management 단원을 참조하십시오.

사용자의 직무 변경

그러다가 개발자 중 한 명인 Paulo가 직무를 바꾸어 관리자가 되었습니다. John은 Paulo를 Developers 그룹에서 Managers 그룹으로 옮겼습니다. 이제 Paulo는 Managers 그룹에 속하며 더 이상 Amazon EC2 인스턴스와 상호 작용할 수 없습니다. 즉, 인스턴스를 실행하거나 시작할 수 없으며, 이전에 자신이 시작한 인스턴스일지라도 더 이상 기존 인스턴스를 중지하거나 종료할 수 없습니다. Example Corp 사용자가 시작한 인스턴스를 나열할 수만 있습니다.

Amazon S3의 IAM 사용 사례

Example Corp와 같은 회사는 또한 기본적으로 Amazon S3와 함께 IAM를 사용합니다. John은 example_bucket이라는 회사용 Amazon S3 버킷을 생성했습니다.

추가 사용자와 그룹 생성

직원인 Zhang과 Mary는 모두 회사의 버킷에 데이터를 생성할 수 있어야 합니다. 또한 개발자들이 작업 중인 공유 데이터를 읽고 쓸 수 있어야 합니다. 이를 위해 John은 다음 그림과 같은 Amazon S3 키 접두사 체계에 따라 example_bucket의 데이터에 대한 논리적 구조를 정했습니다.

```
/example_bucket
    /home
        /zhang
        /mary
    /share
        /developers
        /managers
```

John은 마스터 `/example_bucket`을 각 직원별 홈 디렉터리, 그리고 개발자와 관리자의 그룹에서 함께 공유하는 영역으로 나누었습니다.

그런 다음 John은 다음과 같이 사용자와 그룹에 대해 권한을 부여하는 정책의 조합을 생성했습니다.

- Zhang의 홈 디렉터리 액세스 – John은 Zhang에게 Amazon S3 키 접두사 `/example_bucket/home/Zhang/`로 객체에 대해 읽기, 쓰기 및 나열 권한을 부여하는 정책을 연결했습니다.
- Mary의 홈 디렉터리 액세스 – John은 Mary에게 Amazon S3 키 접두사 `/example_bucket/home/mary/`로 객체에 대해 읽기, 쓰기 및 나열 권한을 부여하는 정책을 연결했습니다.
- Developers 그룹에 대한 공유 디렉터리 액세스 – John은 개발자에게 `/example_bucket/share/developers/` 키 접두사로 객체에 대해 읽기, 쓰기 및 나열 권한을 부여하는 정책을 그룹에 연결했습니다.
- Managers 그룹에 대한 공유 디렉터리 액세스 – John은 관리자에게 `/example_bucket/share/managers/` 키 접두사로 객체에 대해 읽기, 쓰기 및 나열 권한을 부여하는 정책을 연결했습니다.

> **Note**
>
> Amazon S3는 버킷 또는 객체를 만든 사용자에게 해당 버킷 또는 객체에 대해 자동으로 다른 작업을 수행할 권한을 부여하지 않습니다. 따라서 IAM 정책에서 명시적으로 사용자에게 사용자가 생성한 Amazon S3 리소스를 사용할 권한을 부여해야 합니다.

이러한 각 정책의 예를 보려면 Amazon Simple Storage Service 개발자 가이드에서 액세스 제어 단원을 참조하십시오. 런타임 시 정책이 어떻게 평가되는지 알아보려면 정책 평가 로직 (p. 622) 단원을 참조하십시오.

사용자의 직무 변경

그러다가 개발자 중 한 명인 Zhang이 직무를 바꾸어 관리자가 되었습니다. 따라서 더 이상 `share/developers` 디렉터리의 문서에 액세스할 필요가 없으므로 관리자인 John은 Zhang을 `Managers` 그룹에서

`Developers` 그룹으로 옮겼습니다. 이처럼 간단한 재할당만으로 `Managers` 그룹에 허가된 모든 권한이 자동으로 Zhang에게 부여되고, 더 이상 `share/developers` 디렉터리의 데이터에서는 액세스하지 못하게 됩니다.

타사 통합

기업은 종종 파트너 업체와 컨설턴트, 계약자들과 작업합니다. Example Corp는 Widget Company라고 하는 파트너가 있으며, 이 Widget Company의 직원인 Shirley에게 Example Corp에서 사용하는 버킷에 데이터를 추가할 권한을 부여해야 합니다. John은 WidgetCo라는 그룹과 `Shirley`라는 사용자를 생성하고 Shirley를 WidgetCo 그룹에 추가했습니다. John은 또한 example_partner_bucket이라는 Shirley 전용 버킷을 생성했습니다.

John은 기존 정책을 업데이트하거나 새 정책을 추가하여 Widget Company 파트너에게 적절한 권한을 부여할 수 있습니다. 예를 들어 John은 WidgetCo 그룹의 구성원에게는 쓰기 이외의 모든 작업을 사용할 권한을 거부하는 새 정책을 생성할 수 있습니다. 모든 사용자에게 광범위한 Amazon S3 작업에 대해 액세스 권한을 부여하는 정책이 있을 경우에만 이 정책이 필요합니다.

IAM 콘솔 및 로그인 페이지

AWS Management 콘솔에서는 웹을 기반으로 AWS 서비스를 관리할 수 있습니다. 콘솔에 로그인하여 내 계정의 AWS 서비스를 생성하고, 조회하며, 작업을 수행할 수 있습니다. 이러한 작업에는 Amazon EC2 인스턴스 및 Amazon RDS 데이터베이스 시작/중지, Amazon DynamoDB 테이블 생성, IAM 사용자 생성 등이 포함됩니다.

AWS Management 콘솔을 열면 세 개의 별도 로그인 페이지 중 하나가 표시될 수 있습니다.

- 기본 로그인 페이지 (p. 72) – https://console.aws.amazon.com/에서 루트 사용자 이메일 주소 또는 IAM 사용자 계정 ID를 입력합니다.
- AWS 계정 루트 사용자 로그인 페이지 (p. 73) – 루트 사용자 암호를 입력합니다.
- IAM 사용자 로그인 페이지 (p. 74) – 이 페이지에 IAM 사용자 이름과 암호를 입력합니다.

로그인 프로세스

이전에 다른 페이지에 로그인한 경우 브라우저에서 이 기본 설정을 기억할 수 있습니다. 루트 사용자 및 IAM 사용자 로그인 페이지의 링크를 사용하여 기본 페이지로 돌아갈 수 있습니다.

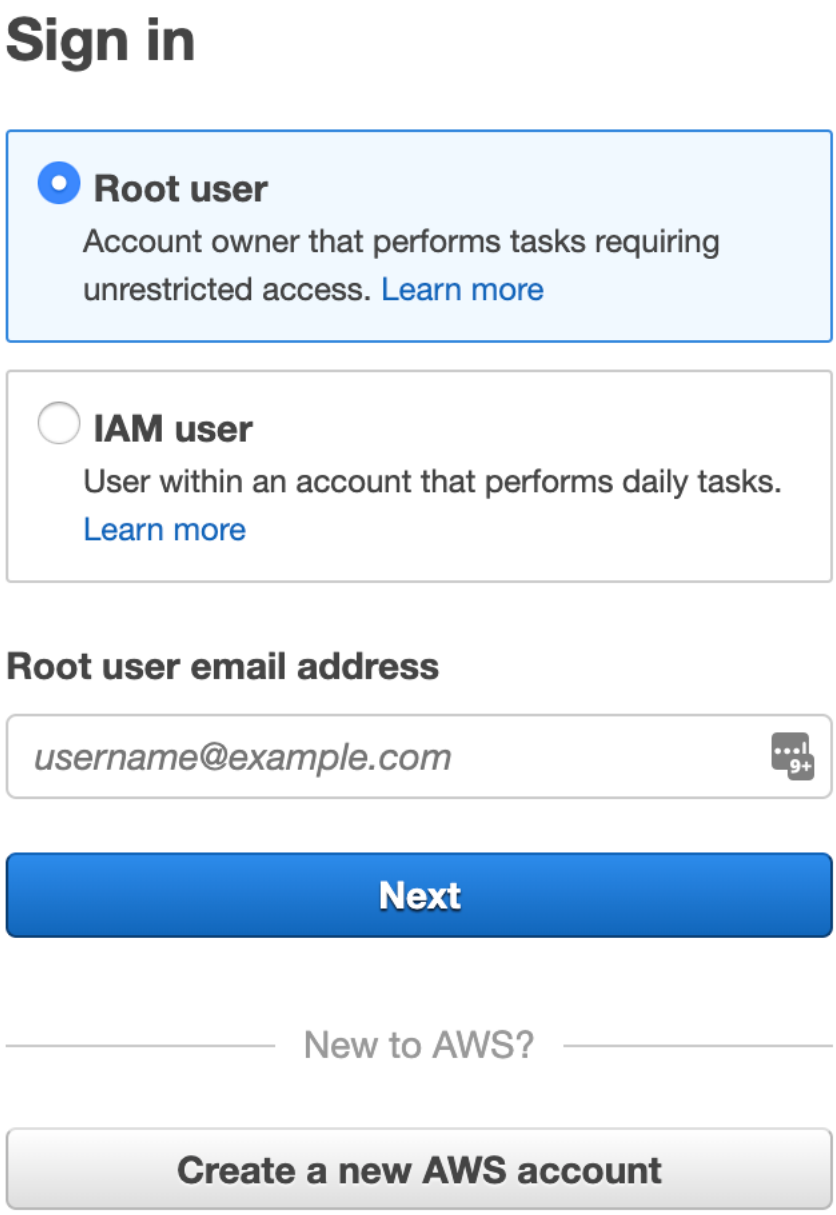
기본 로그인 페이지

https://console.aws.amazon.com/으로 이동하여 기본 로그인 페이지에 액세스할 수 있습니다.

기본 AWS 로그인 페이지에서 루트 사용자 또는 IAM 사용자로 로그인하도록 선택할 수 있습니다. 계정 소유자로 로그인하려면 AWS 계정 루트 사용자 이메일 주소를 입력합니다. 루트 사용자 이메일 주소를 입력하면 루트 사용자 로그인 페이지로 이동합니다.

IAM 사용자로 로그인하려면 IAM user(IAM 사용자)를 선택하고 계정 ID 또는 계정 별칭을 입력합니다. 계정 정보를 입력하면 IAM 사용자 로그인 페이지로 이동합니다.

기본 로그인 페이지



AWS 계정 루트 사용자 로그인 페이지

Amazon Web Services(AWS) 계정을 처음 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 Single Sign-In 자격 증명으로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다.

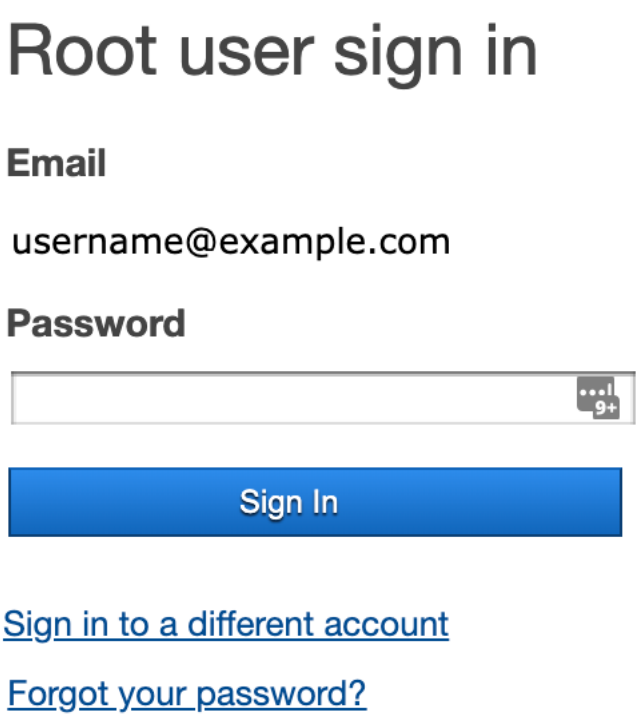
Important

일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 마실 것을 강력히 권장합니다. 대신, IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례 (p. 61)를 준수합니다. 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 작업을 수행

할 때만 사용합니다. 루트 사용자로 로그인해야 하는 작업을 보려면 루트 사용자가 필요한 AWS 작업을 참조하십시오. 일상적 사용을 위해 관리자를 설정하는 방법에 대한 자습서는 첫 번째 IAM 관리자 및 그룹 생성 (p. 20) 단원을 참조하십시오.

루트 사용자 로그인 페이지에 액세스하려면 기본 로그인 페이지에서 루트 사용자를 선택하고 루트 사용자 이메일 주소를 입력해야 합니다. 그런 다음 이 페이지에 암호를 입력할 수 있습니다.

루트 사용자 로그인 페이지



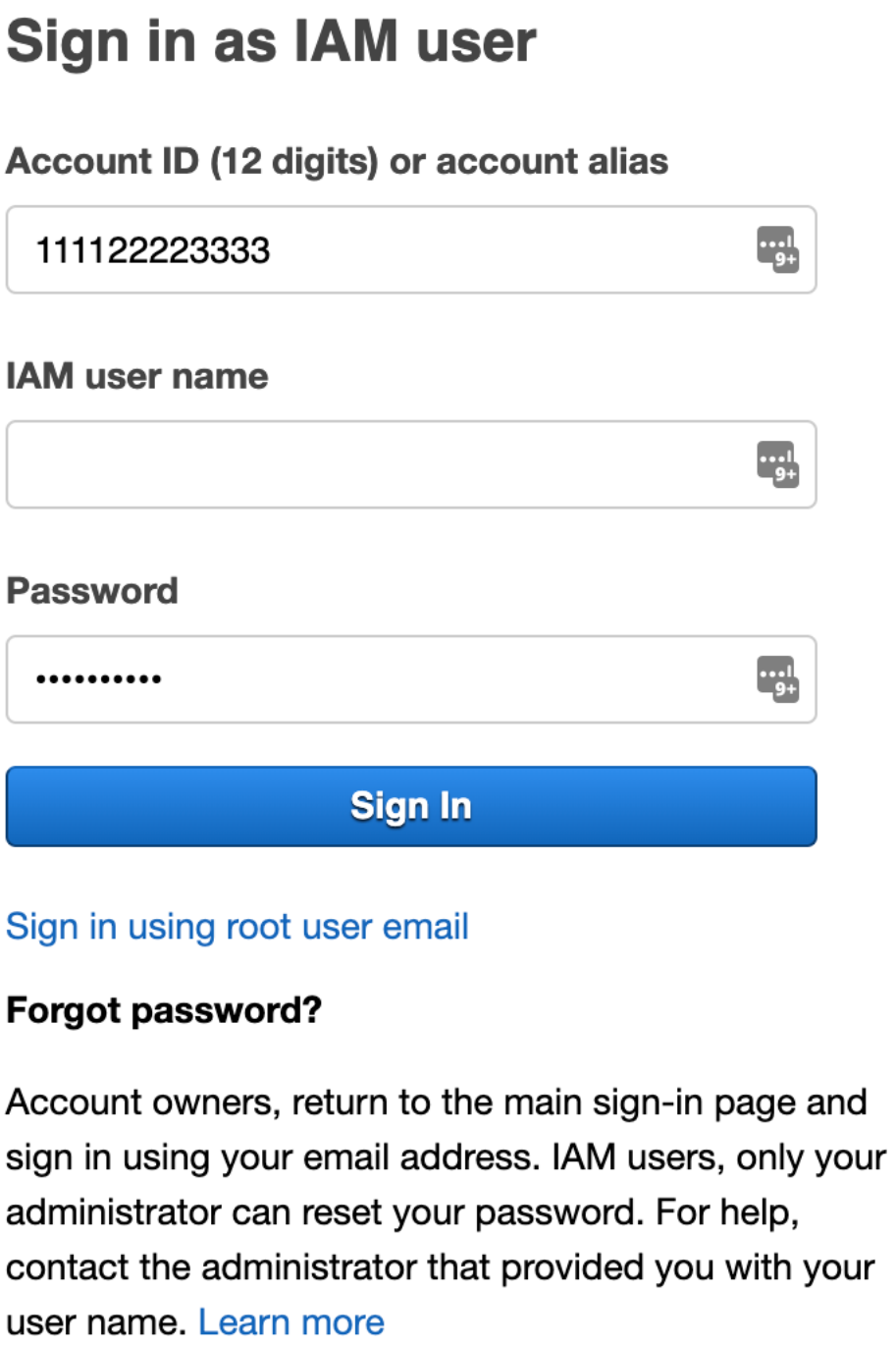
기본 로그인 페이지로 돌아가려면 다른 계정으로 로그인을 선택합니다.

루트 사용자 암호를 잊어버린 경우 암호가 생각나지 않는 경우를 선택하여 재설정합니다. 암호 재설정에 대한 자세한 내용은 분실하거나 잊어버린 암호 또는 액세스 키 재설정 (p. 118) 단원을 참조하십시오.

IAM 사용자 로그인 페이지

IAM 사용자 로그인 페이지에 액세스하려면 기본 로그인 페이지에서 IAM user(IAM 사용자)를 선택하고 계정 ID 또는 별칭을 입력합니다. 그러고 나서 Next(다음)를 선택하여 이 페이지에서 IAM 사용자 이름과 암호를 입력할 수 있습니다.

IAM 로그인 페이지



기본 로그인 페이지로 돌아가려면 Sign-in using 루트 사용자 email(루트 이메일을 사용하여 로그인)을 선택합니다.

IAM 암호를 잊어버린 경우 재설정할 수 없습니다. IAM 관리자만 암호를 재설정할 수 있습니다. 암호 재설정에 대한 자세한 내용은 잊거나 분실한 루트 사용자 암호 재설정 (p. 119) 단원을 참조하십시오.

AWS Management 콘솔을 사용하려면 IAM 사용자는 사용자 이름과 암호 이외에 계정 ID 또는 계정 별칭을 제공해야 합니다. 관리자로서 콘솔에서 IAM 사용자를 생성 (p. 88)하는 경우 사용자 이름과 계정 로그인 페이지 URL을 포함한 로그인 자격 증명을 해당 사용자에게 전송해야 합니다.

Important

IAM 사용자를 설정하는 방법에 따라 모든 사용자에게 첫 로그인용 임시 암호와 적절한 경우 MFA 디바이스를 제공합니다. 암호 및 MFA 디바이스에 대한 자세한 내용은 암호 관리 (p. 100) 및 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.

IAM 사용을 시작하면 고유한 계정 로그인 페이지 URL이 자동으로 생성됩니다. 이 로그인 페이지를 사용하기 위해 해야 할 작업은 전혀 없습니다.

```
https://My_AWS_Account_ID.signin.aws.amazon.com/console/
```

AWS 계정 ID 번호 대신 회사 이름(또는 다른 친숙한 식별자)을 URL에 포함하려는 경우 계정 로그인 URL을 사용자 지정할 수도 있습니다. 계정 별칭 만들기에 대한 자세한 내용은 AWS 계정 ID 및 별칭 (p. 77) 단원을 참조하십시오.

도움말

웹 브라우저에서 계정 로그인 페이지를 위한 북마크를 만들려면 북마크 입력란에 계정의 로그인 URL을 직접 입력해야 합니다. 리디렉션은 로그인 URL을 가릴 수 있으므로 웹 브라우저 북마크 기능을 사용하지 마십시오.

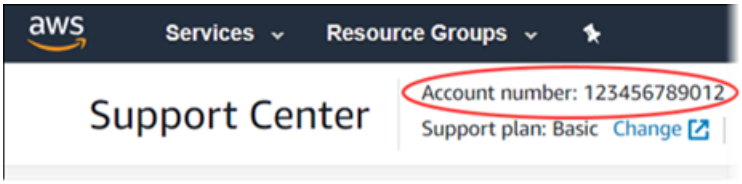
언제든지 IAM 콘솔의 대시보드에서 계정 로그인 페이지의 URL을 찾을 수 있습니다.

IAM 사용자는 다음의 일반 로그인 엔드포인트에서 로그인하고 계정 ID 또는 계정 별칭을 직접 입력할 수도 있습니다.

```
https://console.aws.amazon.com/
```

Note

AWS Management 콘솔에서 AWS 계정 ID 번호를 검색하려면 오른쪽 상단에 있는 탐색 모음에서 지원을 선택한 후 지원 센터를 선택합니다. 현재 로그인한 계정 번호(ID)는 지원 센터 제목 표시줄에 나타납니다.



사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 다음에 사용자가 AWS Management 콘솔의 아무 페이지로든 이동하면 콘솔이 쿠키를 사용하여 사용자를 사용자 로그인 페이지로 리디렉션합니다.

AWS Management 콘솔에 대한 사용자 액세스 제어

AWS Management 콘솔을 통해 AWS 계정에 로그인하는 권한이 있는 사용자는 AWS 리소스에 액세스할 수 있습니다. 다음 목록에서는 AWS Management 콘솔을 통해 AWS 계정 리소스에 대한 액세스 권한을 사용자에게 부여할 수 있는 방법을 보여 줍니다. 또한 사용자가 AWS 웹 사이트를 통해 다른 AWS 계정 기능에 액세스할 수 있는 방법도 보여 줍니다.

Note

IAM 사용은 무료입니다.

AWS Management 콘솔

AWS Management 콘솔에 액세스해야 하는 각 사용자에 대해 암호를 만듭니다. 사용자는 IAM 지원 AWS 계정 로그인 페이지를 통해 콘솔에 액세스합니다. 로그인 페이지 액세스에 대한 자세한 내용은 IAM 콘솔 및 로그인 페이지 (p. 71)를 참조하십시오. 암호 만들기에 대한 자세한 내용은 암호 관리 (p. 100)을 참조하십시오.

Amazon EC2 인스턴스, Amazon S3 버킷 등의 AWS 리소스

사용자에게 암호가 있더라도 AWS 리소스에 액세스하려면 권한이 필요합니다. 사용자를 만들 때 이 사용자에게는 기본적으로 권한이 없습니다. 사용자에게 필요한 권한을 부여하려면 해당 사용자에게 정책을 연결합니다. 같은 리소스로 같은 작업을 수행할 사용자가 많은 경우 해당 사용자를 그룹에 할당한 다음 이 그룹에 권한을 할당할 수 있습니다. 사용자 및 그룹 만들기에 대한 자세한 내용은 자격 증명(사용자, 그룹, 및 역할) (p. 83)을 참조하십시오. 권한 설정을 위한 정책 사용에 대한 자세한 내용은 액세스 관리 (p. 348)을 참조하십시오.

AWS 토론 포럼

누구나 AWS 토론 포럼에서 게시물을 읽을 수 있습니다. AWS 토론 포럼에 질문이나 의견을 게시하고자 하는 사용자는 자신의 사용자 이름을 사용하여 그렇게 할 수 있습니다. 사용자가 처음으로 AWS 토론 포럼에 게시하면 별칭과 이메일 주소를 입력하라는 메시지가 표시됩니다. 해당 사용자만 AWS 토론 포럼에서 해당 별칭을 사용할 수 있습니다.

AWS 계정 결제 및 사용 정보

AWS 계정 결제 및 사용 정보에 대한 액세스 권한을 사용자에게 부여할 수 있습니다. 자세한 내용은 AWS Billing and Cost Management 사용 설명서의 결제 정보에 대한 액세스 제어를 참조하십시오.

AWS 계정 프로필 정보

사용자는 계정 소유자의 AWS 계정 프로필 정보에 액세스할 수 없습니다.

AWS 계정 보안 자격 증명

사용자는 계정 소유자의 AWS 계정 보안 자격 증명에 액세스할 수 없습니다.

Note

IAM 정책은 인터페이스와 관계없이 액세스를 제어합니다. 예를 들어 AWS Management 콘솔에 액세스하기 위한 암호를 사용자에게 제공할 수 있습니다. 해당 사용자(또는 사용자가 속한 그룹)에 대한 정책은 사용자가 AWS Management 콘솔에서 수행할 수 있는 작업을 제어합니다. 또는 AWS에 대해 API 호출을 실행하기 위한 AWS 액세스 키를 사용자에게 제공할 수 있습니다. 이렇게 하면 인증을 위해 해당 액세스 키를 사용하는 라이브러리 또는 클라이언트를 통해 사용자가 호출할 수 있는 작업이 정책을 통해 제어됩니다.

AWS 계정 ID 및 별칭

계정 별칭은 계정의 웹 주소에서 계정 ID를 대신합니다. AWS Management 콘솔, AWS CLI 또는 AWS API에서 계정 별칭을 만들고 관리할 수 있습니다.

주제

AWS 계정 ID 찾기

계정 ID는 AWS Management 콘솔에서, 혹은 AWS CLI 또는 AWS API를 사용해 찾을 수 있습니다.

계정 ID 찾기(콘솔)

탐색 모음에서 지원을 선택한 후 지원 센터를 선택합니다. 현재 로그인한 12자리 계정 번호(ID)는 지원 센터 제목 표시줄에 나타납니다.

계정 ID 찾기(AWS CLI)

사용자 ID, 계정 ID 및 사용자 ARN을 보려면

- `aws sts get-caller-identity`

계정 ID 찾기(AWS API)

사용자 ID, 계정 ID 및 사용자 ARN을 보려면

- `GetCallerIdentity`

계정 별칭 정보

AWS 계정 ID 대신 회사 이름이나 기타 친숙한 식별자를 로그인 페이지의 URL에 포함하려는 경우 계정 별칭을 만들 수 있습니다. 이 섹션에서는 AWS 계정 별칭에 대한 정보를 제공하고 별칭을 만드는 데 사용하는 API 작업을 나열합니다.

로그인 페이지 URL의 형식은 기본적으로 다음과 같습니다.

```
https://Your_AWS_Account_ID.signin.aws.amazon.com/console/
```

AWS 계정 ID의 AWS 계정 별칭을 만드는 경우 로그인 페이지 URL이 다음 예제와 같습니다.

```
https://Your_Alias.signin.aws.amazon.com/console/
```

> **Note**
>
> AWS 계정 별칭을 만든 후에도 AWS 계정 ID를 포함하는 원래 URL은 활성 상태로 유지되며 사용할 수 있습니다.
>
> **도움말**
>
> 웹 브라우저에서 계정의 로그인 페이지를 위한 북마크를 만들려면 북마크 입력란에 로그인 URL을 직접 입력해야 합니다. 웹 브라우저의 "페이지 즐겨찾기" 기능을 사용하지 마십시오.

AWS 계정 별칭 만들기, 삭제 및 나열

AWS Management Console, IAM API 또는 명령줄 인터페이스를 사용하여 AWS 계정 별칭을 만들거나 삭제할 수 있습니다.

> **Important**
>
> - AWS 계정은 별칭을 하나만 가질 수 있습니다. AWS 계정의 새 별칭을 만들면 새 별칭이 이전 별칭을 덮어쓰며 이전 별칭을 포함하는 URL이 작동하지 않습니다.

- 계정 별칭은 모든 Amazon Web Services 제품에서 고유해야 하며, 숫자, 소문자 및 하이픈만 포함해야 합니다. AWS 계정 주체 제한에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569)을 참조하십시오.

별칭 생성 및 삭제(콘솔)

AWS Management 콘솔에서 계정 별칭을 만들고 삭제할 수 있습니다.

계정 별칭을 만들거나 제거하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 대시보드를 선택합니다.
3. IAM users sign-in link(IAM 사용자 로그인 링크)를 찾아 링크 오른쪽에 있는 사용자 지정을 선택합니다.
4. 별칭에 사용할 이름을 입력한 후 예, 생성을 선택합니다.
5. 별칭을 제거하려면 사용자 지정을 선택한 다음 예, 삭제합니다.를 선택합니다. 로그인 URL에 다시 AWS 계정 ID가 사용됩니다.

별칭 만들기, 삭제 및 나열(AWS CLI)

AWS Management 콘솔 로그인 페이지 URL의 별칭을 만들려면 다음 명령을 실행합니다.

- `aws iam create-account-alias`

AWS 계정 ID 별칭을 삭제하려면 다음 명령을 실행합니다.

- `aws iam delete-account-alias`

AWS 계정 ID 별칭을 표시하려면 다음 명령을 실행합니다.

- `aws iam list-account-aliases`

별칭 만들기, 삭제 및 나열(AWS API)

AWS Management 콘솔 로그인 페이지 URL의 별칭을 만들려면 다음 연산을 호출합니다.

- `CreateAccountAlias`

AWS 계정 ID 별칭을 삭제하려면 다음 연산을 호출합니다.

- `DeleteAccountAlias`

AWS 계정 ID 별칭을 표시하려면 다음 연산을 호출합니다.

- `ListAccountAliases`

IAM 로그인 페이지에 MFA 디바이스 사용

멀티 팩터 인증(MFA) (p. 119) 디바이스로 구성된 IAM 사용자는 자신의 MFA 디바이스를 사용하여 AWS Management 콘솔에 로그인해야 합니다. 사용자가 사용자 이름과 암호를 입력하면 AWS는 해당 사용자의

계정에서 해당 사용자에게 MFA가 필요한지 여부를 확인합니다. 다음 단원은 MFA가 필요할 때 사용자가 로그인을 완료하는 방법이 나와 있습니다.

주제

가상 MFA 디바이스로 로그인

MFA가 필요한 사용자에게는 두 번째 로그인 페이지가 나타납니다. MFA code(MFA 코드) 상자에 MFA 애플리케이션에서 제공한 숫자 코드를 입력해야 합니다.

MFA 코드가 올바르면 사용자는 AWS Management 콘솔에 액세스할 수 있습니다. 코드가 올바르지 않으면 다른 코드로 다시 시도할 수 있습니다.

가상 MFA 디바이스는 동기화되지 않을 수 있습니다. 여러 번 시도한 후에도 사용자가 AWS Management 콘솔에 로그인할 수 없으면 가상 MFA 디바이스를 동기화하라는 메시지가 표시됩니다. 사용자는 화면에 표시되는 메시지에 따라 가상 MFA 디바이스를 동기화할 수 있습니다. AWS 계정에 속한 사용자 대신 디바이스를 동기화할 수 있는 방법에 대한 자세한 내용은 가상 및 하드웨어 MFA 디바이스 재동기화 (p. 138)를 참조하십시오.

U2F 보안 키로 로그인

MFA가 필요한 사용자에게는 두 번째 로그인 페이지가 나타납니다. 사용자가 U2F 보안 키를 터치해야 합니다.

다른 MFA 디바이스와 달리 U2F 보안 키는 항상 동기화되어 있습니다. U2F 보안 키를 분실했거나 도난당한 경우 관리자가 비활성화할 수 있습니다. 자세한 내용은 MFA 디바이스 비활성화(콘솔) (p. 143) 단원을 참조하십시오.

U2F를 지원하는 브라우저 및 AWS를 지원하는 U2F 디바이스 정보는 U2F 보안 키 사용에 지원되는 구성 (p. 129)을 확인하십시오.

하드웨어 MFA 디바이스로 로그인

MFA가 필요한 사용자에게는 두 번째 로그인 페이지가 나타납니다. MFA code(MFA 코드) 상자에 하드웨어 MFA 디바이스에서 제공한 숫자 코드를 입력해야 합니다.

MFA 코드가 올바르면 사용자는 AWS Management 콘솔에 액세스할 수 있습니다. 코드가 올바르지 않으면 다른 코드로 다시 시도할 수 있습니다.

하드웨어 MFA 디바이스는 동기화되지 않을 수 있습니다. 여러 번 시도하여 실패한 후에도 사용자가 AWS Management 콘솔에 로그인할 수 없으면 MFA 토큰 디바이스를 동기화하라는 메시지가 표시됩니다. 사용자는 화면에 표시되는 메시지에 따라 MFA 토큰 디바이스를 동기화할 수 있습니다. AWS 계정에 속한 사용자 대신 디바이스를 동기화할 수 있는 방법에 대한 자세한 내용은 가상 및 하드웨어 MFA 디바이스 재동기화 (p. 138)를 참조하십시오.

IAM 콘솔 검색

IAM 관리 콘솔을 탐색하며 다양한 IAM 리소스를 관리할 때 액세스 키를 찾아야 하는 경우가 많습니다. 또는 깊이 중첩된 IAM 리소스를 탐색하여 필요한 항목을 찾아야 할 수도 있습니다. 보다 빠른 방법은 IAM 콘솔 검색 페이지를 사용하여 계정, IAM 자격 증명(예: 사용자, 그룹, 역할, 자격 증명 공급자), 이름별 정책 등을 찾는 것입니다.

IAM 콘솔 검색 기능으로 찾을 수 있는 항목은 다음과 같습니다.

- 검색 키워드(예: 사용자, 그룹, 역할, 자격 증명 공급자, 정책)와 일치하는 IAM 엔터티 이름
- 검색 키워드와 일치하는 AWS 문서 주제 이름
- 검색 키워드와 일치하는 작업

IAM 콘솔 검색 기능은 IAM Access Analyzer에 대한 정보를 반환하지 않습니다.

검색 결과의 각 행은 활성 링크입니다. 예를 들어 검색 결과에서 사용자 이름을 선택할 수 있습니다. 그러면 사용자 세부 정보 페이지로 이동합니다. 또는 예를 들어 사용자 만들기 활성 링크를 선택하여 사용자 생성 페이지로 이동할 수 있습니다.

> **Note**
>
> 액세스 키 검색에서는 검색 상자에 전체 액세스 키 ID를 입력해야 합니다. 검색 결과는 해당 키와 연결된 사용자를 보여줍니다. 여기에서 해당 사용자의 액세스 키를 관리할 수 있는 사용자 페이지로 이동할 수 있습니다.

IAM 콘솔 검색 사용

IAM의 검색 페이지를 사용하여 해당 계정과 관련된 항목을 찾습니다.

IAM 콘솔에서 항목을 검색하는 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 검색을 선택합니다.
3. 검색 상자에 검색 키워드를 입력합니다.
4. 검색 결과 목록에서 링크를 선택하여 콘솔 또는 문서의 해당 부분으로 이동합니다.

IAM 콘솔 검색 결과 내 아이콘

다음 아이콘은 검색으로 찾을 수 있는 항목의 유형을 식별합니다.

아이콘	설명
	IAM 사용자
	IAM 그룹
	IAM 역할
	IAM 정책
	"사용자 만들기" 또는 "정책 연결"과 같은 작업

아이콘	설명
	키워드 **delete**의 결과
	IAM 설명서

샘플 검색 문구

IAM 검색 시 다음과 같은 문구를 사용할 수 있습니다. 기울임꼴로 표시된 용어를 찾으려는 실제 IAM 사용자, 그룹, 역할, 액세스 키, 정책 또는 자격 증명 공급자의 이름으로 각각 대체합니다.

- ***user_name*** 또는 ***group_name*** 또는 ***role_name*** 또는 ***policy_name*** 또는 ***identity_provider_name***
- ***access_key***
- **add user *user_name* to groups** 또는 **add users to group *group_name***
- **remove user *user_name* from groups**
- **delete *user_name*** 또는 **delete *group_name*** 또는 **delete *role_name*** 또는 **delete *policy_name*** 또는 **delete *identity_provider_name***
- **manage access keys *user_name***
- **manage signing certificates *user_name***
- **users**
- **manage MFA for *user_name***
- **manage password for *user_name***
- **create role**
- **password policy**
- **edit trust policy for role *role_name***
- **show policy document for role *role_name***
- **attach policy to *role_name***
- **create managed policy**
- **create user**
- **create group**
- **attach policy to *group_name***
- **attach entities to *policy_name***
- **detach entities to *policy_name***
- **what is IAM**
- **how do I create an IAM user**
- **how do I use IAM console**
- **what is a user** 또는 **what is a group**, 또는 **what is a policy**, 또는 **what is a role**, 또는 **what is an identity provider**

자격 증명(사용자, 그룹, 및 역할)

이 섹션에서는 AWS 계정의 사용자와 프로세스에 대한 인증을 제공하기 위해 생성하는 IAM 자격 인증을 설명합니다. 이 섹션은 또한 한 단위로 관리할 수 있는 IAM 사용자 집합인 IAM 그룹에 대해서도 설명합니다. 자격 증명은 사용자를 대표하며, 인증된 후 AWS에서 작업을 수행할 수 있는 권한을 부여받습니다. 각 자격 증명은 1개 이상의 정책 (p. 348)과 연결되어 사용자, 역할 또는 그룹 구성원이 어떤 AWS 리소스로 어떤 조건에서 어떤 작업을 할지 결정할 수 있습니다.

AWS 계정 루트 사용자 (p. 331)

Amazon Web Services(AWS) 계정을 처음 생성하는 경우에는 전체 AWS 서비스 및 계정 리소스에 대해 완전한 액세스 권한을 지닌 단일 로그인 자격 증명으로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다.

> **Important**
>
> 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 않는 것이 좋습니다. 대신, IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례를 준수하십시오. 그런 다음 루트 사용자를 안전하게 보관해 두고 몇 가지 계정 및 서비스 관리 작업을 수행할 때만 자격 증명을 사용합니다. 루트 사용자로 로그인해야 하는 작업을 보려면 루트 사용자가 필요한 AWS 작업을 참조하십시오.

IAM 사용자 (p. 85)

IAM 사용자 (p. 85)는 AWS에서 만드는 엔터티입니다. IAM 사용자는 IAM 사용자를 사용하여 AWS와 상호 작용하는 사람 또는 서비스를 나타냅니다. IAM 사용자의 주된 용도는 대화형 작업을 위해 AWS Management 콘솔에 로그인하고 API 또는 CLI를 사용해 AWS 서비스로 프로그래밍 방식의 요청을 보내는 데 사용할 수 있는 능력을 사람들에게 제공하는 것입니다. AWS에서 사용자는 이름, AWS Management 콘솔에 로그인할 암호, 그리고 API 또는 CLI와 함께 사용할 수 있는 2개의 액세스 키로 이루어져 있습니다. IAM 사용자를 생성하는 경우, 그 사용자를 적절한 권한 정책이 연결된 그룹의 구성원으로 만들거나(이 방식을 추천함) 그 사용자에게 정책을 직접 연결하여 권한을 부여합니다. 기존 IAM 사용자의 권한을 복제하여 신규 사용자를 자동으로 같은 그룹의 구성원으로 만들고 동일한 정책을 모두 연결할 수도 있습니다.

IAM 그룹 (p. 167)

IAM 그룹 (p. 167)은 IAM 사용자들의 집합입니다. 그룹을 활용하면 사용자 모음에 대한 권한을 지정하여 해당 사용자에 대한 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 Admins라는 그룹을 만들어 일반적으로 관리자에게 필요한 유형의 권한을 부여할 수 있습니다. 이 그룹에 할당된 권한이 이 그룹에 속하는 모든 사용자에게 자동으로 부여됩니다. 관리자 권한을 필요로 하는 새로운 사용자가 조직에 들어올 경우 해당 사용자를 이 그룹에 추가하여 적절한 권한을 할당할 수 있습니다. 마찬가지로 조직에서 직원의 업무가 바뀌면 해당 사용자의 권한을 편집하는 대신 이전 그룹에서 해당 사용자를 제거한 후 적절한 새 그룹에 추가하면 됩니다. 그룹은 리소스 기반 정책 또는 신뢰 정책 (p. 372)에서 `Principal`로 식별될 수 없기 때문에 진정한 자격 증명이 아니라는 점에 유의하십시오. 그것은 다수의 사용자에게 한 번에 정책을 연결하는 방법일 뿐입니다.

IAM역할 (p. 174)

AWS에서 자격 증명이 할 수 있는 것과 없는 것을 결정하는 권한 정책을 갖춘 자격 증명이라는 점에서 IAM 역할 (p. 174)은 사용자와 아주 유사합니다. 그러나 역할은 그와 연관된 어떤 자격 증명(암호 또는 액세스

키)도 없습니다. 역할은 한 사람과만 연관되는 것이 아니라 그 역할이 필요한 사람이면 누구든지 맡을 수 있도록 고안되었습니다. IAM 사용자는 한 가지 역할을 맡음으로써 특정 작업을 위해 다른 권한을 임시로 얻을 수 있습니다. 역할은 IAM 대신에 외부 자격 증명 공급자를 사용해 로그인하는 연동 사용자 (p. 183)에게 할당될 수 있습니다. AWS는 자격 증명 공급자가 전달하는 세부 정보를 사용해 연동 사용자에게 어떤 역할을 매핑할지 결정합니다.

임시 자격 증명 (p. 302)

임시 자격 증명은 기본적으로 IAM 역할에 사용되지만 다른 용도로도 사용됩니다. 일반 IAM 사용자보다 제한된 권한을 갖는 임시 자격 증명을 요청할 수 있습니다. 이렇게 하면 제한된 자격 증명으로는 허용되지 않는 작업을 뜻하지 않게 수행하는 것을 방지할 수 있습니다. 임시 자격 증명의 장점은 설정한 기간이 지나면 자동으로 만료된다는 것입니다. 자격 증명의 유효 기간을 통제할 수 있습니다.

IAM 사용자를 만들어야 하는 경우(역할이 아님)

IAM 사용자는 계정에서 특정 권한을 갖는 자격 증명일 뿐이므로 자격 증명이 필요한 모든 경우를 위해 IAM 사용자를 만들 필요는 없습니다. 많은 경우 IAM 사용자와 연결된 장기 자격 증명 대신 IAM 역할과 그 역할들의 임시 보안 자격 증명을 활용할 수 있습니다.

- AWS 계정을 만들었는데 계정 내에 다른 사람이 없는 경우

  AWS 계정의 루트 사용자 자격 증명을 사용하여 AWS로 작업할 수 있지만 이 방법은 권장하지 않습니다. 그 대신 자신을 위한 IAM 사용자를 만들고 AWS로 작업할 때 해당 사용자의 자격 증명을 사용하실 것을 권합니다. 자세한 내용은 IAM 모범 사례 (p. 60) 단원을 참조하십시오.
- 그룹에 속한 다른 사람들이 AWS 계정에서 작업해야 하며 이 그룹이 다른 자격 증명 메커니즘을 사용하고 있지 않는 경우

  AWS 리소스에 액세스해야 하는 사람 각자에 대해 IAM 사용자를 만들어 각 사용자에게 적절한 권한을 할당하고 고유한 자격 증명을 부여합니다. 다수의 사용자들이 자격 증명을 공유하는 일이 절대 없도록 해주십시오.

IAM 역할을 만들어야 하는 경우(사용자가 아님)

다음 상황에서 IAM 역할을 만듭니다.

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 실행되는 애플리케이션을 만들고 그 애플리케이션이 AWS로 요청을 보내는 경우.

IAM 사용자를 만들어 해당 사용자의 자격 증명을 애플리케이션에 전달하거나 자격 증명을 애플리케이션에 포함하지 않습니다. 대신 EC2 인스턴스에 연결하는 IAM 역할을 생성하여 인스턴스에서 실행되는 애플리케이션에 임시 보안 자격 증명을 부여하십시오. 애플리케이션이 AWS에서 이러한 자격 증명을 사용하면 역할에 연결된 정책에서 허용하는 모든 작업을 수행할 수 있습니다. 세부 정보는 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265) 단원을 참조하십시오.

휴대폰에서 실행되는 앱을 만들고 그 앱이 AWS로 요청을 보내는 경우

IAM 사용자를 만들어 앱을 통해 해당 사용자의 액세스 키를 배포하지 않습니다. 대신 Login with Amazon, Amazon Cognito, Facebook 또는 Google과 같은 자격 증명 공급자를 사용하여 사용자를 인증한 다음 사용자를 IAM 역할에 매핑하십시오. 앱은 역할을 사용함으로써 역할에 연결된 정책에 의해 지정된 권한을 갖는 임시 보안 자격 증명을 얻을 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- Android용 AWS Mobile SDK Developer Guide의 Amazon Cognito 개요

- AWS Mobile SDK for iOS Developer Guide의 Amazon Cognito 개요
- 웹 자격 증명 연동에 대하여 (p. 183)

회사의 사용자들이 기업 네트워크에서 인증을 받았는데 다시 로그인하지 않고도 AWS를 사용할 수 있기를 원합니다. 즉, 사용자들이 AWS로 연동되도록 허용하고 싶습니다.

IAM 사용자는 만들지 마십시오. 엔터프라이즈 자격 증명 시스템과 AWS 사이의 연동 관계를 구성하십시오. 두 가지 방법으로 수행할 수 있습니다.

- 회사의 자격 증명 시스템이 SAML 2.0과 호환된다면 회사의 자격 증명 시스템과 AWS 간에 신뢰를 구축할 수 있습니다. 자세한 내용은 SAML 2.0 기반 연동에 대하여 (p. 188) 단원을 참조하십시오.
- 사용자의 엔터프라이즈 자격 증명을 임시 AWS 보안 자격 증명을 제공하고 IAM 역할로 변환하는 사용자 지정 프록시 서버를 만들고 사용하십시오. 자세한 내용은 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210)를 참조하십시오.

IAM 사용자

AWS Identity and Access Management(IAM) 사용자는 AWS에서 생성하는 엔터티로서 AWS와 상호 작용하기 위해 그 엔터티를 사용하는 사람 또는 애플리케이션을 나타냅니다. AWS에서 사용자는 이름과 자격 증명으로 구성됩니다.

관리자 권한을 가진 IAM 사용자는 AWS 계정 루트 사용자와 같은 것이 아닙니다. 루트 사용자에 대한 자세한 정보는 AWS 계정 루트 사용자 (p. 331) 단원을 참조하십시오.

Important

애플리케이션이나 웹 사이트에 Amazon Advertising을 활성화하려는 중에 이 페이지로 오게 된 경우, Product Advertising API 구독 단원을 참조하십시오.

AWS가 IAM 사용자를 식별하는 방법

사용자를 생성하면 IAM이 그 사용자를 식별하기 위한 방법을 다음과 같이 생성합니다.

- 사용자 생성시 지정한 이름으로서 `Richard` 또는 `Anaya`와 같은 사용자가 "쉽게 알 수 있는 이름"입니다. 이 이름들은 AWS Management 콘솔에서 볼 수 있습니다.
- 사용자의 Amazon 리소스 이름(ARN)입니다. 모든 AWS 전반에 사용자를 특별하게 식별할 필요가 있는 경우 ARN을 사용합니다. 예를 들어, ARN을 사용하여 사용자를 Amazon S3 버킷에 대한 IAM 정책에서 `Principal`로서 지정할 수 있습니다. IAM 사용자의 ARN은 다음과 같은 모습입니다.

  `arn:aws:iam::`*`account-ID-without-hyphens`*`:user/Richard`
- 사용자의 고유 식별자입니다. 이 ID는 사용자를 생성하기 위해 API, Windows PowerShell용 도구 또는 AWS CLI를 사용할 때만 반환됩니다. 콘솔에서는 이 ID를 볼 수 없습니다.

이 식별자에 대한 자세한 정보는 IAM 식별자 (p. 563) 단원을 참조하십시오.

사용자 및 자격 증명

AWS는 사용자 자격 증명에 따라 다양한 방법으로 액세스할 수 있습니다.

- 콘솔 암호 (p. 100): 사용자가 입력해 AWS Management 콘솔과 같은 상호 작용 세션으로 로그인할 수 있는 암호.
- 액세스 키 (p. 111): 액세스 키 ID와 보안 액세스 키의 조합입니다. 한 사용자에게 한 번에 두 개를 지정할 수 있습니다. 이것들은 AWS를 프로그래밍 방식으로 호출하는 데 사용될 수 있습니다. 예를 들어, AWS

CLI 또는 AWS PowerShell 도구를 사용할 때 코드 또는 명령 프롬프트에 대한 API를 사용할 경우 액세스 키를 사용할 수 있습니다.

- CodeCommit용 SSH 키 (p. 160): CodeCommit를 사용한 인증에 사용할 수 있는 OpenSSH 형식의 SSH 퍼블릭 키.
- 서버 인증서 (p. 163): 일부 AWS 서비스를 사용한 인증에 사용할 수 있는 SSL/TLS 인증서. 서버 인증서를 프로비저닝 및 관리하고 배포할 때 AWS Certificate Manager(ACM)을 사용하는 것이 좋습니다. ACM에서 지원되지 않는 리전에서 HTTPS 연결을 지원해야 하는 경우에만 IAM을 사용합니다. ACM을 지원하는 리전을 알아보려면 AWS General Reference의 AWS Certificate Manager 리전 및 엔드포인트를 참조하십시오.

IAM 사용자에게 적절한 자격 증명을 선택할 수 있습니다. AWS Management 콘솔을 사용하여 사용자를 생성할 때 최소한 콘솔 암호 또는 액세스 키를 포함하도록 선택해야 합니다. 기본적으로 AWS CLI 또는 AWS API를 사용하여 새로 생성된 IAM 사용자는 어떤 종류의 자격 증명도 보유하지 않습니다. 사용자의 요구 사항을 기반으로 IAM 사용자에 대한 자격 증명의 유형을 생성해야 합니다.

다음 옵션을 이용해 암호, 액세스 키 및 MFA 디바이스를 관리하십시오.

- IAM 사용자 암호 관리 (p. 100). AWS Management 콘솔에 대한 액세스를 허용하는 암호를 생성 및 변경합니다. 암호 정책을 최소 암호 복잡성을 적용하도록 설정 사용자에게 자신의 암호를 변경할 수 있도록 허용
- IAM 사용자의 액세스 키 관리 (p. 111). 계정의 리소스에 대한 프로그래밍 방식의 액세스를 위해 액세스 키를 생성하고 업데이트합니다.
- 사용자에 대해 멀티 팩터 인증(MFA) (p. 119)을 활성화하여 해당 사용자 자격 증명의 보안을 강화할 수 있습니다. MFA를 사용할 경우 사용자는 두 가지 형식의 식별이 가능합니다. 먼저, 사용자는 자격 증명(암호 또는 액세스 키)의 일부분인 자격 증명을 제공합니다. 또한, 하드웨어 디바이스에서나 스마트폰 또는 태블릿의 애플리케이션을 통해서 생성된 또는 SMS 호환성 모바일 디바이스로 AWS가 보낸 임시 숫자 코드를 제공해야 합니다.
- 미사용 암호 및 액세스 키 찾기 (p. 154). 계정 또는 계정 내 IAM 사용자에 대한 암호 또는 액세스 키를 보유하는 사람은 누구든지 AWS 리소스에 대한 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 암호와 액세스 키가 필요하지 않을 때 그것들을 제거하는 것입니다.
- 계정의 자격 증명 보고서 다운로드 (p. 156). 계정의 모든 IAM 사용자와 암호, 액세스 키, MFA 디바이스를 포함하여 이들의 자격 증명 상태를 나열하는 자격 증명 보고서를 생성하고 다운로드할 수 있습니다. 암호와 액세스 키의 경우 자격 증명 보고서를 통해 암호 또는 액세스 키가 언제 마지막으로 사용되었는지 알 수 있습니다.

사용자 및 권한

기본적으로 신규 IAM 사용자는 어떤 작업도 할 수 있는 권한 (p. 348)이 없습니다. 사용자는 AWS 작업을 수행하거나 AWS 리소스에 액세스할 수 있는 권한이 없습니다. 개별 IAM 사용자를 두면 각 사용자에게 개별적으로 권한을 할당할 수 있다는 장점이 있습니다. 사용자 몇 명에게 관리 권한을 할당하면 이들이 AWS 리소스를 관리하고 다른 IAM 사용자까지 생성하고 관리할 수 있습니다. 그러나 대부분의 경우 사용자의 업무에 필요한 작업(AWS 작업)과 리소스로 사용자의 권한을 제한합니다.

Diego라는 사용자가 있다고 가정해 보겠습니다. IAM 사용자 `Diego`를 생성하면 그 사용자의 암호를 생성할 수 있습니다. 특정 Amazon EC2 인스턴스를 시작하고(`GET`) 정보를 Amazon RDS 데이터베이스의 테이블에서 읽을 수 있도록 IAM 사용자에게 권한을 부여합니다. 사용자를 생성하여 초기 자격 증명과 권한을 부여하는 절차는 AWS 계정의 IAM 사용자 생성 (p. 87) 단원을 참조하십시오. 기존 사용자에 대한 권한을 변경하는 절차는 IAM 사용자의 권한 변경 (p. 96) 단원을 참조하십시오. 사용자의 암호나 액세스 키를 변경하는 절차는 암호 관리 (p. 100) 및 IAM 사용자의 액세스 키 관리 (p. 111) 단원을 참조하십시오.

사용자에게 권한 경계를 추가할 수 있습니다. 권한 경계는 AWS 관리형 정책을 사용하여 자격 증명 기반 정책이 사용자 또는 역할에 부여할 수 있는 최대 권한을 제한할 수 있는 고급 기능입니다. 정책 유형 및 활용에 대한 자세한 정보는 정책 및 권한 (p. 349) 단원을 참조하십시오.

사용자 및 계정

각 IAM 사용자는 오직 한 개의 AWS 계정과만 연결됩니다. 사용자는 AWS 계정 내에서 정의되기 때문에 AWS에서 파일에 결제 방법을 저장해 두지 않아도 됩니다. 계정에 속한 사용자가 수행하는 모든 AWS 활동은 해당 계정으로 청구됩니다.

AWS 계정에서 보유할 수 있는 IAM 사용자 수는 제한되어 있습니다. 자세한 정보는 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

서비스 계정인 사용자

IAM 사용자는 연결된 자격 증명 및 권한을 지닌 IAM의 리소스입니다. IAM 사용자는 자격 증명을 사용하여 AWS 요청을 생성하는 사용자 또는 애플리케이션을 나타낼 수 있습니다. 이를 일반적으로 서비스 계정이라 합니다. 애플리케이션에 있는 IAM 사용자의 장기 자격 증명을 사용하기로 선택한 경우 액세스 키를 애플리케이션 코드에 직접 포함시키지 마십시오. AWS SDK 및 AWS Command Line Interface를 사용하면 코드에서 유지할 필요가 없도록 알려진 위치에 액세스 키를 추가할 수 있습니다. 자세한 정보는 AWS General Reference의 적절하게 IAM 사용자 액세스 키 관리 단원을 참조하십시오. 또는 모범 사례로서 장기 액세스 키 대신 임시 보안 자격 증명(IAM 역할)을 사용할 수 있습니다.

AWS 계정의 IAM 사용자 생성

Follow us on Twitter

AWS 계정에서 하나 이상의 IAM 사용자를 만들 수 있습니다. 팀에 새로 합류하는 사람이 있거나 AWS에 대한 API 호출이 필요한 새 애플리케이션을 생성할 때 IAM 사용자를 생성할 수 있습니다.

> **Important**
>
> 애플리케이션이나 웹 사이트에 Amazon 광고를 설정하는 동안 이 페이지로 오게 된 경우, Product Advertising API 개발자 되기 단원을 참조하십시오.
> IAM 콘솔에서 이 페이지로 이동했을 경우 로그인을 했더라도 계정에 IAM 사용자가 포함되지 않을 수 있습니다. 역할을 사용하거나, 임시 자격 증명으로 로그인하여 AWS 계정 루트 사용자로 로그인할 수 있습니다. 이러한 IAM 자격 증명에 대한 자세한 내용은 자격 증명(사용자, 그룹, 및 역할) (p. 83) 단원을 참조하십시오.

주제

다음 단계에 따라 사용자를 생성하고 사용자가 작업을 수행할 수 있습니다.

1. AWS Management 콘솔, AWS CLI, Windows PowerShell용 도구 또는 AWS API 작업을 사용하여 사용자를 생성합니다. AWS Management 콘솔에서 사용자를 생성하면, 자신의 선택에 따라 1–4단계는 자동으로 처리됩니다. 프로그래밍 방식으로 사용자를 생성하는 경우, 각 단계를 개별적으로 수행해야 합니다.
2. 사용자에게 필요한 액세스 유형에 따라 사용자의 자격 증명을 생성합니다.
   - 프로그래밍 방식으로 액세스: IAM 사용자가 API를 호출해야 하거나, AWS CLI 또는 Windows PowerShell용 도구을 사용해야 할 수 있습니다. 이 경우 해당 사용자의 액세스 키를 만드십시오(액세스 키 ID 및 보안 액세스 키).
   - AWS Management 콘솔 액세스: 사용자가 AWS Management 콘솔에서 액세스해야 할 경우, 에서 해당 사용자의 암호를 생성합니다 (p. 104).

   사용자가 필요한 자격 증명만 생성하는 것이 가장 좋습니다. 예를 들어, AWS Management 콘솔을 통해서만 액세스해야 하는 사용자에게는 액세스 키를 생성해서는 안 됩니다.
3. 해당 사용자를 하나 이상의 그룹에 추가하여 필요한 작업을 수행할 수 있는 권한을 부여합니다. 권한 정책을 사용자에게 직접 연결하여 권한을 부여할 수 있습니다. 하지만, 사용자를 그룹에 추가한 후 그 그룹에

연결된 정책을 통해 정책과 권한을 관리하는 것이 좋습니다. 권한 경계 (p. 363)를 사용하여 일반적이지는 않지만 사용자에게 있는 권한을 제한할 수 있습니다.

4. (선택 사항) 태그를 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서의 태그 사용에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
5. 사용자에게 필요한 로그인 정보를 제공합니다. 여기에는 암호를 비롯해 사용자가 자격 증명을 제공하는 계정 로그인 웹 페이지의 콘솔 URL이 포함됩니다. 자세한 내용은 IAM 사용자가 AWS에 로그인하는 방법 (p. 91) 단원을 참조하십시오.
6. (선택 사항) 사용자에 대한 멀티 팩터 인증(MFA) (p. 119)을 구성합니다. MFA의 경우, 사용자가 AWS Management 콘솔에 로그인할 때마다 일회용 코드를 입력해야 합니다.
7. (선택 사항) 사용자에게 자신의 보안 자격 증명을 관리할 권한을 부여합니다. (기본적으로 사용자는 자신의 자격 증명을 관리할 권한이 없습니다.) 자세한 내용은 IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108) 단원을 참조하십시오.

사용자를 생성하기 위해 필요한 권한에 대한 자세한 내용은 IAM 리소스에 액세스하는 데 필요한 권한 (p. 507) 단원을 참조하십시오.

IAM 사용자 생성(콘솔)

AWS Management 콘솔을 사용하여 IAM 사용자를 생성할 수 있습니다.

한 명 이상의 IAM 사용자를 생성하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자와 Add user(사용자 추가)를 차례로 선택합니다.
3. 신규 사용자의 사용자 이름을 입력합니다. 이것은 AWS에 로그인할 때 사용하는 이름입니다. 하나 이상의 사용자를 동시에 추가하려면, 추가하는 각 사용자에 대해 Add another user(다른 사용자 추가)를 선택한 후 사용자 이름을 입력합니다. 한 번에 최대 10명까지 사용자를 추가할 수 있습니다.

   Note

   사용자 이름에는 최대 64개의 문자, 숫자 및 더하기(+), 등호(=), 쉼표(,), 마침표(.), 앳(@) 및 하이픈(-) 조합을 사용할 수 있습니다. 이름은 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어 "TESTUSER"와 "testuser"라는 두 사용자를 만들 수는 없습니다. IAM 엔터티 관련 제한에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.
4. 이 사용자 세트에게 부여할 액세스 권한의 유형을 선택합니다. 프로그래밍 방식 액세스나 AWS Management 콘솔에 대한 액세스 또는 둘 다를 선택할 수 있습니다.

   - 사용자가 API, AWS CLI, 또는 Windows PowerShell용 도구에 대한 액세스 권한이 필요한 경우, Programmatic access(프로그래밍 방식 액세스)를 선택합니다. 이렇게 하면 각 사용자에 대한 액세스 키가 생성됩니다. 최종(Final) 페이지에 이르면 액세스 키를 보거나 다운로드할 수 있습니다.
   - 사용자에게 AWS Management 콘솔에 대한 액세스 권한이 필요한 경우, AWS Management 콘솔 access(콘솔 액세스)를 선택합니다. 이렇게 하면 각 신규 사용자에 대한 암호가 생성됩니다.

   a. 콘솔 암호의 경우 다음 중 하나를 선택합니다.

      - Autogenerated password(자동 생성된 비밀 번호). 각 사용자는 유효한 계정 암호 정책(있는 경우)에 따라 임의로 생성되는 암호를 받습니다. Final(최종) 페이지에 이르면 암호를 보거나 다운로드할 수 있습니다.
      - Custom password(사용자 지정 비밀 번호). 입력란에 입력하는 암호가 각 사용자에게 할당됩니다.

   b. (선택 사항) 암호 재설정 필요를 선택하여 사용자가 처음 로그인할 때 의무적으로 암호를 변경하도록 설정하는 것이 바람직합니다.

Note

Allow users to change their own password(사용자 자신의 암호 변경 허용)으로 설정된 계정 수준 암호 정책을 활성화하지 않은 경우, Require password reset(암호 재설정 필요)를 선택하면 자신의 암호를 변경할 수 있는 권한을 부여하는 `IAMUserChangePassword`라는 AWS 관리형 정책이 신규 사용자에게 자동 연결됩니다.

5. Next: Permissions(다음: 권한)을 선택합니다.
6. 권한 설정 페이지에서 이 신규 사용자 세트에 권한을 할당하는 방식을 지정합니다. 다음 세 가지 옵션 중 하나를 선택합니다.

   - Add user to group(그룹에 사용자 추가). 이미 권한 정책을 보유한 하나 이상의 그룹에 사용자를 할당하고자 하는 경우, 이 옵션을 선택합니다. IAM에 계정 그룹의 목록이 연결된 정책과 함께 표시됩니다. 기존의 보안 그룹을 한 개 이상 선택하거나 그룹 생성을 선택하여 새 그룹을 만들 수 있습니다. 자세한 내용은 IAM 사용자의 권한 변경 (p. 96) 단원을 참조하십시오.
   - Copy permissions from existing user(기존 사용자에서 권한 복사). 이 옵션을 선택하여 그룹 멤버십, 연결된 관리형 정책, 포함된 인라인 정책 및 기존 권한 경계 (p. 363)를 기존 사용자에게서 신규 사용자로 모두 복사합니다. IAM는 계정에 속한 사용자 목록을 보여줍니다. 보유한 권한이 새로운 사용자의 요구 사항과 가장 근접하는 사용자를 선택합니다.
   - Attach existing policies to user directly(기존 정책을 사용자에게 직접 연결). 이 옵션을 선택하여 계정의 AWS 관리형 또는 사용자 관리형 정책 목록을 봅니다. 신규 사용자에게 연결하려는 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 절차의 4단계 단원을 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아와 신규 사용자에게 정책을 추가합니다. 그 대신에 그룹에 정책을 연결한 다음, 사용자들을 적절한 그룹의 구성원으로 만드는 것이 바람직한 모범 사례 (p. 61)입니다.
7. (선택 사항) 권한 경계 (p. 363)로서 설정됨. 이는 고급 기능입니다.

   Set permissions boundary(권한 경계 설정) 섹션을 열고 Use a permissions boundary to control the maximum user permissions(최대 사용자 권한을 관리하기 위한 권한 경계 사용)을 선택합니다. IAM은 계정의 AWS 관리형 또는 사용자 관리형 정책 목록을 보여줍니다. 권한 경계를 사용하기 위한 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 절차의 4단계 단원을 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아와 권한 경계에 사용할 정책을 선택합니다.
8. Next: Tags(다음: 태그)를 선택합니다.
9. (선택 사항) 태그를 키-값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서의 태그 사용에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
10. Next: Review(다음: 검토)를 선택하여 이 시점까지 한 선택을 모두 확인합니다. 계속 진행할 준비가 되었으면 Create user를 선택합니다.
11. 사용자의 액세스 키(액세스 키 ID와 보안 액세스 키)를 보려면 보고 싶은 각 암호와 액세스 키 옆에 있는 표시를 선택합니다. 액세스 키를 저장하려면 Download .csv(csv 다운로드)를 선택한 후 안전한 위치에 파일을 저장합니다.

    Important

    보안 액세스 키는 이 때만 확인 및 다운로드가 가능하기 때문에 사용자에게 AWS API를 사용하도록 하려면 이 정보를 제공해야 합니다. 사용자의 새 액세스 키 ID와 보안 액세스 키를 안전한 장소에 보관하십시오. 이 단계 이후에는 보안 키에 다시 액세스할 수 없습니다.
12. 각 사용자에게 해당 자격 증명을 제공합니다. 최종 페이지에서 각 사용자 옆에 있는 Send email(이메일 전송)을 선택합니다. 로컬 메일 클라이언트는 사용자 지정을 거쳐 발송할 수 있는 초안 형태로 열립니다. 이메일 템플릿에는 각 사용자에 대한 세부 정보가 다음과 같이 포함되어 있습니다.

    - 사용자 이름
    - 계정 로그인 페이지의 URL. 다음 예를 사용하여 정확한 계정 ID 번호 또는 계정 별칭으로 대치합니다.

```
https://AWS-account-ID or alias.signin.aws.amazon.com/console
```

자세한 내용은 IAM 사용자가 AWS에 로그인하는 방법 (p. 91) 단원을 참조하십시오.

Important

생성된 이메일에는 사용자 암호가 포함되어 있지 않습니다. 고객에게 보내는 이메일은 소속된 조직의 보안 지침을 준수하는 방식으로 제공되어야 합니다.

IAM 사용자 만들기(AWS CLI)

AWS CLI를 사용하여 IAM 사용자를 생성할 수 있습니다.

IAM 사용자를 생성하려면(AWS CLI)

1. 사용자를 생성합니다.
   - aws iam create-user
2. (선택 사항) 사용자에게 AWS Management 콘솔에 대한 액세스 권한 부여. 이를 위해서는 암호가 필요합니다. 또한 사용자에게 계정 로그인 페이지의 URL (p. 91)도 제공해야 합니다.
   - aws iam create-login-profile
3. (선택 사항) 사용자에게 프로그래밍 방식 액세스 권한 부여. 이를 위해서는 액세스 키가 필요합니다.
   - aws iam create-access-key
   - Windows PowerShell용 도구: New-IAMAccessKey
   - IAM API: CreateAccessKey

   Important

   보안 액세스 키는 이 때만 확인 및 다운로드가 가능하기 때문에 사용자에게 AWS API를 사용하도록 하려면 이 정보를 제공해야 합니다. 사용자의 새 액세스 키 ID와 보안 액세스 키를 안전한 장소에 보관하십시오. 이 단계 이후에는 보안 키에 다시 액세스할 수 없습니다.
4. 사용자를 하나 이상의 그룹에 추가합니다. 지정하는 그룹에는 사용자에게 적절한 권한을 부여하는 연결된 정책이 있어야 합니다.
   - aws iam add-user-to-group
5. (선택 사항) 사용자 권한을 정의한 정책을 사용자에게 추가합니다. 주의:사용자에게 직접 정책을 추가하는 대신 그룹에 사용자를 추가하고 그 그룹에 정책을 추가하여 사용자 권한을 관리하시는 것이 좋습니다.
   - aws iam attach-user-policy
6. (선택 사항) 태그를 연결하여 사용자 지정 속성을 사용자에게 추가합니다. 자세한 내용은 IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API) (p. 293) 단원을 참조하십시오.
7. (선택 사항) 사용자에게 자신의 보안 자격 증명을 관리할 수 있는 권한을 부여합니다. 자세한 내용은 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391) 단원을 참조하십시오.

IAM 사용자 만들기(AWS API)

AWS API를 사용하여 IAM 사용자를 생성할 수 있습니다.

(AWS API)에서 IAM 사용자를 생성하려면

1. 사용자를 생성합니다.

   - CreateUser
2. (선택 사항) 사용자에게 AWS Management 콘솔에 대한 액세스 권한 부여. 이를 위해서는 암호가 필요합니다. 또한 사용자에게 계정 로그인 페이지의 URL (p. 91)도 제공해야 합니다.

   - CreateLoginProfile
3. (선택 사항) 사용자에게 프로그래밍 방식 액세스 권한 부여. 이를 위해서는 액세스 키가 필요합니다.

   - CreateAccessKey

     Important

     보안 액세스 키는 이 때만 확인 및 다운로드가 가능하기 때문에 사용자에게 AWS API를 사용하도록 하려면 이 정보를 제공해야 합니다. 사용자의 새 액세스 키 ID와 보안 액세스 키를 안전한 장소에 보관하십시오. 이 단계 이후에는 보안 키에 다시 액세스할 수 없습니다.
4. 사용자를 하나 이상의 그룹에 추가합니다. 지정하는 그룹에는 사용자에게 적절한 권한을 부여하는 연결된 정책이 있어야 합니다.

   - AddUserToGroup
5. (선택 사항) 사용자 권한을 정의한 정책을 사용자에게 추가합니다. 주의:사용자에게 직접 정책을 추가하는 대신 그룹에 사용자를 추가하고 그 그룹에 정책을 추가하여 사용자 권한을 관리하시는 것이 좋습니다.

   - AttachUserPolicy
6. (선택 사항) 태그를 연결하여 사용자 지정 속성을 사용자에게 추가합니다. 자세한 내용은 IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API) (p. 293) 단원을 참조하십시오.
7. (선택 사항) 사용자에게 자신의 보안 자격 증명을 관리할 수 있는 권한을 부여합니다. 자세한 내용은 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391) 단원을 참조하십시오.

IAM 사용자가 AWS에 로그인하는 방법

IAM 사용자로 AWS Management 콘솔에 로그인하려면 사용자 이름과 암호 이외에 계정 ID 또는 계정 별칭을 제공해야 합니다. 관리자가 콘솔에서 IAM 사용자를 만든 경우 (p. 88), 계정 ID 또는 계정 별칭이 포함된 계정 로그인 페이지 URL과 사용자 이름 등 로그인 자격 증명이 전송되었어야 합니다.

```
https://My_AWS_Account_ID.signin.aws.amazon.com/console/
```

도움말

웹 브라우저에서 계정 로그인 페이지를 위한 북마크를 만들려면 북마크 입력란에 계정의 로그인 URL을 직접 입력해야 합니다. 리디렉션은 로그인 URL을 가릴 수 있으므로 웹 브라우저 북마크 기능을 사용하지 마십시오.

다음의 일반 로그인 엔드포인트에서 로그인하고 계정 ID 또는 계정 별칭을 직접 입력할 수도 있습니다.

```
https://console.aws.amazon.com/
```

사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 다음에 사용자가 AWS Management 콘솔의 아무 페이지로든 이동하면 콘솔이 쿠키를 사용하여 사용자를 사용자 로그인 페이지로 리디렉션합니다.

IAM 사용자 자격 증명에 첨부되는 정책에서 관리자가 지정하는 AWS 리소스에만 액세스할 수 있습니다. 콘솔에서 작업하려면 AWS 리소스 나열 및 생성 등 콘솔이 수행하는 작업을 수행할 권한이 있어야 합니다. 자세한 내용은 액세스 관리 (p. 348) 및 IAM 자격 증명 기반 정책 예제 (p. 387) 단원을 참조하십시오.

Note

조직에 기존의 자격 증명 시스템이 있는 경우, Single Sign-On(SSO) 옵션을 만드는 것이 좋습니다. SSO는 AWS Management 콘솔 사용자 자격 증명이 없어도 계정의 IAM에 액세스할 수 있는 권한을 사용자에게 제공합니다. 또한 SSO를 사용하면 사용자가 조직의 사이트와 AWS에 따로 로그인하지 않아도 됩니다. 자세한 내용은 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.

CloudTrail의 로그인 세부 정보 기록

CloudTrail에서 로그인 이벤트를 사용자 로그에 기록하도록 설정할 경우 CloudTrail에서 이벤트를 기록할 위치를 어떻게 선택하는지 잘 이해할 필요가 있습니다.

- 사용자가 콘솔에 직접 로그인할 경우 선택한 서비스 콘솔이 리전을 지원하는지 여부를 기준으로 글로벌 또는 리전 로그인 종단점으로 리디렉션됩니다. 예를 들어 메인 콘솔 홈 페이지는 리전을 지원합니다. 따라서 다음 URL에 로그인할 경우

```
https://alias.signin.aws.amazon.com/console
```

`https://us-east-2.signin.aws.amazon.com`과 같은 리전 로그인 종단점으로 리디렉션되어 사용자의 리전 로그에 리전 CloudTrail 로그 항목이 기록됩니다.

반면 Amazon S3 콘솔은 리전을 지원하지 않습니다. 따라서 다음 URL에 로그인할 경우

```
https://alias.signin.aws.amazon.com/console/s3
```

AWS가 사용자의 `https://signin.aws.amazon.com`의 글로벌 로그인 종단점으로 리디렉션하여 글로벌 CloudTrail 로그 항목이 기록됩니다.

- 다음과 같은 URL 구문을 사용하여 리전이 활성화된 메인 콘솔 홈 페이지에 로그인하면 특정 리전 로그인 종단점을 수동으로 요청할 수 있습니다.

```
https://alias.signin.aws.amazon.com/console?region=ap-southeast-1
```

AWS가 사용자를 `ap-southeast-1` 리전 로그인 종단점으로 리디렉션하고 리전 CloudTrail 로그 이벤트가 발생합니다.

CloudTrail 및 IAM에 대한 자세한 내용은 AWS CloudTrail로 IAM 이벤트 로깅 단원을 참조하십시오.

계정을 통해 사용자가 작업하기 위해 프로그래밍 방식의 액세스가 필요할 경우에는 액세스 키 관리(콘솔) (p. 112)에 기술된 대로 각 사용자의 액세스 키 페어(액세스 키 ID와 보안 액세스 키)를 생성할 수 있습니다.

IAM사용자 관리

Amazon Web Services는 AWS 계정에 속한 IAM 사용자들을 관리할 수 있는 다양한 도구를 제공합니다. 계정 또는 그룹에 속한 IAM 사용자를 나열하거나 한 사용자가 속한 모든 그룹을 나열할 수 있습니다. IAM 사용자의 이름을 변경하거나 경로를 변경할 수 있습니다. AWS 계정에서 IAM 사용자를 삭제할 수도 있습니다.

IAM 사용자에 대한 관리형 정책의 추가, 변경, 제거에 대한 자세한 내용은 IAM 사용자의 권한 변경 (p. 96) 단원을 참조하십시오. IAM 사용자에 대한 인라인 정책 관리에 대한 자세한 내용은 IAM 자격 증명 권한 추가 및 제거 (p. 450), IAM 정책 편집 (p. 460), IAM 정책 삭제 (p. 465) 단원을 참조하십시오. 인라인 정책보다는 관리형 정책을 사용하는 것이 좋습니다.

IAM 사용자 암호 관리에 대한 자세한 내용은 IAM 사용자의 암호 관리 (p. 104) 단원을 참조하십시오.

주제

사용자 액세스 보기

사용자를 삭제하기 전에 최근 서비스 수준 활동을 검토해야 합니다. 이 기능은 사용 중인 보안 주체(사람 또는 애플리케이션)의 액세스 권한을 제거하지 않으려는 경우 중요합니다. 서비스에서 마지막으로 액세스한 데이터 보기에 대한 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

IAM 사용자 표시

AWS 계정 또는 특정 IAM 그룹에 속한 IAM 사용자, 그리고 한 사용자가 속한 모든 그룹을 표시할 수 있습니다. 사용자 표시에 필요한 권한에 대한 자세한 내용은 IAM 리소스에 액세스하는 데 필요한 권한 (p. 507) 단원을 참조하십시오.

계정에 속한 모든 사용자를 표시하려면

- AWS Management 콘솔: 탐색 창에서 사용자를 선택합니다. 콘솔에 AWS 계정에 속한 사용자가 표시됩니다.
- AWS CLI: aws iam list-users
- AWS API: ListUsers

특정 그룹에 속한 사용자를 표시하려면

- AWS Management 콘솔: 탐색 창에서 그룹을 선택하고, 그룹 이름을 선택한 후 사용자 탭을 선택합니다.
- AWS CLI: aws iam get-group
- AWS API: GetGroup

사용자가 속한 모든 그룹을 표시하려면

- AWS Management 콘솔: 탐색 창에서 사용자를 선택하고, 사용자 이름을 선택한 후 그룹 탭을 선택합니다.
- AWS CLI: aws iam list-groups-for-user
- AWS API: ListGroupsForUser

IAM 사용자 이름 바꾸기

사용자의 이름 또는 경로를 변경하려면 AWS CLI, Windows PowerShell용 도구 또는 AWS API를 사용해야 합니다. 콘솔에서는 사용자의 이름을 변경할 수 있는 옵션이 없습니다. 사용자의 이름을 변경하기 위해 필요한 권한에 대한 자세한 내용은 IAM 리소스에 액세스하는 데 필요한 권한 (p. 507) 단원을 참조하십시오.

사용자의 이름 또는 경로를 변경하면 다음과 같이 진행됩니다.

- 사용자에 연결된 정책은 이름이 변경되어도 계속 유지됩니다.
- 사용자는 전과 동일한 그룹에 새 이름으로 표시됩니다.
- 사용자의 고유 ID는 전과 같습니다. 고유 ID에 대한 자세한 내용은 고유 식별자 (p. 567) 단원을 참조하십시오.

- 사용자를 보안 주체로 참조(해당 사용자에게 액세스가 부여됨)하는 리소스 또는 역할 정책은 새 이름 또는 경로를 사용하도록 자동 업데이트됩니다. 예를 들어 Amazon SQS의 대기열 기반 정책 또는 Amazon S3의 리소스 기반 정책은 자동 업데이트되어 새 이름과 경로를 사용합니다.

사용자를 리소스로 참조하는 정책은 새 이름 또는 경로를 사용하도록 IAM에서 자동 업데이트하지 않으므로 수동으로 업데이트해야 합니다. 예를 들어 사용자 `Richard`에게 자신의 보안 자격 증명을 관리하는 정책이 연결되어 있을 경우 관리자가 `Richard`에서 `Rich`로 이름을 변경하면 다음과 같이 리소스가 변경되도록 관리자가 정책도 업데이트해야 합니다.

```
arn:aws:iam::111122223333:user/division_abc/subdivision_xyz/Richard
```

다음으로 업데이트:

```
arn:aws:iam::111122223333:user/division_abc/subdivision_xyz/Rich
```

마찬가지로 경로를 변경할 경우에도 관리자가 사용자에 대한 새 경로를 반영하도록 정책을 업데이트해야 합니다.

사용자의 이름을 바꾸려면

- AWS CLI: aws iam update-user
- AWS API: UpdateUser

IAM 사용자 삭제

퇴사자가 생길 경우 계정에서 IAM 사용자를 삭제할 수 있습니다. 사용자가 잠시 회사에 나오지 않는 경우에는 AWS 계정에서 해당 사용자를 완전히 삭제하는 대신 사용자의 자격 증명을 비활성화할 수 있습니다. 이렇게 하면 부재 중 해당 사용자가 AWS 계정의 리소스에 액세스하는 것을 막고 나중에 해당 사용자를 다시 활성화할 수 있습니다.

자격 증명 비활성화에 대한 자세한 내용은 IAM 사용자의 액세스 키 관리 (p. 111) 단원을 참조하십시오. 사용자를 삭제하기 위해 필요한 권한에 대한 자세한 내용은 IAM 리소스에 액세스하는 데 필요한 권한 (p. 507) 단원을 참조하십시오.

주제

IAM 사용자 삭제(콘솔)

AWS Management 콘솔을 사용하여 IAM 사용자를 삭제하면 IAM에서 자동으로 다음 정보를 삭제합니다.

- 해당 사용자
- 모든 그룹 멤버십, 즉 속해 있던 모든 IAM 그룹에서 사용자가 제거됨
- 사용자와 연결된 모든 암호
- 사용자에게 속한 모든 액세스 키
- 사용자에게 포함된 모든 인라인 정책(그룹 권한을 통해 사용자에게 적용되는 정책은 영향을 받지 않음)

  Note

  사용자를 삭제하면 해당 사용자에게 연결된 관리형 정책이 해당 사용자에게서 분리됩니다. 사용자를 삭제해도 관리형 정책은 삭제되지 않습니다.

- 연결된 모든 MFA 디바이스

IAM 사용자를 삭제하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택한 후 삭제하려는 역할 옆에 있는 확인란(사용자 이름이나 행 아님)을 선택합니다.
3. 페이지 상단에서 사용자 삭제를 선택합니다.
4. 확인 대화 상자에 서비스에서 마지막으로 액세스한 데이터가 로드될 때까지 기다렸다 데이터를 검토합니다. 이 대화 상자는 선택한 각 사용자가 언제 마지막으로 AWS 서비스에 액세스했는지 보여줍니다. 직전 30일 이내에 활성화된 적이 있는 사용자를 삭제하려는 경우 활성 사용자를 삭제한다는 추가 확인란을 선택해야 합니다. 계속하려면 예, 삭제를 선택합니다.

IAM 사용자 삭제(AWS CLI)

AWS Management 콘솔과 달리 AWS CLI로 사용자를 삭제할 때는 사용자에게 연결된 항목들을 수동으로 삭제해야 합니다. 다음 절차는 그 과정을 보여줍니다.

계정에서 사용자를 삭제하려면(AWS CLI)

1. 해당 사용자의 암호가 있으면 삭제합니다.

   `aws iam delete-login-profile`
2. 해당 사용자의 액세스 키가 있으면 삭제합니다.

   `aws iam list-access-keys`(사용자의 액세스 키 나열) 및 `aws iam delete-access-key`
3. 사용자 서명 인증서를 삭제합니다. 보안 자격 증명을 삭제하면 영원히 지워져 검색할 수 없습니다.

   `aws iam list-signing-certificates`(사용자의 서명 인증서 나열) 및 `aws iam delete-signing-certificate`
4. 해당 사용자의 SSH 퍼블릭 키가 있으면 삭제합니다.

   `aws iam list-ssh-public-keys`(사용자의 SSH 퍼블릭 키 나열) 및 `aws iam delete-ssh-public-key`
5. 사용자의 Git 자격 증명을 삭제합니다.

   `aws iam list-service-specific-credentials`(사용자의 Git 자격 증명 나열) 및 `aws iam delete-service-specific-credential`
6. 해당 사용자의 Multi-Factor Authentication(MFA) 디바이스가 있으면 비활성화합니다.

   `aws iam list-mfa-devices`(사용자의 MFA 디바이스 나열), `aws iam deactivate-mfa-device`(디바이스 비활성화) 및 `aws iam delete-virtual-mfa-device`(가상 MFA 디바이스를 영구 삭제)
7. 사용자의 인라인 정책을 삭제합니다.

   `aws iam list-user-policies`(사용자에 대한 인라인 정책 나열) 및 `aws iam delete-user-policy`(정책 삭제)
8. 사용자에 연결된 관리형 정책을 모두 분리합니다.

   `aws iam list-attached-user-policies`(사용자에게 연결된 관리형 정책 나열) 및 `aws iam detach-user-policy`(정책 분리)
9. 모든 그룹에서 사용자를 제거합니다.

`aws iam list-groups-for-user`(사용자가 속한 그룹 나열) 및 `aws iam remove-user-from-group`

10. 사용자를 삭제합니다.

    `aws iam delete-user`

IAM 사용자의 권한 변경

그룹 멤버십을 변경하거나 기존 사용자에서 권한을 복사, 사용자에게 바로 정책을 연결 또는 권한 경계 (p. 363)를 설정하여 AWS 계정의 IAM 사용자에 대한 권한을 변경할 수 있습니다. 이 권한 경계는 사용자가 가질 수 있는 최대 권한을 관리합니다. 권한 경계는 고급 AWS 기능입니다.

사용자의 권한을 수정하기 위해 필요한 권한에 대한 자세한 내용은 IAM 리소스에 액세스하는 데 필요한 권한 (p. 507) 단원을 참조하십시오.

주제

사용자 액세스 보기

사용자에 대한 권한을 변경하기 전에 최근 서비스 수준 활동을 검토해야 합니다. 이 기능은 사용 중인 보안 주체(사람 또는 애플리케이션)의 액세스 권한을 제거하지 않으려는 경우 중요합니다. 서비스에서 마지막으로 액세스한 데이터 보기에 대한 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

사용자(콘솔)에게 권한 추가

IAM은 사용자에게 권한 정책을 추가하는 세 가지 방법을 제안합니다.

- 그룹에게 사용자 추가 – 사용자를 그룹의 구성원으로 만듭니다. 그룹의 정책은 사용자로 연결됩니다.
- 기존 사용자에서 권한 복사 – 소스 사용자에서 그룹 멤버십, 연결된 관리형 정책, 인라인 정책 및 기존 권한 경계를 모두 복사합니다.
- 정책을 사용자에 직접 연결 – 관리형 정책을 사용자에 직접 연결합니다. 그 대신에 그룹에 정책을 연결한 다음, 사용자들을 적절한 그룹의 구성원으로 만드는 것이 바람직한 모범 사례 (p. 61)입니다.

> **Important**
>
> 사용자에게 권한 경계가 있다면 권한 경계가 허용한 권한보다 더 많은 권한을 추가할 수 없습니다.

사용자를 그룹에 추가하여 권한을 추가

사용자를 그룹에 추가하여 사용자에게 바로 영향을 줍니다.

사용자를 그룹에 추가하여 사용자에게 권한을 추가하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.

2. 탐색 창에서 사용자를 선택합니다.
3. 콘솔의 그룹 열에서 사용자에 대한 현재 그룹 멤버십을 검토합니다. 필요할 경우 다음 단계를 통해 사용자 테이블에 열을 추가합니다.

   1. 테이블 위 맨 오른쪽에서 설정 기호( )를 선택합니다.
   2. Manage Columns(열 관리) 대화 상자에서 그룹 열을 선택합니다. 필요할 경우 사용자 테이블에 표시하지 않으려는 열이 있으면 해당 열의 확인란 선택을 취소하면 됩니다.
   3. 닫기를 선택하여 사용자 목록으로 돌아갑니다.

   그룹 열에는 사용자가 속한 그룹이 표시됩니다. 열에는 최대 2개 그룹에 대한 그룹 이름이 표시됩니다. 사용자가 3개 이상 그룹의 구성원인 경우 처음 두 개 그룹만 알파벳 순서대로 표시되고 나머지 그룹 멤버십 수가 표시됩니다. 예를 들어 사용자가 그룹 A, 그룹 B, 그룹 C, 그룹 D에 속한 경우 필드에 Group A, Group B + 2 more(그룹 A, 그룹 B 외 2개)라고 표시됩니다. 사용자가 속한 총 그룹 수를 보려면 사용자 테이블에 Group count(그룹 수) 열을 추가합니다.
4. 권한을 수정하려는 사용자의 이름을 선택합니다.
5. 권한 탭을 선택한 다음 Add permissions(권한 추가)를 선택합니다. [Add user to group]을 선택합니다.
6. 사용자를 귀속시키려는 각 그룹의 확인란을 선택합니다. 그 목록에는 각 그룹의 이름과 사용자가 그 그룹의 구성원이 되면 받는 정책이 표시됩니다.
7. (선택 사항) 기존 그룹에서 선택할 수 있을 뿐 아니라 다음과 같이 그룹 생성을 선택하여 새 그룹을 정의할 수 있습니다.

   a. 새로운 탭에서 그룹 이름으로 새로운 그룹의 이름을 입력합니다.

      Note

      그룹 이름에는 최대 128개의 알파벳, 숫자 및 더하기(+), 등호(=), 쉼표(,), 마침표(.), 앳(@), 그리고 하이픈(-) 조합을 사용할 수 있습니다. 이름은 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어 "TESTGROUP"과 "testgroup"이라는 두 그룹을 만들 수는 없습니다. IAM 엔터티 관련 제한에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

   b. 그룹에 연결하고자 하는 관리형 정책에 대해 한 개 이상의 확인란을 선택합니다. 정책 생성을 선택하여 새로운 관리형 정책을 만들 수도 있습니다. 이렇게 하는 경우, 새 정책이 완료되면 이 브라우저 탭 또는 창으로 돌아가 새로 고침을 선택한 다음, 그룹에 연결할 새로운 정책을 선택합니다. 자세한 내용은 IAM 정책 만들기 (p. 435) 단원을 참조하십시오.
   c. Create group을 선택합니다.
   d. 기존 탭으로 반환하고 그룹 목록을 새로 고침합니다. 새로운 그룹에 대한 확인란을 선택합니다.
8. Next: Review(다음: 검토)를 선택하여 사용자에 추가될 그룹 멤버십의 목록을 확인합니다. 그런 다음 Add permissions(권한 추가)를 선택합니다.

다른 사용자에게서 복사하여 권한을 추가

권한 복사는 사용자에게 바로 적용됩니다.

다른 사용자에게서 권한을 복사하여 사용자에게 권한을 추가하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택한 다음, 권한을 수정할 사용자의 이름을 선택하고 권한 탭을 선택합니다.
3. Add permissions(권한 추가)를 선택한 다음, Copy permissions from existing user(기존 사용자에서 권한 복사)를 선택합니다. 목록에는 사용 가능한 사용자들이 그들의 그룹 멤버십 및 연결된 정책과 함께 표시됩니다. 그룹 또는 정책의 전체 목록이 한 줄에 다 표시되지 않는 경우, and ***n*** more(외 ***n***개) 링크를 선택할 수 있습니다. 그러면 새 브라우저 탭이 열리고 정책(권한 탭) 및 그룹(그룹 탭)의 전체 목록을 볼 수 있습니다.

4. 복사하고자 하는 권한을 보유한 사용자 옆에 있는 라디오 버튼을 선택합니다.
5. Next: Review(다음: 검토)를 선택하여 사용자에 대한 변경 사항의 목록을 확인합니다. 그런 다음 Add permissions(권한 추가)를 선택합니다.

사용자에게 직접 정책을 연결하여 권한을 추가

정책 연결은 사용자에게 바로 적용됩니다.

관리형 정책을 직접 연결하여 사용자에게 권한을 추가하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택한 다음, 권한을 수정할 사용자의 이름을 선택하고 권한 탭을 선택합니다.
3. Add permissions(권한 추가)를 선택한 다음, Attach existing policies directly to user(기존 정책을 사용자에게 직접 연결)를 선택합니다.
4. 사용자에 연결하고자 하는 관리형 정책에 대해 한 개 이상의 확인란을 선택합니다. 정책 생성을 선택하여 새로운 관리형 정책을 만들 수도 있습니다. 이렇게 하는 경우, 새 정책이 완료되면 이 브라우저 탭 또는 창으로 돌아가 새로 고침을 선택한 다음, 사용자에게 연결할 새로운 정책 확인란을 선택합니다. 자세한 내용은 IAM 정책 만들기 (p. 435) 단원을 참조하십시오.
5. Next: Review(다음: 검토)를 선택하여 사용자에 연결될 정책의 목록을 확인합니다. 그런 다음 Add permissions(권한 추가)를 선택합니다.

사용자에 대한 권한 경계 설정

권한 경계 설정은 사용자에게 바로 적용됩니다.

사용자에 대한 권한 경계를 설정하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 권한 경계를 변경하려는 사용자의 이름을 선택합니다.
4. Permissions 탭을 선택합니다. 필요하다면 Permissions boundary(권한 경계) 섹션을 열고 Set boundary(경계 설정)를 선택합니다.
5. 정책을 선택하여 원하는 권한 경계를 사용하십시오.
6. Set boundary(경계 설정)을 선택합니다.

사용자(콘솔)의 권한 변경

IAM는 사용자와 관련된 권한을 변경하는 세 가지 방법을 제안합니다.

- 권한 정책 편집 – 사용자 인라인 정책, 사용자 그룹의 인라인 정책을 편집하거나 바로 사용자에게 또는 그룹에서 연결된 관리형 정책을 편집합니다. 사용자에게 권한 경계가 있다면 권한 경계로 사용된 정책이 허용한 권한보다 더 많은 권한을 제공할 수 없습니다.
- 권한 경계 변경 – 사용자에 대한 권한 경계로 사용된 정책을 변경합니다. 이로써 사용자가 가질 수 있는 최대 권한을 확장 또는 제한할 수 있습니다.

사용자에게 연결된 권한 정책을 편집합니다

권한 변경은 사용자에게 바로 적용됩니다.

사용자의 연결된 관리형 정책을 편집하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 권한 정책을 변경하려는 사용자의 이름을 선택합니다.
4. Permissions 탭을 선택합니다. 필요하다면 Permissions policies(권한 정책) 부분을 엽니다.
5. 정책에 대한 세부 정보를 보기 위해서 편집하고자 하는 정책 이름을 선택합니다. Used as(다음과 같이 사용됨) 탭을 선택하여 정책을 편집함으로써 영향을 받을 다른 개체를 봅니다.
6. 그런 다음 Permissions tab(권한 탭)을 정책이 허용한 권한을 검토합니다. 그런 다음 정책 편집을 선택합니다.
7. Visual editor(시각적 편집기) 탭 또는 JSON 탭을 사용하여 정책을 편집합니다. 자세한 내용은 IAM 정책 편집 (p. 460) 단원을 참조하십시오.
8. 정책 검토를 선택한 다음 정책 요약을 검토한 후 변경 사항 저장을 선택합니다.

사용자에 대한 권한 경계를 변경하십시오.

권한 경계 변경은 사용자에게 바로 적용됩니다.

사용자의 권한 경계 설정에 사용된 정책을 변경하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 권한 경계를 변경하려는 사용자의 이름을 선택합니다.
4. Permissions 탭을 선택합니다. 필요하다면 Permissions boundary(권한 경계) 섹션을 열고 Change boundary(경계 변경)을 선택합니다.
5. 정책을 선택하여 원하는 권한 경계를 사용하십시오.
6. Change boundary(경계 변경)을 선택합니다.

사용자(콘솔)에게서 권한 정책 제거

정책 제거는 사용자에게 바로 적용됩니다.

IAM 사용자의 권한을 취소하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 권한 경계를 제거하려는 사용자의 이름을 선택합니다.
4. Permissions 탭을 선택합니다.
5. 기존 정책을 제거하여 권한을 취소하려면 정책을 제거하기 전에 X를 선택하여 정책 유형에서 사용자가 어떻게 정책을 받는지 확인합니다.
   - 그 정책이 그룹 멤버십 때문에 적용되는 경우, X를 선택하면 사용자가 그룹에서 제거됩니다. 한 그룹에 여러 정책이 연결될 수 있습니다. 따라서 그룹에서 사용자를 제거할 경우 사용자는 그 그룹의 멤버십을 통해 받은 모든 정책에 대한 액세스 권한을 잃게 됩니다.
   - 정책이 사용자에 직접 연결된 관리형 정책인 경우 X를 선택하면 정책이 사용자와 분리됩니다. 이렇게 해도 정책 자체 또는 그 정책이 연결되어 있을 수 있는 다른 개체에는 영향을 미치지 않습니다.

- 정책이 인라인 포함 정책인 경우, X를 선택하면 정책이 IAM에서 제거됩니다. 사용자에 직접 연결된 인라인 정책은 해당 사용자에만 존재합니다.

사용자(콘솔)에게서 권한 경계 제거

권한 경계 제거는 사용자에게 바로 적용됩니다.

사용자(콘솔)에게서 권한 경계를 제거하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 권한 경계를 제거하려는 사용자의 이름을 선택합니다.
4. Permissions 탭을 선택합니다. 필요하다면 Permissions boundary(권한 경계) 섹션을 열고 Remove boundary(경계 제거)를 선택합니다.
5. 제거를 선택하여 권한 경계를 제거합니다.

사용자 권한(AWS CLI 또는 AWS API) 추가 및 제거

프로그래밍 방식으로 권한을 추가 또는 제거하려면 그룹 멤버십을 추가 또는 제거하거나 관리형 정책을 연결 또는 분리하거나 인라인 정책을 추가 또는 삭제해야 합니다. 자세한 내용은 다음 주제 단원을 참조하십시오.

- IAM 그룹에서 사용자 추가 및 제거 (p. 170)
- IAM 자격 증명 권한 추가 및 제거 (p. 450)

암호 관리

AWS 계정 루트 사용자 및 계정의 IAM 사용자의 암호를 관리할 수 있습니다. IAM 사용자가 AWS Management 콘솔에 액세스하려면 암호가 필요합니다. 사용자가 AWS CLI, Windows PowerShell용 도구, AWS SDK 또는 API를 사용하여 프로그래밍 방식으로 AWS 리소스에 액세스하는 경우 암호가 필요 없습니다. 대신 그러한 환경에서는 사용자에게 액세스 키 (p. 111)가 필요합니다.

주제

- AWS 계정 루트 사용자 암호 변경 (p. 100)
- IAM 사용자의 계정 암호 정책 설정 (p. 101)
- IAM 사용자의 암호 관리 (p. 104)
- IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108)
- IAM 사용자가 자신의 암호를 변경하는 방법 (p. 110)

AWS 계정 루트 사용자 암호 변경

루트 사용자 암호를 변경하려면 IAM 사용자가 아닌 AWS 계정 루트 사용자로 로그인해야 합니다. 잊어버린 루트 사용자 암호를 재설정하는 방법에 대한 자세한 내용은 분실하거나 잊어버린 암호 또는 액세스 키 재설정 (p. 118) 단원을 참조하십시오.

루트 사용자의 암호를 변경하려면

1. AWS 계정 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 AWS 계정 루트 사용자로 로그인합니다.

Note

텍스트 상자가 세 개 표시되면 이전에 IAM 사용자 자격 증명으로 콘솔에 로그인한 것입니다. 브라우저에서 이 기본 설정을 기억하고 로그인할 때마다 이 계정별 로그인 페이지를 열 수 있습니다. IAM 사용자 로그인 페이지에서는 계정 소유자로 로그인할 수 없습니다. IAM 사용자 로그인 페이지가 표시되면 페이지 하단에 있는 Sign in using 루트 사용자 email(이메일을 사용하여 로그인)을 선택하여 기본 로그인 페이지로 돌아갑니다. 기본 로그인 페이지에서 AWS 계정 이메일 주소와 암호를 입력하여 루트 사용자로 로그인합니다.

2. 콘솔의 오른쪽 상단 모서리 부분에서 계정 이름이나 번호를 선택한 후 내 계정을 선택합니다.
3. 페이지 오른쪽의 계정 설정 섹션 옆에서 편집을 선택합니다.
4. 암호 줄에서 편집을 선택하여 암호를 변경합니다.
5. 강력한 암호를 선택하십시오. IAM 사용자에 대한 계정 암호 정책을 설정 할 수는 있지만 (p. 101), AWS 계정 루트 사용자에게는 이 정책이 적용되지 않습니다.

   AWS는 암호가 다음 조건을 충족하도록 요구합니다.

   - 최소 8자 이상이고 최대 128자 이하여야 함
   - 대문자, 소문자, 숫자, 비-영문자 기호(예: ! @ # $ % ^ & * () <> [] {} | _+-=) 중에서 세 가지 이상의 혼합 문자 유형 포함
   - AWS 계정 이름 또는 이메일 주소와 동일하지 않아야 함

   Note

   AWS가 로그인 프로세스의 개선 사항을 공개합니다. 그중 하나는 사용자 계정에 더 안전한 암호 정책을 강화하는 것입니다. 계정이 업그레이드된 경우 위 암호 정책에 부합해야 합니다. 아직 계정이 업그레이드되지 않았다면 AWS에서는 이 정책이 집행되지 않으나, 더 안전한 암호를 위하여 지침을 따를 것을 강력히 권장합니다.

   암호를 보호하려면 다음과 같은 모범 사례를 활용하는 것이 중요합니다.

   - 주기적으로 암호를 변경하고 암호는 비공개로 유지하십시오. 암호를 아는 사람이 귀하의 계정에 액세스할 수 있습니다.
   - AWS의 암호를 다른 사이트에서 사용하는 것과 다르게 지정하십시오.
   - 짐작하기 쉬운 암호를 사용하지 마십시오. 여기에는 `secret`, `password`, `amazon` 또는 `123456` 같은 암호가 포함됩니다. 또한 사전에 나오는 단어, 사용자 이름, 이메일 주소 또는 알아내기 쉬운 그 밖의 개인 정보도 포함됩니다.

IAM 사용자의 계정 암호 정책 설정

AWS 계정에서 암호 정책을 설정하여 IAM 사용자 암호의 복잡성 요건과 의무적인 교체 주기를 지정할 수 있습니다.

이러한 작업을 실행할 때 암호 정책을 사용할 수 있습니다.

- 최소 암호 길이를 설정합니다.
- 대문자, 소문자, 숫자, 비-영숫자를 포함하는 특정 문자 유형이 필요합니다. 사용자에게 암호의 대소문자가 구분된다는 점을 알려야 합니다.
- 모든 IAM 사용자에게 자신의 암호 변경을 허용합니다.

  Note

  IAM 사용자에게 자신의 암호 변경을 허용하면 IAM이 자동으로 사용자에게 암호 정책을 보여줍니다. IAM 사용자가 정책에 따르는 암호를 생성하려면 계정의 암호 정책을 볼 수 있어야 합니다.
- IAM 사용자에게 지정 시간(암호 만료 설정)이 지나면 암호를 변경하라고 요구합니다.

- IAM 사용자가 이전 암호를 재사용하는 것을 금지합니다.
- IAM 사용자의 암호가 만료된 경우에는 계정 관리자에게 사용자가 연락하게 합니다.

  Important

  여기에서 설명한 암호 설정은 IAM 사용자에게 할당된 암호에만 적용되고 사용자들이 갖고 있을 수 있는 액세스 키에는 영향을 미치지 않습니다. 암호가 만료된 경우, 사용자는 AWS Management 콘솔에 로그인할 수 없습니다. 하지만 사용자에게 유효한 액세스 키가 있으면 여전히 AWS CLI 또는 Windows PowerShell용 도구 명령을 실행할 수 있습니다. 또한 애플리케이션을 통해 사용자의 권한이 허용하는 API 작업을 호출할 수도 있습니다.

암호 정책을 생성 또는 변경하더라도 대부분의 암호 정책 설정은 사용자가 다음에 자신의 암호를 변경할 때 적용됩니다. 하지만 일부 설정은 바로 적용됩니다. 예:

- 최소 길이 및 문자 유형 요건을 설정하면 그 설정 사항은 다음 번에 사용자가 자신의 암호를 변경할 때 적용됩니다. 기존 암호가 업데이트된 암호 정책을 따르지 않는 경우에도 사용자들은 기존 암호를 변경할 필요는 없습니다.
- 암호 만료 기간을 설정하면 만료 기간이 바로 적용됩니다. 예를 들어 암호 만료 기간을 90일로 설정한 경우, 현재 90일 이상 지난 기존 암호를 지닌 IAM 사용자들은 모두 다음 로그인 시 자신의 암호를 변경해야 합니다.

암호 정책을 설정하기 위해 필요한 권한에 대한 자세한 내용은 IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108) 단원을 참조하십시오.

IAM 암호 정책은 AWS 계정 루트 사용자 암호에는 적용되지 않습니다.

현재 사용 가능한 이 옵션으로는 "잠금 정책"이라고 하는 것을 만들 수 없습니다. 이러한 정책은 로그인 시도 실패 횟수가 지정한 횟수에 도달하면 사용자 계정을 잠급니다. 보안을 강화하려면 암호 정책과 멀티 팩터 인증(MFA)을 함께 사용하는 것이 좋습니다. MFA에 대한 자세한 내용은 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.

주제

암호 정책 옵션

아래는 계정의 암호 정책 구성 시 사용할 수 있는 옵션들입니다.

최소 암호 길이

IAM 사용자 암호에서 허용되는 최소 문자 수를 지정할 수 있습니다. 6~128 범위에서 입력할 수 있습니다.

1개 이상의 대문자 필수

IAM 사용자 암호에 ISO 기본 라틴 알파벳(A~Z) 중 1개 이상의 대문자를 사용하도록 요구할 수 있습니다.

1개 이상의 소문자 필수

IAM 사용자 암호에 ISO 기본 라틴 알파벳(a~z) 중 1개 이상의 소문자를 사용하도록 요구할 수 있습니다.

1개 이상의 숫자 필수

IAM 사용자 암호에 숫자(0~9) 중 1개 이상의 숫자를 사용하도록 요구할 수 있습니다.

알파벳이나 숫자가 아닌 1개 이상의 문자 필수

IAM 사용자 암호에 다음과 같이 알파벳이나 숫자가 아닌 최소 1개의 문자를 사용하도록 요구할 수 있습니다.

```
! @ # $ % ^ & * ( ) _ + - = [ ] { } | '
```

사용자 자신의 암호 변경 허용

계정의 IAM 사용자 모두 IAM 콘솔을 사용하여 자신의 암호를 변경할 수 있습니다. 자세한 설명은 IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108) 단원을 참조하십시오.

그 밖에 자신이나 다른 사용자의 암호를 관리하는 사용자를 일부로 제한할 수도 있습니다. 이렇게 하려면 사용자 자신의 암호 변경 허용(Allow users to change their own password) 확인란 선택을 해제하면 됩니다. 암호 관리 제한 정책의 사용에 대한 자세한 내용은 IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108) 단원을 참조하십시오.

Note

IAM 사용자에게 자신의 암호 변경을 허용하면 IAM이 자동으로 사용자에게 암호 정책을 보여줍니다. IAM 사용자가 정책에 따르는 암호를 생성하려면 계정의 암호 정책을 볼 수 있어야 합니다.

암호 만료 활성화

IAM 사용자 암호는 지정 일수 동안만 유효하도록 설정할 수 있습니다. 방법은 암호 설정 후 유효 일수를 지정하면 됩니다. 예를 들어 암호 만료를 활성화하여 암호 만료 기간을 90일로 설정하면 IAM 사용자는 최대 90일까지 암호를 사용할 수 있습니다. 90일이 지나면 암호가 만료되어 IAM 사용자가 AWS Management 콘솔에 액세스하려면 암호를 새로 설정해야 합니다. 암호 만료 기간은 1~1,095(1,095 포함)일 중에서 선택할 수 있습니다.

Note

암호 만료까지 15일이 남으면 AWS Management 콘솔이 IAM 사용자에게 경고를 보냅니다. IAM 사용자는 언제든지 자신의 암호를 변경할 수 있습니다(변경 권한이 있는 경우에 한함). 새 암호를 설정하면 암호 변경 기간이 다시 시작됩니다. IAM 사용자는 한 번에 유효 암호 하나만 사용할 수 있습니다.

암호 재사용 제한

IAM 사용자가 이전 암호를 지정한 수만큼 재사용하지 못하도록 제한할 수 있습니다. 설정할 수 있는 암호 수는 1~24(24 포함)개입니다.

암호 만료 시 관리자 재설정

현재 암호가 만료된 후 IAM 사용자가 새 암호를 선택하지 못하도록 제한할 수 있습니다. 예를 들어 암호 정책은 암호 만료 기간을 지정할 수 있습니다. IAM 사용자가 암호 만료 전에 새 암호를 선택하지 않으면 IAM 사용자는 새 암호를 설정할 수 없습니다. 이 경우 IAM 사용자가 AWS Management 콘솔에 대한 액세스 권한을 다시 얻으려면 계정 관리자의 암호 재설정을 요구해야 합니다. 이 확인란을 그냥 비워 놓아도 됩니다. IAM 사용자가 자신의 암호를 만료되게 둘 경우 사용자는 AWS Management 콘솔에 액세스하기 전에 새 암호를 설정해야 합니다.

Warning

이 옵션을 활성화하기 전에 AWS 계정에 관리자 권한(IAM 사용자 암호의 재설정 권한)을 가진 사용자가 2명 이상인지 확인해야 합니다. 또는 관리자에게도 AWS CLI 또는 Windows PowerShell용 도구를 AWS Management 콘솔;과 별도로 사용할 수 있는 액세스 키가 있는지 확인할 수 있습니다. 이 옵션이 활성화된 상태에서 한 관리자의 암호가 만료된 경우, 첫 번째 관리자의 만료된 암호를 재설정하려면 두 번째 관리자가 콘솔에 로그인해야 합니다. 그러나 암호

가 만료된 관리자에게 유효한 액세스 키가 있는 경우에는 AWS CLI 또는 Windows PowerShell 용 도구 명령을 실행할 수 있습니다. 이러한 명령은 관리자의 암호를 재설정할 수 있습니다. 두 번째 관리자에 대한 요건은 암호가 만료되고 첫 번째 관리자에게 액세스 키가 없는 경우에만 적용됩니다.

암호 정책 설정(콘솔)

AWS Management 콘솔에서 암호 정책을 생성, 변경 또는 삭제할 수 있습니다. 암호 정책 관리의 일환으로 모든 사용자가 자신의 암호를 관리하도록 허용할 수 있습니다.

암호 정책을 생성하거나 변경하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 계정 설정을 클릭합니다.
3. 암호 정책 섹션에서 암호 정책에 적용하려는 옵션을 선택합니다.
4. 암호 정책 적용(Apply Password Policy)를 클릭합니다.

암호 정책을 삭제하는 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 계정 설정을 클릭한 다음 암호 정책 섹션에서 암호 정책 삭제(Delete Password Policy)를 클릭합니다.

암호 정책 설정(AWS CLI)

AWS CLI에서 계정 암호 정책을 관리하려면 다음 명령을 실행하십시오.

- 암호 정책을 생성 또는 변경하는 방법: `aws iam update-account-password-policy`
- 암호 정책 가져오기: `aws iam get-account-password-policy`
- 암호 정책을 삭제하는 방법: `aws iam delete-account-password-policy`

암호 정책 설정(AWS API)

AWS API에서 계정 암호 정책을 관리하려면 다음 작업을 호출하십시오.

- 암호 정책을 생성 또는 변경하는 방법: `UpdateAccountPasswordPolicy`
- 암호 정책 가져오기: `GetAccountPasswordPolicy`
- 암호 정책을 삭제하는 방법: `DeleteAccountPasswordPolicy`

IAM 사용자의 암호 관리

AWS Management 콘솔을 사용하여 AWS 리소스를 작업하는 IAM 사용자가 로그인하려면 암호가 필요합니다. AWS 계정에 속한 IAM 사용자의 암호를 생성, 변경 또는 삭제할 수 있습니다.

사용자에게 암호를 할당한 후 사용자는 다음과 같은 계정의 로그인 URL을 사용하여 AWS Management 콘솔에 로그인할 수 있습니다.

```
https://12-digit-AWS-account-ID or alias.signin.aws.amazon.com/console
```

IAM 사용자가 AWS Management 콘솔에 로그인하는 방법에 대한 자세한 내용은 IAM 콘솔 및 로그인 페이지 (p. 71) 단원을 참조하십시오.

IAM 사용자의 개별 암호를 수동으로 만들 수 있지만 AWS 계정에 속한 모든 IAM 사용자의 암호에 적용되는 암호 정책을 만들 수도 있습니다.

이러한 작업을 실행할 때 암호 정책을 사용할 수 있습니다.

- 최소 암호 길이를 설정합니다.
- 대문자, 소문자, 숫자, 비-영숫자를 포함하는 특정 문자 유형이 필요합니다. 사용자에게 암호의 대소문자가 구분된다는 점을 알려야 합니다.
- 모든 IAM 사용자에게 자신의 암호 변경을 허용합니다.

  Note

  IAM 사용자에게 자신의 암호 변경을 허용하면 IAM이 자동으로 사용자에게 암호 정책을 보여줍니다. IAM 사용자가 정책에 따르는 암호를 생성하려면 계정의 암호 정책을 볼 수 있어야 합니다.
- IAM 사용자에게 지정 시간(암호 만료 설정)이 지나면 암호를 변경하라고 요구합니다.
- IAM 사용자가 이전 암호를 재사용하는 것을 금지합니다.
- IAM 사용자의 암호가 만료된 경우에는 계정 관리자에게 사용자가 연락하게 합니다.

계정의 암호 정책 관리에 대한 자세한 내용은 IAM 사용자의 계정 암호 정책 설정 (p. 101)을 참조하십시오.

사용자에게 암호가 있더라도 AWS 리소스에 액세스하려면 권한이 필요합니다. 기본적으로 사용자에게는 권한이 없습니다. 사용자에게 필요한 권한을 부여하려면 해당 사용자 또는 사용자가 속한 그룹에 정책을 할당합니다. 사용자 및 그룹 만들기에 대한 자세한 내용은 자격 증명(사용자, 그룹, 및 역할) (p. 83)을 참조하십시오. 권한 설정을 위한 정책 사용에 대한 자세한 내용은 IAM 사용자의 권한 변경 (p. 96)을 참조하십시오.

자신의 암호를 변경할 권한을 사용자에게 부여할 수 있습니다. 자세한 내용은 IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108) 단원을 참조하십시오. 사용자가 계정 로그인 페이지에 액세스하는 방법에 대한 자세한 내용은 IAM 콘솔 및 로그인 페이지 (p. 71)를 참조하십시오.

주제

- IAM 사용자 암호 생성, 변경 또는 삭제(콘솔) (p. 105)
- IAM 사용자 암호 생성, 변경 또는 삭제(AWS CLI) (p. 107)
- IAM 사용자 암호 생성, 변경 또는 삭제(AWS API) (p. 108)

IAM 사용자 암호 생성, 변경 또는 삭제(콘솔)

AWS Management 콘솔을 사용하여 IAM 사용자의 암호를 관리할 수 있습니다.

사용자가 조직을 떠나거나 AWS 액세스가 더 이상 필요하지 않은 경우 사용 중인 자격 증명을 찾아서 더 이상 작동하지 않도록 해야 합니다. 더 이상 필요 없는 자격 증명을 삭제하는 것이 가장 좋습니다. 나중에 필요한 경우가 생기면 언제든지 다시 생성할 수 있습니다. 적어도 그 자격 증명을 변경하여 이전 사용자가 더 이상 액세스할 수 없게 해야 합니다.

IAM 사용자의 암호를 추가하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 암호를 생성하려는 사용자의 이름을 선택합니다.
4. 보안 자격 증명(Security credentials) 탭을 선택한 다음, 로그인 자격 증명(Sign-in credentials)에서 콘솔 암호(Console password) 옆에 있는 암호 관리(Manage password)를 선택합니다.

5. 콘솔 액세스 관리(Manage console access)의 콘솔 액세스(Console access)에서 활성화를 선택합니다(선택되어 있지 않은 경우). 콘솔 액세스가 비활성화되어 있는 경우에는 암호가 필요 없습니다.
6. Set password(암호 설정)에 대해서는 IAM에서 암호를 자동으로 생성할지, 아니면 사용자 지정 암호를 만들지를 선택합니다.
   - IAM에서 암호를 자동으로 생성하려면 Autogenerated password(자동 생성 암호)를 선택합니다.
   - 사용자 지정 암호를 만들려면 사용자 지정 암호(Custom password)를 선택하고 암호를 입력합니다.

     Note

     만드는 암호는 계정의 암호 정책 (p. 101)(정책을 설정한 경우)에 부합해야 합니다.
7. 사용자가 로그인할 때 새 암호를 만들도록 요구하려면 암호 재설정 요청(Require password reset)을 선택합니다. 그 다음 적용을 선택합니다.

   Important

   암호 재설정 요청(Require password reset) 옵션을 선택할 경우, 사용자에게 자신의 암호를 변경할 권한이 있는지 확인하십시오. 자세한 내용은 IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108) 단원을 참조하십시오.
8. 암호를 생성하는 옵션을 선택한 경우, 새 비밀번호 대화 상자에서 표시를 선택합니다. 이렇게 하면 암호를 볼 수 있으므로 암호를 사용자와 공유할 수 있습니다.

   Important

   이 단계를 완료한 후에는 보안상의 이유로 암호에 액세스할 수 없지만, 언제든지 새 암호를 만들 수 있습니다.

IAM 사용자의 암호를 변경하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 암호를 변경할 사용자의 이름을 선택합니다.
4. 보안 자격 증명(Security credentials) 탭을 선택한 다음, 로그인 자격 증명(Sign-in credentials)에서 콘솔 암호(Console password) 옆에 있는 암호 관리(Manage password)를 선택합니다.
5. 콘솔 액세스 관리(Manage console access)의 콘솔 액세스(Console access)에서 활성화를 선택합니다(선택되어 있지 않은 경우). 콘솔 액세스가 비활성화되어 있는 경우에는 암호가 필요 없습니다.
6. Set password(암호 설정)에 대해서는 IAM에서 암호를 자동으로 생성할지, 아니면 사용자 지정 암호를 만들지를 선택합니다.
   - IAM에서 암호를 자동으로 생성하려면 Autogenerated password(자동 생성 암호)를 선택합니다.
   - 사용자 지정 암호를 만들려면 사용자 지정 암호(Custom password)를 선택하고 암호를 입력합니다.

     Note

     만드는 암호는 계정의 암호 정책 (p. 101)(정책을 설정한 경우)에 부합해야 합니다.
7. 사용자가 로그인할 때 새 암호를 만들도록 요구하려면 암호 재설정 요청(Require password reset)을 선택합니다. 그 다음 적용을 선택합니다.

   Important

   암호 재설정 요청(Require password reset) 옵션을 선택할 경우, 사용자에게 자신의 암호를 변경할 권한이 있는지 확인하십시오. 자세한 내용은 IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108) 단원을 참조하십시오.
8. 암호를 생성하는 옵션을 선택한 경우, 새 비밀번호 대화 상자에서 표시를 선택합니다. 이렇게 하면 암호를 볼 수 있으므로 암호를 사용자와 공유할 수 있습니다.

Important

이 단계를 완료한 후에는 보안상의 이유로 암호에 액세스할 수 없지만, 언제든지 새 암호를 만들 수 있습니다.

IAM 사용자의 암호를 삭제(비활성화)하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 암호를 삭제할 사용자의 이름을 선택합니다.
4. 보안 자격 증명(Security credentials) 탭을 선택한 다음, 로그인 자격 증명(Sign-in credentials)에서 콘솔 암호(Console password) 옆에 있는 암호 관리(Manage password)를 선택합니다.
5. 콘솔 액세스(Console access)에 대해서는 비활성화에 이어 적용을 선택합니다.

Important

사용자의 암호를 삭제하면 해당 사용자가 더 이상 AWS Management 콘솔에 로그인할 수 없습니다. 사용자에게 액세스 키가 있다면 액세스 키는 계속 제 기능을 수행하고 AWS CLI, Windows PowerShell용 도구 또는 AWS API 함수 호출을 통해 액세스를 허용합니다.

IAM 사용자 암호 생성, 변경 또는 삭제(AWS CLI)

AWS CLI API를 이용해 IAM 사용자의 암호를 관리할 수 있습니다.

암호를 생성하려면(AWS CLI)

1. (선택 사항) 사용자에게 암호가 있는지 확인하려면 aws iam get-login-profile 명령을 실행합니다.
2. 암호를 생성하려면 aws iam create-login-profile 명령을 실행합니다.

사용자의 암호를 변경하려면(AWS CLI)

1. (선택 사항) 사용자에게 암호가 있는지 확인하려면 aws iam get-login-profile 명령을 실행합니다.
2. 암호를 변경하려면 aws iam update-login-profile 명령을 실행합니다.

사용자의 암호를 삭제(비활성화)하려면(AWS CLI)

1. (선택 사항) 사용자에게 암호가 있는지 확인하려면 aws iam get-login-profile 명령을 실행합니다.
2. (선택 사항) 사용자의 암호가 마지막으로 사용된 시간을 확인하려면 aws iam get-user 명령을 실행합니다.
3. 암호를 삭제하려면 aws iam delete-login-profile 명령을 실행합니다.

Important

사용자의 암호를 삭제하면 해당 사용자가 더 이상 AWS Management 콘솔에 로그인할 수 없습니다. 사용자에게 액세스 키가 있다면 액세스 키는 계속 제 기능을 수행하고 AWS CLI, Windows PowerShell용 도구 또는 AWS API 함수 호출을 통해 액세스를 허용합니다. AWS CLI, Windows PowerShell용 도구 또는 AWS API를 사용하여 AWS 계정에서 사용자를 삭제하는 경우 먼저 이 작업을 사용하여 암호를 삭제해야 합니다. 자세한 내용은 IAM 사용자 삭제(AWS CLI) (p. 95) 단원을 참조하십시오.

IAM 사용자 암호 생성, 변경 또는 삭제(AWS API)

AWS API를 이용해 IAM 사용자의 암호를 관리할 수 있습니다.

암호를 생성하려면(AWS API)

1. (선택 사항) 사용자에게 암호가 있는지 확인하려면 GetLoginProfile 연산을 호출합니다.
2. 암호를 생성하려면 CreateLoginProfile 연산을 호출합니다.

사용자의 암호를 변경하려면(AWS API)

1. (선택 사항) 사용자에게 암호가 있는지 확인하려면 GetLoginProfile 연산을 호출합니다.
2. 암호를 변경하려면 UpdateLoginProfile 연산을 호출합니다.

사용자의 암호를 삭제(비활성화)하려면(AWS API)

1. (선택 사항) 사용자에게 암호가 있는지 확인하려면 GetLoginProfile 명령을 실행합니다.
2. (선택 사항) 사용자의 암호가 마지막으로 사용된 시간을 확인하려면 GetUser 명령을 실행합니다.
3. 암호를 삭제하려면 DeleteLoginProfile 명령을 실행합니다.

> **Important**
>
> 사용자의 암호를 삭제하면 해당 사용자가 더 이상 AWS Management 콘솔에 로그인할 수 없습니다. 사용자에게 액세스 키가 있다면 액세스 키는 계속 제 기능을 수행하고 AWS CLI, Windows PowerShell용 도구 또는 AWS API 함수 호출을 통해 액세스를 허용합니다. AWS CLI, Windows PowerShell용 도구 또는 AWS API를 사용하여 AWS 계정에서 사용자를 삭제하는 경우 먼저 이 작업을 사용하여 암호를 삭제해야 합니다. 자세한 내용은 IAM 사용자 삭제(AWS CLI) (p. 95) 단원을 참조하십시오.

IAM 사용자에게 자신의 암호 변경 허용하기

IAM 사용자에게 AWS Management 콘솔에 로그인하기 위해 자신의 암호를 변경할 권한을 부여할 수 있습니다. 이 작업을 두 가지 방법으로 수행할 수 있습니다.

- 계정의 모든 IAM 사용자에게 자신의 암호 변경을 허용합니다 (p. 108).
- 선택된 IAM 사용자에게만 자신의 암호 변경을 허용합니다 (p. 109). 이 시나리오에서는 모든 사용자의 암호 변경 옵션을 비활성화한 후 IAM 정책을 사용하여 일부 사용자에게만 암호, 그리고 선택 사항으로 액세스 키와 같은 기타 자격 증명을 변경할 수 있는 권한을 부여합니다.

> **Important**
>
> 사용자가 강력한 암호를 만들도록 암호 정책을 설정 (p. 101)하는 것이 좋습니다.

모든 IAM 사용자에게 자신의 암호 변경을 허용하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 계정 설정을 클릭합니다.
3. 암호 정책 섹션에서 사용자 자신의 암호 변경 허용(Allow users to change their own password)을 선택한 후 암호 정책 적용(Apply Password Policy)을 클릭합니다.
4. 사용자가 암호 변경 방법이 나와 있는 IAM 사용자가 자신의 암호를 변경하는 방법 (p. 110) 지침을 따르도록 해야 합니다.

계정의 암호 정책(모든 사용자가 직접 암호를 변경하게 하는 정책 포함) 변경에 사용할 수 있는 AWS CLI, Windows PowerShell용 도구 및 API 명령에 대한 자세한 내용은 암호 정책 설정(AWS CLI) (p. 104) 단원을 참조하십시오.

선택된 IAM 사용자에게 자신의 암호 변경을 허용하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 계정 설정을 클릭합니다.
3. 계정 설정 섹션에서 사용자의 본인 암호 변경 허용(Allow users to change their own password) 확인란이 해제되어 있는지 확인합니다. 이 확인란을 선택하면 모든 사용자가 직접 암호를 변경할 수 있게 됩니다. (위 절차 참조).
4. 암호를 변경하도록 허용할 사용자가 아직 없다면 사용자를 만듭니다. 세부 정보는 AWS 계정의 IAM 사용자 생성 (p. 87) 단원을 참조하십시오.
5. 직접 암호를 변경하게 할 IAM 사용자 그룹을 만든 다음 앞 단계에서 만든 사용자를 그룹에 추가합니다. 자세한 내용은 첫 번째 IAM 관리자 및 그룹 생성 (p. 20) 및 IAM 그룹 관리 (p. 169) 단원을 참조하십시오.

   이 단계는 선택 사항이지만, 그룹을 사용하여 권한을 관리하면 사용자를 그룹에 추가 및 삭제하고 전체 그룹에 대해 일괄적으로 권한을 변경할 수 있어 더욱 편리합니다.
6. 그룹에 다음 정책을 할당합니다. 세부 정보는 IAM 정책 관리 (p. 435) 단원을 참조하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:GetAccountPasswordPolicy",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:ChangePassword",
      "Resource": "arn:aws:iam::account-id-without-hyphens:user/${aws:username}"
    }
  ]
}
```

   이 정책은 암호 변경 작업에 대한 액세스 권한을 부여하여 사용자가 콘솔, AWS CLI, Windows PowerShell용 도구 또는 API로부터 본인의 암호만을 변경할 수 있게 합니다. 또한, 사용자가 현재 암호 정책을 볼 수 있도록 GetAccountPasswordPolicy 작업에 대한 액세스 권한도 부여합니다. 이 권한은 사용자가 콘솔에서 비밀번호 변경 페이지를 표시하는 데 필요합니다. 사용자는 반드시 현재 암호 정책을 읽고 변경된 암호가 정책의 요건을 충족하는지 확인해야 합니다.
7. 사용자가 암호 변경 방법이 나와 있는 IAM 사용자가 자신의 암호를 변경하는 방법 (p. 110) 지침을 따르도록 해야 합니다.

자세한 정보

자격 증명 관리에 대한 자세한 내용은 다음 주제를 참조하십시오.

- IAM 사용자에게 자신의 암호 변경 허용하기 (p. 108)
- 암호 관리 (p. 100)
- IAM 사용자의 계정 암호 정책 설정 (p. 101)
- IAM 정책 관리 (p. 435)
- IAM 사용자가 자신의 암호를 변경하는 방법 (p. 110)

IAM 사용자가 자신의 암호를 변경하는 방법

자신의 IAM 사용자 암호를 변경할 수 있는 권한이 부여된 경우 AWS Management 콘솔의 특별 페이지를 사용하여 이 작업을 수행할 수 있습니다. AWS CLI 또는 AWS API도 사용할 수 있습니다.

주제

필요한 권한

자신의 IAM 사용자에 대한 암호를 변경하려면 다음 정책에 따른 권한이 있어야 합니다. AWS: IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 콘솔 암호를 변경할 수 있도록 허용합니다. (p. 398)

IAM 사용자가 자신의 암호를 변경하는 방법(콘솔)

다음 절차는 IAM 사용자가 AWS Management 콘솔을 사용하여 자신의 암호를 변경하는 방법을 설명합니다.

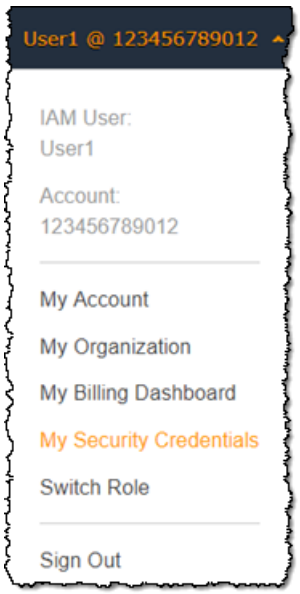
자신의 IAM 사용자 암호를 변경하려면(콘솔)

1. AWS 계정 ID나 계정 별칭, IAM 사용자 이름 및 암호를 사용하여 IAM 콘솔에 로그인합니다.

   Note

   사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 이전에 다른 사용자로 로그인한 경우 페이지 하단 근처의 Sign in to a different account(다른 계정에 로그인)를 선택하여 기본 로그인 페이지로 돌아갑니다. 여기서 AWS 계정 ID 또는 계정 별칭을 입력하면 계정의 IAM 사용자 로그인 페이지로 리디렉션됩니다.

   AWS 계정 ID를 받으려면 관리자에게 문의하십시오.
2. 오른쪽 상단의 탐색 모음에서 사용자 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)를 선택합니다.



3. AWS IAM Credentials(AWS IAM 자격 증명) 탭에서 비밀번호 변경을 선택합니다.

4. Current password(현재 암호)에 현재 암호를 입력합니다. New password(새 암호) 및 Confirm new password(새 암호 확인)에 새 암호를 입력합니다. 그런 다음 Change password(암호 변경)를 클릭합니다.

   Note

   계정에 암호 정책이 있는 경우에는 새 암호가 해당 정책의 요건을 따라야 합니다. 자세한 내용은 IAM 사용자의 계정 암호 정책 설정 (p. 101) 단원을 참조하십시오.

IAM 사용자가 자신의 암호를 변경하는 방법(AWS CLI 또는 AWS API)

다음 절차는 IAM 사용자가 AWS CLI 또는 AWS API를 사용하여 자신의 암호를 변경하는 방법을 설명합니다.

자신의 IAM 암호를 변경하려면 다음을 사용하십시오.

- AWS CLI: `aws iam change-password`
- AWS API: `ChangePassword`

IAM 사용자의 액세스 키 관리

Follow us on Twitter

Note

웹 사이트에서 Amazon 제품을 팔기 위해 Product Advertising API를 구성하기 위해 이 주제를 찾았다면 다음 주제들 단원을 참조하십시오.

- Product Advertising API로 시작하기
- Product Advertising API 개발자로서 시작하기

액세스 키는 IAM 사용자 또는 AWS 계정 루트 사용자에 대한 장기 자격 증명입니다. 액세스 키를 사용하여 AWS CLI 또는 AWS API에 대한 프로그래밍 요청에 서명할 수 있습니다(직접 또는 AWS SDK를 사용하여). 자세한 내용은 Amazon Web Services 일반 참조의 AWS API 요청 서명을 참조하십시오.

액세스 키는 액세스 키 ID(예: `AKIAIOSFODNN7EXAMPLE`)와 보안 액세스 키(예: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)의 2가지 부분으로 구성됩니다. 사용자 이름 및 암호와 같이 액세스 키 ID와 보안 액세스 키를 함께 사용하여 요청을 인증해야 합니다. 사용자 이름과 암호를 관리하는 것처럼 안전하게 액세스 키를 관리합니다.

Important

정식 사용자 ID를 찾는 데 도움이 되더라도 액세스 키를 제3자에게 제공하지 마십시오. 이로 인해 다른 사람에게 계정에 대한 영구 액세스를 제공하게 될 수 있습니다.

가장 좋은 방법은 액세스 키 대신 임시 보안 자격 증명(IAM 역할)을 사용하고 모든 AWS 계정 루트 사용자 액세스 키는 비활성화하는 것입니다. 자세한 내용은 Amazon Web Services 일반 참조의 AWS 액세스 키 관리 모범 사례 단원을 참조하십시오.

장기 액세스 키를 사용해야 하는 경우 액세스 키(액세스 키 ID 및 보안 액세스 키)를 생성, 수정, 보기 또는 교체할 수 있습니다. 최대 두 개의 액세스 키를 가질 수 있습니다. 이렇게 하면 모범 사례에 따라 활성 키를 교체할 수 있습니다.

액세스 키 페어를 생성할 때는 액세스 키 ID와 보안 액세스 키를 안전한 위치에 저장합니다. 보안 액세스 키는 생성할 때만 사용할 수 있습니다. 보안 액세스 키를 분실한 경우 액세스 키를 삭제하고 새 키를 생성해야 합니다. 자세한 내용은 분실하거나 잊어버린 암호 또는 액세스 키 재설정 (p. 118) 단원을 참조하십시오.

주제

필요한 권한

자신의 IAM 사용자에 대한 액세스 키를 생성하려면 다음 정책에 따른 권한이 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateOwnAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:CreateAccessKey",
                "iam:GetUser",
                "iam:ListAccessKeys"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        }
    ]
}
```

자신의 IAM 사용자에 대한 액세스 키를 교체하려면 다음 정책에 따른 권한이 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageOwnAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:CreateAccessKey",
                "iam:DeleteAccessKey",
                "iam:GetAccessKeyLastUsed",
                "iam:GetUser",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        }
    ]
}
```

액세스 키 관리(콘솔)

AWS Management 콘솔을 사용하여 IAM 사용자의 액세스 키를 관리할 수 있습니다.

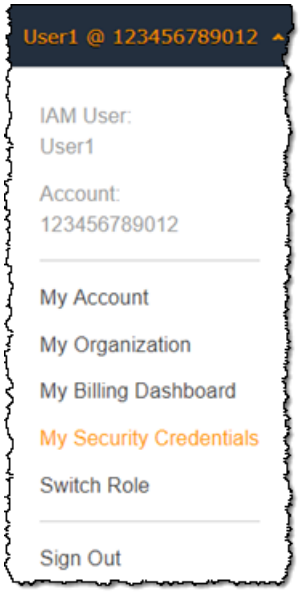
자신의 IAM 사용자 액세스 키를 생성, 수정 또는 삭제하려면(콘솔)

1. AWS 계정 ID나 계정 별칭, IAM 사용자 이름 및 암호를 사용하여 IAM 콘솔에 로그인합니다.

> **Note**
>
> 사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 이전에 다른 사용자로 로그인한 경우 페이지 하단 근처의 Sign in to a different account(다른 계정에 로그인)를 선택하여 기본 로그인 페이지로 돌아갑니다. 여기서 AWS 계정 ID 또는 계정 별칭을 입력하면 계정의 IAM 사용자 로그인 페이지로 리디렉션됩니다.

AWS 계정 ID를 받으려면 관리자에게 문의하십시오.

2. 오른쪽 상단의 탐색 모음에서 사용자 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)를 선택합니다.



3. AWS IAM Credentials(AWS IAM 자격 증명) 탭의 Access keys for CLI, SDK, and API access(CLI, SDK 및 API 액세스를 위한 액세스 키) 섹션에서 다음 작업을 수행합니다.

   - 액세스 키를 생성하려면 Create access key(액세스 키 생성)을 선택합니다. 그런 다음 Download .csv file(.csv 파일 다운로드)를 선택하여 액세스 키 ID 및 보안 액세스 키를 컴퓨터에 `.csv` 파일로 저장합니다. 안전한 위치에 파일을 저장합니다. 이 대화 상자를 닫은 후에는 보안 액세스 키에 다시 액세스할 수 없습니다. `.csv` 파일을 다운로드한 후 닫기를 클릭합니다. 액세스 키를 생성하면 키 페어가 기본적으로 활성화되므로 해당 페어를 즉시 사용할 수 있습니다.
   - 활성 상태의 액세스 키를 비활성화하려면 비활성화를 선택합니다.
   - 비활성 상태의 액세스 키를 다시 활성화하려면 활성화를 선택합니다.
   - 액세스 키를 삭제하려면 행의 맨 왼쪽에 있는 X 버튼을 선택합니다. 삭제를 선택하여 확인합니다. 액세스 키를 삭제하면 영구 삭제되어 되돌릴 수 없습니다. 그러나 언제든지 새 키를 만들 수 있습니다.

다른 IAM 사용자의 액세스 키를 생성, 수정 또는 삭제하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Users(사용자)를 선택합니다.
3. 액세스 키를 관리하려는 사용자 이름을 선택한 다음 보안 자격 증명 탭을 선택합니다.
4. 액세스 키 섹션에서 다음 작업을 수행합니다.

   - 액세스 키를 생성하려면 Create access key(액세스 키 생성)을 선택합니다. 그런 다음 .csv 파일 다운로드를 선택하여 액세스 키 ID 및 보안 액세스 키를 컴퓨터에 CSV 파일로 저장합니다. 안전한 위치에 파일을 저장합니다. 이 대화 상자를 닫은 후에는 보안 액세스 키에 다시 액세스할 수 없습니다. CSV

파일을 다운로드한 후 닫기를 선택합니다. 액세스 키를 생성하면 키 페어가 기본적으로 활성화되므로 해당 페어를 즉시 사용할 수 있습니다.

- 활성 상태의 액세스 키를 비활성화하려면 비활성화를 선택합니다.
- 비활성 상태의 액세스 키를 다시 활성화하려면 활성화를 선택합니다.
- 액세스 키를 삭제하려면 행의 맨 왼쪽에 있는 X 버튼을 선택합니다. 삭제를 선택하여 확인합니다. 액세스 키를 삭제하면 영구 삭제되어 되돌릴 수 없습니다. 그러나 언제든지 새 키를 만들 수 있습니다.

IAM 사용자에 대한 액세스 키를 나열하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 해당 사용자의 이름을 선택한 후 보안 자격 증명 탭을 선택합니다. 사용자의 액세스 키와 각 키의 상태가 표시됩니다.

   Note

   사용자의 액세스 키 ID만 표시됩니다. 보안 액세스 키는 키를 만들 때만 가져올 수 있습니다.

여러 IAM 사용자의 액세스 키 ID를 나열하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 필요할 경우 다음 단계를 통해 사용자 테이블에 액세스 키 ID 열을 추가합니다.

   a. 테이블 위 맨 오른쪽에서 설정 아이콘( )을 선택합니다.
   b. Manage columns(열 관리)에서 액세스 키 ID를 선택합니다.
   c. 닫기를 선택하여 사용자 목록으로 돌아갑니다.
4. 액세스 키 ID 열에는 각 액세스 키 ID가 표시되고 그 다음에 키의 상태가 표시됩니다. 예: 234782070278420732307623740 23 (Active) 또는 220937402396702370248434203 27 (Inactive).

   이 정보를 사용하여 한 개 또는 두 개의 액세스 키를 가진 사용자의 액세스 키를 보고 복사할 수 있습니다. 액세스 키가 없는 사용자는 이 열에 없음이라고 표시됩니다.

   Note

   사용자의 액세스 키 ID와 상태만 표시됩니다. 보안 액세스 키는 키를 만들 때만 가져올 수 있습니다.

어떤 IAM 사용자가 특정 액세스 키를 소유하고 있는지 확인하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 검색 상자에 해당 사용자의 액세스 키 ID를 입력하거나 붙여 넣습니다.
4. 필요할 경우 다음 단계를 통해 사용자 테이블에 액세스 키 ID 열을 추가합니다.

   a. 테이블 위 맨 오른쪽에서 설정 아이콘( )을 선택합니다.
   b. Manage columns(열 관리)에서 액세스 키 ID를 선택합니다.
   c. 닫기를 선택하여 사용자 목록으로 돌아간 후 지정된 액세스 키를 소유하는 사용자로 필터링되었는지 확인합니다.

액세스 키 관리(AWS CLI)

AWS CLI에서 IAM 사용자의 액세스 키를 관리하려면 다음 명령을 실행합니다.

- 액세스 키 생성: `aws iam create-access-key`
- 액세스 키 비활성화 또는 다시 활성화: `aws iam update-access-key`
- 사용자의 액세스 키를 나열하려면: `aws iam list-access-keys`
- 가장 최근에 액세스 키를 사용한 시기 확인: `aws iam get-access-key-last-used`
- 액세스 키 삭제: `aws iam delete-access-key`

액세스 키 관리(AWS API)

AWS API에서 IAM 사용자의 액세스 키를 관리하려면 다음 작업을 호출합니다.

- 액세스 키 생성: `CreateAccessKey`
- 액세스 키 비활성화 또는 다시 활성화: `UpdateAccessKey`
- 사용자의 액세스 키를 나열하려면: `ListAccessKeys`
- 가장 최근에 액세스 키를 사용한 시기 확인: `GetAccessKeyLastUsed`
- 액세스 키 삭제: `DeleteAccessKey`

액세스 키 교체

최상의 보안을 위해 IAM 사용자 액세스 키를 정기적으로 교체(변경)하는 것이 좋습니다. 관리자가 필요한 권한을 부여한 경우 사용자 고유의 액세스 키를 교체할 수 있습니다.

관리자가 사용자에게 액세스 키를 직접 교체할 수 있는 권한을 부여하는 방법에 대한 자세한 내용은 AWS: IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 암호, 액세스 키 및 SSH 퍼블릭 키를 관리할 수 있도록 허용합니다. (p. 399) 단원을 참조하십시오. 또한, 모든 IAM 사용자가 주기적으로 암호를 교체하도록 요구하는 암호 정책을 계정에 적용할 수 있습니다. 얼마나 자주 교체하도록 할지 선택할 수 있습니다. 자세한 내용은 IAM 사용자의 계정 암호 정책 설정 (p. 101) 단원을 참조하십시오.

> **Important**
>
> 가장 좋은 방법은 AWS 계정 루트 사용자를 사용하지 않는 것입니다. AWS 계정 루트 사용자 자격 증명을 사용할 경우 그 자격 증명도 정기적으로 교체할 것을 권장합니다. 계정 암호 정책은 루트 사용자 자격 증명에는 적용되지 않습니다. IAM 사용자는 AWS 계정 루트 사용자의 자격 증명을 관리할 수 없으므로 루트 사용자의 자격 증명(사용자의 자격 증명이 아님)을 사용하여 루트 사용자 자격 증명을 변경해야 합니다. AWS의 일상적인 작업에서는 루트 사용자를 사용하지 않는 것이 좋습니다.

주제

IAM 사용자 액세스 키 교체(콘솔)

AWS Management 콘솔에서 액세스 키를 교체할 수 있습니다.

애플리케이션을 중단하지 않고 IAM 사용자의 액세스 키를 교체하려면(콘솔)

1. 최초 액세스 키가 활성 상태일 때 두 번째 액세스 키를 만듭니다.

a. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
b. 탐색 창에서 Users(사용자)를 선택합니다.
c. 해당 사용자의 이름을 선택한 후 보안 자격 증명 탭을 선택합니다.
d. Create access key(액세스 키 생성)을 선택하고 Download .csv file(.csv 파일 다운로드)를 선택하여 액세스 키 ID와 보안 액세스 키를 컴퓨터의 `.csv` 파일에 저장합니다. 안전한 위치에 파일을 저장합니다. 이 단계를 끝낸 후에는 보안 액세스 키에 다시 액세스할 수 없습니다. `.csv` 파일을 다운로드한 후 닫기를 클릭합니다.

   새 액세스 키는 기본적으로 활성화됩니다. 따라서 사용자에게 두 개의 활성 액세스 키가 생깁니다.

2. 새 액세스 키를 사용하도록 모든 애플리케이션과 도구를 업데이트합니다.
3. 가장 오래된 액세스 키의 Last used(마지막 사용) 열을 검토하여 최초 액세스 키가 아직 사용 중인지 확인합니다. 한 가지 접근 방식은 며칠을 기다린 다음 계속하기 전에 사용된 적이 있는 기존 액세스 키가 있는지 확인하는 것입니다.
4. Last used(마지막 사용) 열에 오래된 키가 사용된 적이 없다고 표시되더라도 최초 액세스 키를 바로 삭제하지 않는 것이 좋습니다. 대신 Make inactive(비활성화)를 선택하여 최초 액세스 키를 비활성화합니다.
5. 새 액세스 키만 사용하여 애플리케이션이 작동 중인지 확인합니다. 원래 액세스 키를 계속 사용하는 어떤 애플리케이션도 AWS 리소스에 더 이상 액세스할 수 없기 때문에 이 시점에 작업을 중단합니다. 그러한 애플리케이션 또는 도구를 찾는다면 활성화(Make active)를 선택하여 최초 액세스 키를 다시 활성화할 수 있습니다. 그런 다음 Step 3 (p. 116) 단원으로 돌아가 이 애플리케이션을 업데이트하여 새 키를 사용하십시오.
6. 일정 기간 기다린 후 모든 애플리케이션과 도구가 업데이트되었는지 확인한 뒤에 최초 액세스 키를 삭제할 수 있습니다:

   a. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
   b. 탐색 창에서 사용자를 선택합니다.
   c. 해당 사용자의 이름을 선택한 후 보안 자격 증명 탭을 선택합니다.
   d. 삭제할 액세스 키를 찾아 해당 행 맨 오른쪽에 있는 X 버튼을 선택합니다. 삭제를 선택하여 확인합니다.

액세스 키 교체 시점을 결정하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 필요할 경우 다음 단계를 통해 사용자 테이블에 Access key age(액세스 키 수명) 열을 추가합니다.

   a. 테이블 위 맨 오른쪽에서 설정 아이콘( )을 선택합니다.
   b. Manage Columns(열 관리)에서 Access key age(액세스 키 수명)을 선택합니다.
   c. 닫기를 선택하여 사용자 목록으로 돌아갑니다.

4. Access key age(액세스 키 수명) 열에는 가장 오래된 활성 액세스 키가 생성된 이후로 경과한 일수가 표시됩니다. 이 정보를 사용하여 교체가 필요한 액세스 키를 소유한 사용자를 확인할 수 있습니다. 액세스 키가 없는 사용자는 이 열에 없음이라고 표시됩니다.

액세스 키 교체(AWS CLI)

AWS Command Line Interface에서 액세스 키를 교체할 수 있습니다.

애플리케이션을 중단하지 않고 액세스 키를 교체하려면(AWS CLI)

1. 최초 액세스 키가 활성 상태일 때 두 번째 액세스 키를 만들면 이 키도 기본적으로 활성 상태가 됩니다. 다음 명령을 실행합니다.

   - `aws iam create-access-key`

   따라서 사용자에게 두 개의 활성 액세스 키가 생깁니다.
2. 새 액세스 키를 사용하도록 모든 애플리케이션과 도구를 업데이트합니다.
3. 다음 명령을 사용하여 최초 액세스 키가 아직 사용 중인지 확인합니다.

   - `aws iam get-access-key-last-used`

   한 가지 접근 방식은 며칠을 기다린 다음 계속하기 전에 사용된 적이 있는 기존 액세스 키가 있는지 확인하는 것입니다.
4. Step 3 단계를 통해 기존 키를 사용한 적이 없다는 것이 밝혀진 경우 최초의 액세스 키를 즉시 삭제하지 말 것을 권장합니다. 그 대신 다음 명령을 사용하여 최초 액세스 키의 상태를 `Inactive`로 변경하십시오.

   - `aws iam update-access-key`
5. 새 액세스 키만 사용하여 애플리케이션이 작동 중인지 확인합니다. 원래 액세스 키를 계속 사용하는 어떤 애플리케이션도 AWS 리소스에 더 이상 액세스할 수 없기 때문에 이 시점에 작업을 중단합니다. 그러한 애플리케이션 또는 도구를 찾는다면 그 상태를 `Active`로 되돌려 최초 액세스 키를 다시 활성화할 수 있습니다. 그런 다음 Step 2 단계로 돌아가 이 애플리케이션을 업데이트해 새 키를 사용하십시오.
6. 일정 기간 기다린 후 모든 애플리케이션과 도구가 업데이트되었는지 확인한 뒤에 다음 명령을 사용하여 최초 액세스 키를 삭제할 수 있습니다.

   - `aws iam delete-access-key`

자세한 내용은 다음 단원을 참조하십시오.

- IAM 사용자의 액세스 키 교체 방법. AWS 보안 블로그의 이 게시물에서는 키 교체에 대한 자세한 내용을 설명합니다.
- IAM 모범 사례 (p. 60). 이 페이지에서는 AWS 리소스를 보호하기 위한 일반적인 권장 사항을 설명합니다.

액세스 키 교체(AWS API)

AWS API를 사용하여 액세스 키를 교체할 수 있습니다.

애플리케이션을 중단하지 않고 액세스 키를 교체하려면(AWS API)

1. 최초 액세스 키가 활성 상태일 때 두 번째 액세스 키를 만들면 이 키도 기본적으로 활성 상태가 됩니다. 다음 작업을 호출합니다.

   - `CreateAccessKey`

   따라서 사용자에게 두 개의 활성 액세스 키가 생깁니다.
2. 새 액세스 키를 사용하도록 모든 애플리케이션과 도구를 업데이트합니다.
3. 다음 연산을 호출하여 최초 액세스 키가 아직 사용 중인지 확인합니다.

   - `GetAccessKeyLastUsed`

   한 가지 접근 방식은 며칠을 기다린 다음 계속하기 전에 사용된 적이 있는 기존 액세스 키가 있는지 확인하는 것입니다.

4. Step 3 단계를 통해 기존 키를 사용한 적이 없다는 것이 밝혀진 경우 최초의 액세스 키를 즉시 삭제하지 말 것을 권장합니다. 그 대신 다음 연산을 호출하여 최초 액세스 키의 상태를 `Inactive`로 변경하십시오.

   - `UpdateAccessKey`
5. 새 액세스 키만 사용하여 애플리케이션이 작동 중인지 확인합니다. 원래 액세스 키를 계속 사용하는 어떤 애플리케이션도 AWS 리소스에 더 이상 액세스할 수 없기 때문에 이 시점에 작업을 중단합니다. 그러한 애플리케이션 또는 도구를 찾는다면 그 상태를 `Active`로 되돌려 최초 액세스 키를 다시 활성화할 수 있습니다. 그런 다음 Step 2 단계로 돌아가 이 애플리케이션을 업데이트해 새 키를 사용하십시오.
6. 일정 기간 기다린 후 모든 애플리케이션과 도구가 업데이트되었는지 확인한 뒤에 다음 연산을 호출하여 최초 액세스 키를 삭제할 수 있습니다.

   - `DeleteAccessKey`

자세한 내용은 다음 단원을 참조하십시오.

- IAM 사용자의 액세스 키 교체 방법. AWS 보안 블로그의 이 게시물에서는 키 교체에 대한 자세한 내용을 설명합니다.
- IAM 모범 사례 (p. 60). 이 페이지에서는 AWS 리소스를 보호하기 위한 일반적인 권장 사항을 설명합니다.

액세스 키 감사

코드에서 AWS 액세스 키를 살펴보면 키가 자신의 계정에 속한 것인지 알 수 있습니다. 액세스 키 ID는 `aws sts get-access-key-info` AWS CLI 명령 또는 `GetAccessKeyInfo` AWS API 작업을 사용해 전달할 수 있습니다.

AWS CLI 및 AWS API 작업은 액세스 키가 속한 AWS 계정의 ID를 반환합니다. `AKIA`로 시작하는 액세스 키 ID는 IAM 사용자 또는 AWS 계정 루트 사용자을 위한 장기 자격 증명입니다. `ASIA`로 시작하는 액세스 키 ID는 AWS STS 작업으로 생성된 임시 자격 증명입니다. 응답으로 반환되는 계정이 자신의 소유라면 루트 사용자로 로그인하여 루트 사용자 액세스 키를 살펴볼 수 있습니다. 그런 다음 자격 증명 보고서 (p. 156)를 가져와서 키를 소유하고 있는 IAM 사용자를 알아볼 수 있습니다. `ASIA` 액세스 키의 경우 누가 임시 자격 증명을 요청했는지 알아보려면 CloudTrail 로그 (p. 334)에서 AWS STS 이벤트를 확인하십시오.

이 작업은 액세스 키의 상태를 표시하지 않지만 키는 활성, 비활성 또는 삭제된 상태일 수 있습니다. 활성 키에도 작업을 실행할 수 있는 권한이 없는 경우도 있습니다. 삭제된 액세스 키를 입력하면 키가 존재하지 않는다는 오류 메시지가 반환될 수 있습니다.

분실하거나 잊어버린 암호 또는 액세스 키 재설정

로그인하는 데 문제가 있습니까? 사용자 유형에 맞는 올바른 AWS 로그인 페이지 (p. 71)에 있는지 확인합니다. 표시되는 로그인 페이지는 사용자 유형에 따라 다릅니다. AWS 계정 루트 사용자(계정 소유자)로 로그인하거나 계정 관리자가 생성한 IAM 사용자로 로그인할 수 있습니다.

기본 로그인 페이지에서 루트 사용자로 로그인하려면 이메일 주소를 입력하고 IAM 사용자로 로그인하려면 계정 ID를 입력해야 합니다. 사용자 유형과 일치하는 로그인 페이지에서만 암호를 제공할 수 있습니다. 로그인 페이지에 대한 자세한 내용은 IAM 콘솔 및 로그인 페이지 (p. 71) 단원을 참조하십시오.

올바른 로그인 페이지에서 암호 또는 액세스 키를 분실하거나 잊어버린 경우 IAM에서 검색할 수 없습니다. 그 대신 다음과 같은 방법으로 재설정할 수는 있습니다.

- AWS 계정 루트 사용자 암호 – 사용자 암호를 잊어버린 경우, AWS Management 콘솔에서 암호를 재설정할 수 있습니다. 자세한 내용은 이 주제의 후반부에 나오는 the section called “잊거나 분실한 루트 사용자 암호 재설정” (p. 119) 단원을 참조하십시오.
- AWS 계정 액세스 키 – 계정 액세스 키를 잊었다면 기존 액세스 키를 비활성화하지 않고 액세스 키를 새로 만들어도 됩니다. 기존 키를 사용하고 있지 않았다면 삭제하면 됩니다. 자세한 내용은 루트 사용자를 위한 액세스 키 생성 (p. 332) 및 루트 사용자로부터 액세스 키 삭제하기 (p. 333) 단원을 참조하십시오.

- IAM 사용자 암호 – IAM 사용자인데 암호를 잊었다면 관리자에게 암호를 재설정해 달라고 부탁해야 합니다. 관리자가 암호를 관리하는 방법에 대한 자세한 내용은 IAM 사용자의 암호 관리 (p. 104) 단원을 참조하십시오.
- IAM 사용자 액세스 키 – IAM 사용자인데 액세스 키를 잊은 경우에는 새 액세스 키가 필요합니다. 고유한 액세스 키를 생성할 권한이 있다면 액세스 키 관리(콘솔) (p. 112) 단원에서 새 액세스 키 생성에 관한 지침을 찾아보십시오. 필요한 권한이 없으면 관리자에게 액세스 키를 새로 생성해 달라고 부탁해야 합니다. 예전 키를 아직 사용하고 있다면 관리자에게 예전 키를 삭제하지 말라고 요청하십시오. 관리자가 액세스 키를 관리하는 방법에 대한 자세한 내용은 IAM 사용자의 액세스 키 관리 (p. 111) 단원을 참조하십시오.

AWS 모범 사례 (p. 65)를 따라 주기적으로 암호와 AWS 액세스 키를 변경해야 합니다. AWS에서는 교체를 통해 액세스 키를 변경합니다. 이는 키를 새로 생성하고, 새로 만든 키를 사용하도록 애플리케이션을 구성한 다음, 이전 키를 삭제한다는 의미입니다. 이런 이유만으로도 동시에 2개의 액세스 키 페어를 활성화하도록 허용합니다. 자세한 내용은 액세스 키 교체 (p. 115) 단원을 참조하십시오.

잊거나 분실한 루트 사용자 암호 재설정

AWS 계정을 처음 생성할 때 이메일 주소와 암호를 입력했습니다. 그 주소와 암호가 바로 AWS 계정 루트 사용자 자격 증명입니다. 루트 사용자 암호를 잊어버린 경우, AWS Management 콘솔에서 암호를 재설정할 수 있습니다.

루트 사용자 암호를 재설정하려면:

1. AWS 계정 이메일 주소를 사용하여 AWS Management 콘솔에 루트 사용자로 로그인한 후 다음을 선택합니다.

   Note

   IAM 사용자 자격 증명으로 AWS Management 콘솔에 로그인되어 있다면 먼저 로그아웃해야 루트 사용자 암호를 재설정할 수 있습니다. 해당 계정의 IAM 사용자 로그인 페이지가 표시되면, 페이지 하단에 있는 루트 계정 자격 증명을 이용한 로그인을 선택합니다. 필요한 경우 계정 이메일 주소를 입력하고 다음을 선택하여 Root user sign in(루트 사용자 로그인) 페이지에 액세스합니다.
2. 비밀번호가 생각나지 않는 경우를 선택합니다.
3. 계정과 연결된 이메일 주소를 입력합니다. 그런 다음 CAPTCHA 텍스트를 입력하고 계속을 선택합니다.
4. AWS 계정과 연결된 이메일로 Amazon Web Services의 메시지가 왔는지 점검합니다. `@amazon.com` 또는 `@aws.amazon.com`으로 끝나는 주소에서 보낸 이메일입니다. 이메일 지침을 따릅니다. 계정으로 이메일이 오지 않았으면 스팸 폴더를 점검합니다. 그 이메일에 더 이상 액세스할 수 없는 경우에는 예전 계정에 액세스해야 합니다 (p. 533) 단원을 참조하십시오.

AWS에서 멀티 팩터 인증(MFA) 사용하기

Follow us on Twitter

보안 강화를 위해 멀티 팩터 인증(MFA)을 구성하여 AWS 리소스를 보호하는 것이 좋습니다. IAM 사용자 또는 AWS 계정 루트 사용자에 대해 MFA를 활성화할 수 있습니다. 루트 사용자에 대해 MFA를 활성화하면 해당 루트 사용자 자격 증명에만 적용됩니다. 이 계정의 IAM 사용자들은 자신의 자격 증명에 더하여 별도로 자격 증명을 갖게 되며, 이 별도의 자격 증명에 고유의 MFA가 구성됩니다.

주제

MFA란 무엇입니까?

MFA는 사용자가 AWS 웹 사이트 또는 서비스에 액세스할 때 사용자의 정규 로그인 자격 증명 외에도 AWS가 지원되는 MFA 메커니즘의 고유 인증을 제출하라고 요청함으로써 보안을 더욱 강화합니다.

- 가상 MFA 디바이스 스마트폰 또는 기타 디바이스에서 실행되며 물리적 디바이스를 에뮬레이션하는 소프트웨어 애플리케이션입니다. 디바이스가 동기화된 1회 암호 알고리즘에 따라 여섯 자리 숫자 코드를 생성합니다. 사용자는 로그인할 때 두 번째 웹페이지에서 디바이스의 유효 코드를 입력해야 합니다. 사용자에게 할당된 각 가상 MFA 디바이스는 고유해야 합니다. 사용자는 다른 사용자의 가상 MFA 디바이스의 코드를 입력하여 인증할 수 없습니다. 가상 MFA는 안전하지 않은 모바일 디바이스에서 실행될 수 있으므로 U2F 디바이스 또는 하드웨어 MFA 디바이스와 동일한 수준의 보안을 제공하지 않을 수 있습니다. 하드웨어 구매 승인을 기다리는 동안 또는 하드웨어 도착을 기다리는 동안 가상 MFA 디바이스를 사용하는 것이 좋습니다. 가상 MFA 디바이스로 사용할 수 있도록 지원되는 몇 가지 앱의 목록은 멀티 팩터 인증 단원을 참조하십시오. AWS를 사용하여 가상 MFA 디바이스를 설정하기 위한 지침은 가상 멀티 팩터 인증(MFA) 디바이스 활성화(콘솔) (p. 122) 단원을 참조하십시오.
- U2F 보안 키. 컴퓨터의 USB 포트에 연결하는 디바이스입니다. U2F는 FIDO Alliance에서 호스팅하는 공개 인증 표준입니다. U2F 보안 키를 활성화하려면, 코드를 수동으로 입력하는 대신, 본인의 자격 증명을 입력한 다음 디바이스를 터치하여 로그인합니다. 지원되는 AWS U2F 보안 키에 대한 자세한 내용은 멀티 팩터 인증 단원을 참조하십시오. AWS를 사용하여 가상 U2F 보안 키를 설정하기 위한 지침은 U2F 보안 키 활성화(콘솔) (p. 125) 단원을 참조하십시오.
- 하드웨어 MFA 디바이스 동기화된 1회 암호 알고리즘에 따라 여섯 자리 숫자 코드를 생성하는 하드웨어 디바이스입니다. 사용자는 로그인할 때 두 번째 웹페이지에서 디바이스의 유효 코드를 입력해야 합니다. 사용자에게 할당된 각 MFA 디바이스는 고유해야 합니다. 사용자는 다른 사용자의 디바이스의 코드를 입력하여 인증받을 수 없습니다. 지원되는 하드웨어 MFA 디바이스에 대한 자세한 내용은 멀티 팩터 인증 단원을 참조하십시오. AWS를 사용하여 하드웨어 MFA 디바이스를 설정하기 위한 지침은 하드웨어 MFA 디바이스 활성화(콘솔) (p. 130) 단원을 참조하십시오.
- SMS 문자 메시지 기반 MFA. IAM 사용자 설정이 해당 사용자의 SMS 호환 모바일 디바이스의 전화번호를 포함하는 MFA 유형입니다. 사용자가 로그인하면 AWS가 SMS 문자 메시지로 여섯 자리 숫자 코드를 사용자의 모바일 디바이스로 전송합니다. 사용자는 로그인 시 두 번째 웹 페이지에서 이 코드를 입력해야 합니다. SMS 기반 MFA는 IAM 사용자만 사용할 수 있습니다. AWS 계정 루트 사용자에서는 이러한 유형의 MFA를 사용할 수 없습니다. SMS 문자 메시지 기반 MFA 활성화에 대한 자세한 내용은 미리 보기 – SMS 문자 메시지 MFA 디바이스 활성화 (p. 135) 단원을 참조하십시오.

  Note

  AWS는 곧 SMS 멀티 팩터 인증(MFA) 지원을 종료할 예정입니다. 신규 고객은 이 기능을 미리 볼 수 없습니다. 기존 고객은 가상(소프트웨어 기반) MFA 디바이스 (p. 122), U2F 보안 키 (p. 125) 또는 하드웨어 MFA 디바이스 (p. 130) 등 MFA의 대체 방법 중 하나로 전환하는 것이 좋습니다. 계정의 사용자 중에서 SMS MFA 디바이스가 할당된 사용자를 볼 수 있습니다. 이렇게 하려면 IAM 콘솔로 이동하여 탐색 창에서 사용자를 선택하고 표의 MFA 열에서 SMS가 표시된 사용자를 찾습니다.

AWS MFA에 대한 공통 질문 답변은 AWS Multi-Factor Authentication FAQ에서 확인할 수 있습니다.

MFA 디바이스 활성화

MFA 구성 단계는 사용하고 있는 MFA 디바이스의 유형에 따라 다릅니다.

주제

- 가상 멀티 팩터 인증(MFA) 디바이스 활성화(콘솔) (p. 122)
- U2F 보안 키 활성화(콘솔) (p. 125)
- 하드웨어 MFA 디바이스 활성화(콘솔) (p. 130)
- 미리 보기 – SMS 문자 메시지 MFA 디바이스 활성화 (p. 135)
- 가상 MFA 디바이스 활성화 및 관리(AWS CLI 또는 AWS API) (p. 136)

MFA 디바이스 활성화의 일반적 단계

다음 개요 절차에는 MFA를 설정하고 사용하는 방법이 설명되어 있으며, 관련된 정보에 대한 링크가 나와 있습니다.

1. 다음과 같은 MFA 디바이스를 가져옵니다. MFA 디바이스는 AWS 계정 루트 사용자 1개 또는 IAM 사용자 1명 당 단 1개를 활성화할 수 있습니다.
   - 가상 MFA 디바이스로, 표준 기반 TOTP(시간 기반 일회용 암호) 알고리즘인 RFC 6238과 호환되는 소프트웨어 애플리케이션. 앱을 스마트폰이나 다른 디바이스에 설치할 수 있습니다. 가상 MFA 디바이스로 사용할 수 있도록 지원되는 몇 가지 앱의 목록은 멀티 팩터 인증 단원을 참조하십시오.
   - AWS 지원 구성 (p. 129)을 갖춘 U2F 보안 키(예: 멀티 팩터 인증 페이지에서 논의한 U2F 디바이스)
   - 하드웨어 기반 MFA 디바이스(예: 멀티 팩터 인증 페이지에서 논의한 AWS 지원 하드웨어 토큰 디바이스).
   - 표준 SMS 문자 메시지를 받을 수 있는 휴대폰.

     메모

     - SMS 기반 MFA를 사용하는 경우 해당 모바일 디바이스 이동 통신 사업자가 부과하는 문자 메시지 요금이 적용될 수 있습니다.
     - SMS 기반 MFA는 IAM 사용자만 사용할 수 있으며 루트 사용자는 사용할 수 없습니다.
2. MFA 디바이스를 활성화합니다.
   - 가상 또는 하드웨어 MFA 디바이스를 보유한 IAM 사용자: AWS Management 콘솔, AWS CLI 또는 IAM API에서 활성화합니다.
   - SMS 문자 메시지를 수신할 수 있는 U2F 보안 키 또는 휴대폰을 보유한 IAM 사용자: AWS Management 콘솔에서만 활성화할 수 있습니다.
   - (루트 사용자에게 지원되지 않는 SMS MFA를 제외한) 모든 유형의 MFA 디바이스를 보유한 AWS 계정 루트 사용자: AWS Management 콘솔에서만 활성화할 수 있습니다.

   각 MFA 디바이스 유형 활성화에 대한 자세한 내용은 다음 페이지를 참조하십시오.
   - 가상 MFA 디바이스: 가상 멀티 팩터 인증(MFA) 디바이스 활성화(콘솔) (p. 122)
   - U2F 보안 키: U2F 보안 키 활성화(콘솔) (p. 125)
   - 하드웨어 MFA 디바이스: 하드웨어 MFA 디바이스 활성화(콘솔) (p. 130)
   - SMS MFA 디바이스: 미리 보기 – SMS 문자 메시지 MFA 디바이스 활성화 (p. 135)
3. AWS 리소스에 로그인하거나 액세스할 때 MFA 디바이스를 사용합니다. 다음 사항에 유의하십시오.
   - U2F 보안 키: AWS 웹 사이트에 액세스하려면 자격 증명을 입력한 다음 메시지가 나타나면 U2F 보안 키를 터치합니다.
   - 가상 MFA 디바이스, 하드웨어 MFA 디바이스 및 SMS MFA 디바이스: AWS 웹 사이트에 액세스하려면 사용자 이름 및 암호 외에도 해당 디바이스의 MFA 코드가 필요합니다. 본인의 로그인에 사용된 IAM 사용자가 SMS를 통해 MFA를 활성화했음을 AWS에서 확인하면, 자동으로 MFA 코드를 구성된 전화번호로 보냅니다.

     MFA 보호 API 작업에 액세스하려면 다음이 필요합니다.
     - MFA 코드
     - MFA 디바이스의 식별자(물리적 디바이스의 일련 번호나 가상 또는 AWS에 정의된 SMS 디바이스의 ARN)
     - 일반 액세스 키 ID 및 보안 액세스 키.

메모

- U2F 보안 키 또는 SMS MFA 디바이스의 MFA 정보를 AWS STS API 작업으로 전달하여 임시 자격 증명을 요청할 수 없습니다.
- AWS CLI 명령 또는 AWS API 작업을 사용하여 U2F 보안 키 (p. 125)를 활성화할 수 없습니다.

자세한 내용은 IAM 로그인 페이지에 MFA 디바이스 사용 (p. 79) 단원을 참조하십시오.

가상 멀티 팩터 인증(MFA) 디바이스 활성화(콘솔)

스마트폰 또는 기타 디바이스를 가상 MFA 디바이스로 사용할 수 있습니다. 이를 위해서는 표준 기반 TOTP(시간 기반 일회용 암호) 알고리즘인 RFC 6238과 호환되는 모바일 앱을 설치해야 합니다. 이러한 앱에서는 6자리 인증 코드가 생성됩니다. 가상 MFA는 안전하지 않은 모바일 디바이스에서 실행될 수 있으므로 U2F 디바이스 또는 하드웨어 MFA 디바이스와 동일한 수준의 보안을 제공하지 않을 수 있습니다. 하드웨어 구매 승인을 기다리는 동안 또는 하드웨어 도착을 기다리는 동안 가상 MFA 디바이스를 사용하는 것이 좋습니다.

대부분의 가상 MFA 앱은 여러 개의 가상 디바이스 생성을 지원하므로 여러 개의 AWS 계정이나 사용자에게 동일한 앱을 사용할 수 있습니다. 그러나 MFA 디바이스는 사용자 1명당 단 1개만 활성화할 수 있습니다.

사용할 수 있는 가상 MFA 앱 목록은 멀티 팩터 인증 단원을 참조하십시오. 단, AWS에서 사용하려면 가상 MFA 앱이 6자리 OTP를 생성해야 합니다.

주제

- 필요한 권한 (p. 122)
- IAM 사용자에 대한 가상 MFA 디바이스 활성화(콘솔) (p. 122)
- AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) (p. 123)
- 가상 MFA 디바이스 교체 또는 "로테이션" (p. 125)

필요한 권한

IAM 사용자의 가상 MFA 디바이스를 관리하려면 다음 정책에 따른 권한이 있어야 합니다. AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 MFA 디바이스를 관리할 수 있도록 허용합니다. (p. 396)

IAM 사용자에 대한 가상 MFA 디바이스 활성화(콘솔)

AWS Management 콘솔에서 IAM을 사용하여 계정의 IAM 사용자를 위한 가상 MFA 디바이스를 활성화 및 관리할 수 있습니다. AWS CLI 또는 AWS API를 사용하여 MFA 장치를 활성화하고 관리하려면 가상 MFA 디바이스 활성화 및 관리(AWS CLI 또는 AWS API) (p. 136) 단원을 참조하십시오.

Note

MFA를 구성하려면 사용자의 가상 MFA 디바이스가 호스팅되는 하드웨어에 대한 물리적 액세스가 필요합니다. 예를 들어, 스마트폰에서 가상 MFA 디바이스를 실행하는 사용자에게 MFA를 구성할 수 있습니다. 이 경우 마법사를 완료하기 위해 스마트폰을 사용할 수 있어야 합니다. 이러한 이유로 사용자가 자신의 가상 MFA 디바이스를 직접 구성 및 관리할 수 있도록 허용하는 것이 좋습니다. 이 경우에는 사용자에게 필요한 IAM 작업 권한을 부여해야 합니다. 이러한 작업 권한을 부여하는 IAM 정책에 대한 자세한 내용과 예는 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 MFA 디바이스를 관리할 수 있도록 허용합니다. (p. 396) 단원을 참조하십시오.

IAM 사용자에 대한 가상 MFA 디바이스 활성화(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.

2. 탐색 창에서 Users(사용자)를 선택합니다.
3. 사용자 이름 목록에서 원하는 MFA 사용자 이름을 선택합니다.
4. Security credentials(보안 자격 증명) 탭을 선택합니다. Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.
5. Manage MFA Device(할당된 MFA 디바이스) 마법사에서 Virtual MFA device(가상 MFA 디바이스 비활성화)를 선택한 후 계속을 선택합니다.

   IAM은 QR 코드 그래픽을 포함하여 가상 MFA 디바이스의 구성 정보를 생성 및 표시합니다. 그래픽은 QR 코드를 지원하지 않는 디바이스 상에서 수동 입력할 수 있는 '보안 구성 키'를 표시한 것입니다.
6. 가상 MFA 앱을 엽니다. 가상 MFA 디바이스의 호스팅에 사용되는 앱 목록은 멀티 팩터 인증을 참조하십시오.

   가상 MFA 앱이 다수의 가상 MFA 디바이스 또는 계정을 지원하는 경우 새로운 가상 MFA 디바이스 또는 계정을 생성하는 옵션을 선택합니다.
7. MFA 앱의 QR 코드 지원 여부를 결정한 후 다음 중 한 가지를 실행합니다.

   - 마법사에서 Show QR code(QT 코드 표시)를 선택한 다음 해당 앱을 사용하여 QR 코드를 스캔합니다. 예를 들어 카메라 모양의 아이콘을 선택하거나 코드 스캔(Scan code)과 비슷한 옵션을 선택한 다음, 디바이스의 카메라를 사용하여 코드를 스캔합니다.
   - Manage MFA Device(MFA 디바이스 관리) 마법사에서 Show secret key(보안 키 표시)을 선택한 다음 MFA 앱에 보안 키를 입력합니다.

   모든 작업을 마치면 가상 MFA 디바이스가 일회용 암호 생성을 시작합니다.
8. Manage MFA Device(MFA 디바이스 관리) 마법사의 MFA code 1(MFA 코드 1) 상자에 현재 가상 MFA 디바이스에 표시된 일회용 암호를 입력합니다. 디바이스가 새로운 일회용 암호를 생성할 때까지 최대 30초 기다립니다. 그런 다음 두 번째 일회용 암호를 MFA code 2(MFA 코드 2) 상자에 입력합니다. Assign MFA(MFA 할당)을 선택합니다.

   > **Important**
   >
   > 코드를 생성한 후 즉시 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화 (p. 138)할 수 있습니다.

이제 AWS에서 가상 MFA 디바이스를 사용할 준비가 끝났습니다. AWS Management 콘솔의 MFA 사용 방법에 대한 자세한 내용은 IAM 로그인 페이지에 MFA 디바이스 사용 (p. 79) 단원을 참조하십시오.

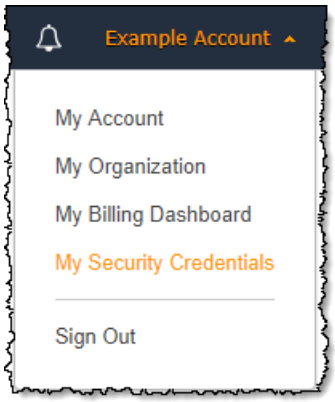
AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔)

AWS Management 콘솔을 사용하여 루트 사용자의 가상 MFA 디바이스를 구성 및 활성화할 수 있습니다. AWS 계정에 대해 MFA 디바이스를 활성화하려면 루트 사용자 자격 증명으로 AWS에 로그인해야 합니다.

루트 사용자용 MFA를 활성화하기 전에 계정 설정과 연락처 정보를 검토하여 이메일 및 전화번호에 대한 액세스 권한이 있는지 확인하십시오. MFA 디바이스가 분실, 도난 또는 작동하지 않는 경우에도 해당 이메일과 전화 번호를 사용하여 자격 증명을 확인함으로써 루트 사용자로 로그인할 수 있습니다. 이러한 다른 인증 요소를 사용하여 로그인하는 방법은 MFA 디바이스 분실 또는 작동 중단 시 문제 해결 (p. 144) 단원을 참조하십시오.

루트 사용자에서 사용할 목적으로 가상 MFA 디바이스를 구성 및 활성화하려면(콘솔)

1. AWS Management 콘솔에 로그인합니다.
2. 탐색 표시줄 오른쪽에서 계정 이름을 선택하고 내 보안 자격 증명(My Security Credentials)을 선택합니다. 필요한 경우 보안 자격 증명으로 계속(Continue to Security Credentials)을 선택합니다. 그런 다음 해당 페이지의 멀티 팩터 인증(MFA) 섹션을 펼칩니다.



3. Activate MFA(MFA 활성화)를 선택합니다.
4. 마법사에서 Virtual MFA device(가상 MFA 디바이스)를 선택한 후 계속을 선택합니다.

   IAM은 QR 코드 그래픽을 포함하여 가상 MFA 디바이스의 구성 정보를 생성 및 표시합니다. 그래픽은 QR 코드를 지원하지 않는 디바이스 상에서 수동 입력할 수 있는 보안 구성 키를 표시한 것입니다.
5. 디바이스에서 가상 MFA 앱을 엽니다.

   가상 MFA 앱이 다수의 가상 MFA 디바이스 또는 계정을 지원하는 경우 새로운 가상 MFA 디바이스 또는 계정을 생성하는 옵션을 선택합니다.
6. 앱을 구성하는 가장 쉬운 방법은 앱을 사용하여 QR 코드를 스캔하는 것입니다. 코드를 스캔하지 못하는 경우 구성 정보를 직접 입력할 수 있습니다. IAM에서 생성된 QR 코드와 보안 구성 키는 AWS 계정과 연동되기 때문에 다른 계정에서는 사용할 수 없습니다. 하지만 사용하던 MFA 디바이스에 대한 액세스 권한을 잃은 경우 재사용을 통해 계정에 대한 새로운 MFA 디바이스를 구성할 수 있습니다.

   - QR 코드를 사용하여 가상 MFA 디바이스를 구성하려면, 마법사에서 Show QR code(QT 코드 표시)를 선택합니다. 그리고 코드 스캔에 대한 앱 지침을 따릅니다. 예를 들어 카메라 모양의 아이콘을 선택하거나, 계정 바코드 스캔(Scan account barcode)과 같은 명령을 선택한 다음, 디바이스의 카메라를 사용하여 QR 코드를 스캔할 수 있습니다.
   - Manage MFA Device(MFA 디바이스 관리) 마법사에서 Show secret key(보안 키 표시)을 선택한 다음 MFA 앱에 보안 키를 입력합니다.

     Important

     QR 코드 또는 보안 구성 키를 안전하게 백업하거나, 혹은 계정의 여러 가상 MFA 디바이스를 활성화하십시오. 예를 들어 가상 MFA 디바이스가 호스팅되어 있는 스마트폰을 분실하는 경우 가상 MFA 디바이스를 사용할 수 없습니다). 이 경우, 계정에 로그인할 수 없으므로 고객 서비스 센터에 연락하여 계정의 MFA 보호 기능을 제거해야 합니다.

   그 디바이스는 6자리 번호를 생성합니다.
7. Manage MFA Device(MFA 디바이스 관리) 마법사의 Authentication Code 1(인증 코드 1) 상자에 MFA 디바이스에 현재 표시된 6자리 번호를 입력합니다. 디바이스가 새 번호를 생성할 때까지 최대 30초를 기다린 후 새로 생성된 6자리 번호를 MFA code 2(MFA 코드 2) 상자에 입력합니다.

   Important

   코드를 생성한 후 즉시 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화 (p. 138)할 수 있습니다.
8. Assign MFA(MFA 할당)을 선택한 다음 완료를 선택합니다.

이제 AWS에서 디바이스를 사용할 준비가 끝났습니다. AWS Management 콘솔의 MFA 사용 방법에 대한 자세한 내용은 IAM 로그인 페이지에 MFA 디바이스 사용 (p. 79) 단원을 참조하십시오.

가상 MFA 디바이스 교체 또는 "로테이션"

한 사용자에게는 한 번에 하나의 MFA 디바이스만 할당할 수 있습니다. 사용자가 디바이스를 분실하거나 이유를 불문하고 교체할 필요가 있을 경우, 먼저 기존 디바이스를 비활성화해야 합니다. 그런 다음, 해당 사용자를 위한 새 디바이스를 추가할 수 있습니다.

- 현재 다른 IAM 사용자와 연결되어 있는 디바이스를 비활성화하는 방법은 MFA 디바이스 비활성화 (p. 142) 단원을 참조하십시오.
- 다른 IAM 사용자를 위한 교체용 가상 MFA 디바이스를 추가하려면 위의 IAM 사용자에 대한 가상 MFA 디바이스 활성화(콘솔) (p. 122) 절차에 나와 있는 단계를 따르십시오.
- AWS 계정 루트 사용자용 교체 가상 MFA 디바이스를 추가하려면 이 주제 앞부분의 AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) (p. 123) 절차에 나오는 단계를 따르십시오.

U2F 보안 키 활성화(콘솔)

U2F(Universal 2nd Factor) 보안 키는 AWS 리소스 보호에 사용할 수 있는 MFA 디바이스 (p. 119)의 한 유형입니다. U2F 보안 키를 컴퓨터의 USB 포트에 연결하여 다음의 지침에 따라 활성화할 수 있습니다. 활성화한 후 로그인 절차를 안전하게 완료하라는 메시지가 나타나면 터치합니다. 이미 다른 서비스에 U2F 보안 키를 사용 중이고 AWS가 지원되는 구성 (p. 129)(예: Yubico의 Yubikey 4 또는 5)을 보유한 경우 AWS에도 사용할 수 있습니다. 그렇지 않은 경우, AWS의 MFA에 U2F를 사용하려면 U2F 보안 키를 구입해야 합니다. 사양 및 구입 관련 정보는 멀티 팩터 인증 단원을 참조하십시오.

U2F는 FIDO Alliance에서 호스팅하는 공개 인증 표준입니다. AWS에서 U2F 키를 활성화하는 경우 U2F 보안 키가 AWS 전용의 새로운 키 페어를 생성합니다. 먼저 자격 증명을 입력합니다. 메시지가 나타나면 U2F 보안 키를 터치하여 AWS에서 야기된 인증 문제에 대응합니다. U2F 표준에 대해 자세히 알아보려면 Universal 2nd Factor 단원을 참조하십시오.

루트 사용자 또는 IAM 사용자별로 (어떤 종류든) 한 개의 MFA 디바이스를 활성화할 수 있습니다.

주제

- 필요한 권한 (p. 125)
- 자신의 IAM 사용자에 대한 U2F 보안 키 활성화(콘솔) (p. 126)
- 다른 IAM 사용자에 대한 U2F 보안 키 활성화(콘솔) (p. 127)
- AWS 계정 루트 사용자에 대한 U2F 보안 키 활성화(콘솔) (p. 128)
- U2F 보안 키 교체 (p. 129)
- U2F 보안 키 사용에 지원되는 구성 (p. 129)

필요한 권한

중요한 MFA 관련 작업을 보호하면서 자신의 IAM 사용자에 대한 U2F 보안 키를 관리하려면 다음 정책에 따른 권한이 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowManageOwnUserMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice",
                "iam:EnableMFADevice",
```

```
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "DenyAllExceptListedIfNoMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:EnableMFADevice",
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

자신의 IAM 사용자에 대한 U2F 보안 키 활성화(콘솔)

AWS Management 콘솔에서만 자신의 IAM 사용자에 대한 U2F 보안 키를 활성화할 수 있으며, AWS CLI 또는 AWS API에서는 활성화할 수 없습니다.

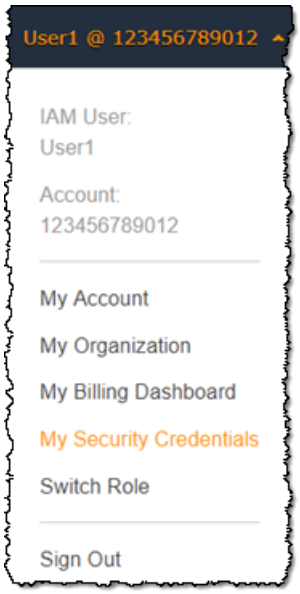
> **Note**
>
> U2F 보안 키를 활성화하려면 디바이스에 물리적으로 액세스할 수 있어야 합니다.

자신의 IAM 사용자에 대한 U2F 보안 키를 활성화하려면(콘솔)

1. AWS 계정 ID나 계정 별칭, IAM 사용자 이름 및 암호를 사용하여 IAM 콘솔에 로그인합니다.

   > **Note**
   >
   > 사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 이전에 다른 사용자로 로그인한 경우 페이지 하단 근처의 Sign in to a different account(다른 계정에 로그인)를 선택하여 기본 로그인 페이지로 돌아갑니다. 여기서 AWS 계정 ID 또는 계정 별칭을 입력하면 계정의 IAM 사용자 로그인 페이지로 리디렉션됩니다.

   AWS 계정 ID를 받으려면 관리자에게 문의하십시오.
2. 오른쪽 상단의 탐색 모음에서 사용자 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)를 선택합니다.



3. AWS IAM credentials(AWS IAM 자격 증명) 탭의 Multi-factor authentication(멀티 팩터 인증) 섹션에서 Manage MFA device(내 MFA 디바이스 관리)를 선택합니다.
4. Manage MFA device(MFA 디바이스 관리) 마법사에서 U2F security key(U2F 보안 키)를 선택한 다음 Continue(계속)를 선택합니다.
5. 컴퓨터의 USB 포트에 U2F 보안 키를 삽입합니다.

6. U2F 보안 키를 터치한 다음, U2F 설정이 완료되었을 때 닫기를 선택합니다.

AWS에서 U2F 보안 키를 사용할 준비가 끝났습니다. AWS Management 콘솔의 MFA 사용 방법에 대한 자세한 내용은 IAM 로그인 페이지에 MFA 디바이스 사용 (p. 79) 단원을 참조하십시오.

다른 IAM 사용자에 대한 U2F 보안 키 활성화(콘솔)

AWS Management 콘솔에서만 다른 IAM 사용자에 대한 U2F 보안 키를 활성화할 수 있으며, AWS CLI 또는 AWS API에서는 활성화할 수 없습니다.

다른 IAM 사용자에 대한 U2F 보안 키를 활성화하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Users(사용자)를 선택합니다.
3. MFA를 활성화하려는 사용자의 이름을 선택한 다음 Security credentials(보안 자격 증명) 탭을 선택합니다.
4. Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.
5. Manage MFA device(MFA 디바이스 관리) 마법사에서 U2F security key(U2F 보안 키)를 선택한 다음 Continue(계속)를 선택합니다.
6. 컴퓨터의 USB 포트에 U2F 보안 키를 삽입합니다.

7. U2F 보안 키를 터치한 다음, U2F 설정이 완료되었을 때 닫기를 선택합니다.

AWS에서 U2F 보안 키를 사용할 준비가 끝났습니다. AWS Management 콘솔의 MFA 사용 방법에 대한 자세한 내용은 IAM 로그인 페이지에 MFA 디바이스 사용 (p. 79) 단원을 참조하십시오.

AWS 계정 루트 사용자에 대한 U2F 보안 키 활성화(콘솔)

AWS Management 콘솔에서만 루트 사용자에 대한 가상 MFA 디바이스를 구성하고 활성화할 수 있으며, AWS CLI 또는 AWS API에서는 이 작업을 수행할 수 없습니다.

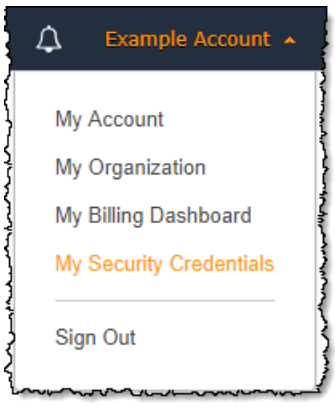
U2F 보안 키를 분실했거나, 도난당했거나, 작동하지 않을 경우에도 다른 인증 요소를 사용하여 로그인할 수 있습니다. 다른 인증 요소를 사용하여 로그인하는 방법은 MFA 디바이스 분실 또는 작동 중단 시 문제 해결 (p. 144) 단원을 참조하십시오. 이 기능을 비활성화하려면 AWS Support에 문의하십시오.

루트 사용자용 U2F 키를 활성화하려면(콘솔)

1. AWS 계정 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 AWS 계정 루트 사용자로 로그인합니다.

   Note

   텍스트 상자가 세 개 표시되면 이전에 IAM 사용자 자격 증명으로 콘솔에 로그인한 것입니다. 브라우저에서 이 기본 설정을 기억하고 로그인할 때마다 이 계정별 로그인 페이지를 열 수 있습니다. IAM 사용자 로그인 페이지에서는 계정 소유자로 로그인할 수 없습니다. IAM 사용자 로그인 페이지가 표시되면 페이지 하단에 있는 Sign in using 루트 사용자 email(이메일을 사용하여 로그인)을 선택하여 기본 로그인 페이지로 돌아갑니다. 기본 로그인 페이지에서 AWS 계정 이메일 주소와 암호를 입력하여 루트 사용자로 로그인합니다.
2. 탐색 모음의 오른쪽에서 계정 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)을 선택합니다. 필요한 경우 보안 자격 증명으로 계속(Continue to Security Credentials)을 선택합니다.



3. Multi-factor authentication (MFA)(멀티 팩터 인증(MFA)) 섹션을 확장합니다.
4. 이전 단계에서 선택한 옵션에 따라 MFA 관리 또는 MFA 활성화(Activate MFA)를 선택합니다.
5. 마법사에서 U2F security key(U2F 보안 키)를 선택한 후 계속을 선택합니다.
6. 컴퓨터의 USB 포트에 U2F 보안 키를 삽입합니다.

7. U2F 보안 키를 터치한 다음, U2F 설정이 완료되었을 때 닫기를 선택합니다.

AWS에서 U2F 보안 키를 사용할 준비가 끝났습니다. 다음에 루트 사용자 자격 증명을 사용하여 로그인할 때도 U2F 보안 키를 터치해 로그인 절차를 완료해야 합니다.

U2F 보안 키 교체

한 사용자에게는 한 번에 하나의 MFA 디바이스(가상, U2F 보안 키 또는 하드웨어)만 할당할 수 있습니다. 사용자가 U2F 보안 키를 분실하거나 이유를 불문하고 교체할 필요가 있을 경우, 먼저 기존 U2F 키를 비활성화해야 합니다. 그런 다음, 해당 사용자를 위한 새 MFA 디바이스를 추가할 수 있습니다.

- 현재 어떤 사용자와 연결되어 있는 디바이스를 비활성화하는 방법은 MFA 디바이스 비활성화 (p. 142) 단원을 참조하십시오.
- IAM 사용자에 대한 새 U2F 보안 키를 추가하려면 U2F 보안 키 활성화(콘솔) (p. 125) 단원을 참조하십시오.

새로운 U2F 보안 키에 대한 액세스 권한이 없는 경우 새로운 가상 MFA 디바이스 또는 하드웨어 MFA 디바이스를 활성화할 수 있습니다. 관련 지침을 보려면 다음 중 하나를 참조하십시오.

- 가상 멀티 팩터 인증(MFA) 디바이스 활성화(콘솔) (p. 122)
- 하드웨어 MFA 디바이스 활성화(콘솔) (p. 130)

U2F 보안 키 사용에 지원되는 구성

AWS에서 현재 지원되는 구성을 사용하여 U2F를 멀티 팩터 인증(MFA) 방법으로 사용할 수 있습니다. 이에는 AWS 및 U2F를 지원하는 브라우저가 지원되는 U2F 디바이스가 포함됩니다.

AWS 지원 U2F 디바이스

AWS는 현재 컴퓨터의 USB 포트에 연결되는 U2F 준수 보안 디바이스를 지원합니다.

> **Note**
>
> AWS의 경우 U2F 디바이스 검사를 위해 컴퓨터에 있는 물리적 USB 포트에 대한 액세스가 필요합니다. U2F MFA는 가상 머신 또는 원격 연결에서 작동하지 않습니다.

지원되는 디바이스의 구입에 대한 자세한 내용은 멀티 팩터 인증 단원을 참조하십시오.

U2F 지원 브라우저

다음 브라우저들은 현재 U2F 보안 키의 사용을 지원합니다.

- Google Chrome 버전 38 이상.
- Opera 버전 40 이상.
- Mozilla Firefox 버전 57 이상.

> **Note**
>
> 현재 U2F를 지원하는 대부분의 Firefox 버전은 기본적으로 지원을 활성화하지 않습니다. Firefox에서 U2F 지원을 활성하기 위한 지침은 U2F 보안 키 문제 해결 (p. 551) 단원을 참조하십시오.

브라우저 플러그인

현재 AWS는 U2F 표준을 기본적으로 지원하는 브라우저만을 지원합니다. AWS는 U2F 브라우저 지원을 추가하기 위한 플러그인 사용을 지원하지 않습니다. 또한 일부 브라우저 플러그인은 U2F 표준과 호환되지 않으며 U2F 보안 키와 연결할 때 예기치 않은 결과를 초래할 수 있습니다.

브라우저 플러그인 비활성화 및 기타 문제 해결을 위한 자세한 내용은 U2F 보안 키를 활성화할 수 없습니다. (p. 551) 단원을 참조하십시오.

모바일 환경

AWS에서는 현재 모바일 브라우저 또는 USB 방식이 아닌 U2F 디바이스에 대해서는 U2F 보안 키의 사용을 지원하지 않습니다.

AWS 콘솔 모바일 앱은 현재 MFA에 대한 U2F 보안 키의 사용을 지원하지 않습니다.

AWS CLI 및 AWS API

AWS는 현재 AWS Management 콘솔에서만 U2F 보안 키의 사용을 지원합니다. MFA에 대한 U2F 보안 키의 사용은 현재 AWS CLI 및 AWS API 또는 MFA 보호 API 작업 (p. 146)에 대한 액세스에는 지원되지 않습니다.

추가 리소스

- AWS에서 U2F 보안 키 사용에 대한 자세한 내용은 U2F 보안 키 활성화(콘솔) (p. 125) 단원을 참조하십시오.
- AWS에서 U2F 문제 해결에 대한 도움말은 U2F 보안 키 문제 해결 (p. 551) 단원을 참조하십시오.
- U2F 지원에 대한 전반적인 업계 정보는 Universal 2nd Factor 단원을 참조하십시오.

하드웨어 MFA 디바이스 활성화(콘솔)

동기화된 일회용 암호 알고리즘에 따라 6자리 숫자 코드를 생성하는 하드웨어 MFA 디바이스입니다. 사용자는 로그인 과정 중 디바이스의 유효 코드를 입력해야 합니다. 사용자에게 할당된 각 MFA 디바이스는 고유해야 합니다. 사용자는 다른 사용자의 디바이스 코드를 입력하여 인증받을 수 없습니다.

하드웨어 MFA 디바이스 및 U2F 보안 키 (p. 125)는 모두 본인이 구입한 물리적 디바이스이어야 합니다. 차이점이 있다면 하드웨어 MFA 디바이스가 코드를 생성하여 보여준 후 AWS에 로그인할 때 메시지가 나타나면 해당 란에 입력한다는 점입니다. U2F 보안 키로는 인증 코드를 확인하거나 입력할 수 없습니다. 대신 U2F 보안 키가 응답을 생성하되 사용자에게 보여주지는 않으며 서비스에서 이를 확인합니다. 두 디바이스 유형의 사양 및 구입 관련 정보는 멀티 팩터 인증 단원을 참조하십시오.

AWS Management 콘솔, 명령줄 또는 IAM API에서 IAM 사용자의 하드웨어 MFA 디바이스를 활성화할 수 있습니다. AWS 계정 루트 사용자에 따른 MFA 디바이스 활성화 방법은 AWS 계정 루트 사용자용 하드웨어 MFA 디바이스 활성화(콘솔) (p. 133) 단원을 참조하십시오.

루트 사용자 또는 IAM 사용자별로 (어떤 종류든) 한 개의 MFA 디바이스를 활성화할 수 있습니다.

> **Note**
>
> 명령줄에서 디바이스를 활성화하려는 경우 `iam-userenablemfadevice` `aws iam enable-mfa-device`를 사용합니다. IAM API를 사용하여 MFA 디바이스를 활성화하려면 `EnableMFADevice` 작업을 사용합니다.

주제

- 필요한 권한 (p. 131)
- 자신의 IAM 사용자에 대해 하드웨어 MFA 디바이스 활성화(콘솔) (p. 131)
- 다른 IAM 사용자에 대해 하드웨어 MFA 디바이스 활성(콘솔) (p. 132)

- AWS 계정 루트 사용자용 하드웨어 MFA 디바이스 활성화(콘솔) (p. 133)
- 물리적 MFA 디바이스 교체 또는 "회전" (p. 134)

필요한 권한

중요한 MFA 관련 작업을 보호하면서 자신의 IAM 사용자에 대한 하드웨어 MFA 디바이스를 관리하려면 다음 정책에 따른 권한이 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowManageOwnUserMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice",
                "iam:EnableMFADevice",
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "DenyAllExceptListedIfNoMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:EnableMFADevice",
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

자신의 IAM 사용자에 대해 하드웨어 MFA 디바이스 활성화(콘솔)

AWS Management 콘솔에서 자신의 하드웨어 MFA 디바이스를 활성화할 수 있습니다.

> **Note**
>
> 하드웨어 MFA 디바이스를 활성화하려면 디바이스에 물리적으로 액세스할 수 있어야 합니다.

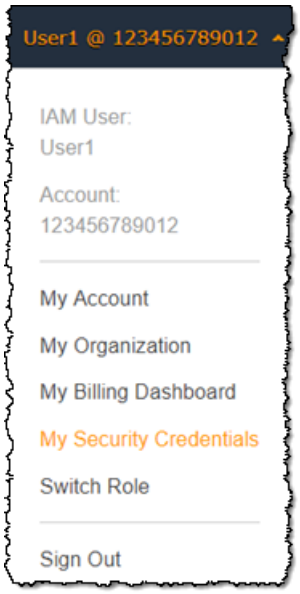
자신의 IAM 사용자에 대한 하드웨어 MFA 디바이스를 활성화하려면(콘솔)

1. AWS 계정 ID나 계정 별칭, IAM 사용자 이름 및 암호를 사용하여 IAM 콘솔에 로그인합니다.

   > **Note**
   >
   > 사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 이전에 다른 사용자로 로그인한 경우 페이지 하단 근처의 Sign in to a different account(다른 계정에 로그인)를 선택하여 기본 로그인 페이지로 돌아갑니다. 여기서 AWS 계정 ID 또는 계정 별칭을 입력하면 계정의 IAM 사용자 로그인 페이지로 리디렉션됩니다.

   AWS 계정 ID를 받으려면 관리자에게 문의하십시오.

2. 오른쪽 상단의 탐색 모음에서 사용자 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)를 선택합니다.



3. AWS IAM credentials(AWS IAM 자격 증명) 탭의 Multi-factor authentication(멀티 팩터 인증) 섹션에서 Manage MFA device(내 MFA 디바이스 관리)를 선택합니다.
4. Manage MFA device(MFA 디바이스 관리) 마법사에서 Hardware MFA device(하드웨어 MFA 디바이스)를 선택한 다음 Continue(계속)를 선택합니다.
5. 디바이스 일련 번호를 입력합니다. 일련 번호는 보통 디바이스 후면에 있습니다.
6. MFA code 1(MFA 코드 1) 상자에 MFA 디바이스에 표시된 6자리 번호를 입력합니다. 디바이스 전면의 버튼을 눌러야 번호가 표시되는 경우도 있습니다.

7. 디바이스가 코드를 새로 고칠 때까지 30초 동안 기다린 다음 MFA code 2(MFA 코드 2) 상자에 다음 6자리 번호를 입력합니다. 다시 디바이스 전면의 버튼을 눌러야 두 번째 번호가 표시되는 경우도 있습니다.
8. Assign MFA(MFA 할당)을 선택합니다.

   Important

   인증 코드를 생성한 후 바로 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화 (p. 138)할 수 있습니다.

이제 AWS에서 디바이스를 사용할 준비가 끝났습니다. AWS Management 콘솔의 MFA 사용 방법에 대한 자세한 내용은 IAM 로그인 페이지에 MFA 디바이스 사용 (p. 79) 단원을 참조하십시오.

다른 IAM 사용자에 대해 하드웨어 MFA 디바이스 활성(콘솔)

AWS Management 콘솔에서 다른 IAM 사용자에 대해 하드웨어 MFA 디바이스를 활성화할 수 있습니다.

다른 IAM 사용자에 대해 하드웨어 MFA 디바이스를 활성화하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.

2. 탐색 창에서 Users(사용자)를 선택합니다.
3. MFA를 활성화하려는 사용자의 이름을 선택한 다음 Security credentials(보안 자격 증명) 탭을 선택합니다.
4. Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.
5. Manage MFA device(MFA 디바이스 관리) 마법사에서 Hardware MFA device(하드웨어 MFA 디바이스)를 선택한 다음 Continue(계속)를 선택합니다.
6. 디바이스 일련 번호를 입력합니다. 일련 번호는 보통 디바이스 후면에 있습니다.
7. MFA code 1(MFA 코드 1) 상자에 MFA 디바이스에 표시된 6자리 번호를 입력합니다. 디바이스 전면의 버튼을 눌러야 번호가 표시되는 경우도 있습니다.

8. 디바이스가 코드를 새로 고칠 때까지 30초 동안 기다린 다음 MFA code 2(MFA 코드 2) 상자에 다음 6자리 번호를 입력합니다. 다시 디바이스 전면의 버튼을 눌러야 두 번째 번호가 표시되는 경우도 있습니다.
9. Assign MFA(MFA 할당)을 선택합니다.

   Important

   인증 코드를 생성한 후 바로 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화 (p. 138)할 수 있습니다.

이제 AWS에서 디바이스를 사용할 준비가 끝났습니다. AWS Management 콘솔의 MFA 사용 방법에 대한 자세한 내용은 IAM 로그인 페이지에 MFA 디바이스 사용 (p. 79) 단원을 참조하십시오.

AWS 계정 루트 사용자용 하드웨어 MFA 디바이스 활성화(콘솔)

AWS Management 콘솔에서만 루트 사용자에 대한 가상 MFA 디바이스를 구성하고 활성화할 수 있으며, AWS CLI 또는 AWS API에서는 이 작업을 수행할 수 없습니다.

MFA 디바이스를 분실하거나, 도난당했거나, 디바이스가 작동하지 않을 경우에도 다른 인증 요소를 사용하여 로그인할 수 있습니다. MFA 디바이스로 로그인할 수 없는 경우에 사용자 계정으로 등록된 이메일 및 전화로 사용자 ID를 확인하여 로그인할 수 있습니다. 루트 사용자용 MFA를 활성화하기 전에 계정 설정과 연락처 정보를 검토하여 이메일 및 전화번호에 대한 액세스 권한이 있는지 확인하십시오. 다른 인증 요소를 사용하여 로그인하는 방법은 MFA 디바이스 분실 또는 작동 중단 시 문제 해결 (p. 144) 단원을 참조하십시오. 이 기능을 비활성화하려면 AWS Support에 문의하십시오.

Note

MFA를 사용하여 로그인 및 인증 디바이스 문제 해결과 같은 다른 텍스트가 나타날 수 있습니다. 그러나 동일한 기능이 제공됩니다. 어느 경우든 대체 인증 팩터를 사용하여 계정 이메일 주소 및 전화번호를 확인할 수 없는 경우 AWS Support에 문의하여 MFA 설정을 비활성화하십시오.

루트 사용자용 MFA 디바이스를 활성화하려면(콘솔)

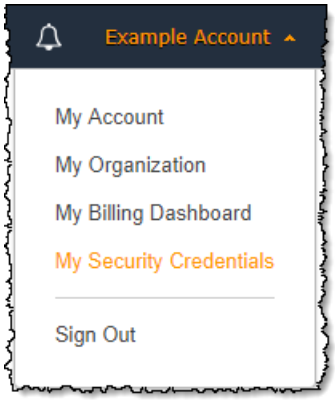
1. AWS 계정 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 AWS 계정 루트 사용자로 로그인합니다.

   Note

   텍스트 상자가 세 개 표시되면 이전에 IAM 사용자 자격 증명으로 콘솔에 로그인한 것입니다. 브라우저에서 이 기본 설정을 기억하고 로그인할 때마다 이 계정별 로그인 페이지를 열 수 있습니다. IAM 사용자 로그인 페이지에서는 계정 소유자로 로그인할 수 없습니다. IAM 사용자 로그인

페이지가 표시되면 페이지 하단에 있는 Sign in using 루트 사용자 email(이메일을 사용하여 로그인)을 선택하여 기본 로그인 페이지로 돌아갑니다. 기본 로그인 페이지에서 AWS 계정 이메일 주소와 암호를 입력하여 루트 사용자로 로그인합니다.

2. 탐색 모음의 오른쪽에서 계정 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)을 선택합니다. 필요한 경우 보안 자격 증명으로 계속(Continue to Security Credentials)을 선택합니다.



3. Multi-factor authentication (MFA)(멀티 팩터 인증(MFA)) 섹션을 확장합니다.
4. 이전 단계에서 선택한 옵션에 따라 MFA 관리 또는 MFA 활성화(Activate MFA)를 선택합니다.
5. 마법사에서 Hardware MFA device(하드웨어 MFA 디바이스)를 선택한 후 계속을 선택합니다.
6. Serial number(일련 번호) 상자에 MFA 디바이스 뒷면에 있는 일련 번호를 입력합니다.
7. MFA code 1(MFA 코드 1) 상자에 MFA 디바이스에 표시된 6자리 번호를 입력합니다. 디바이스 전면의 버튼을 눌러야 번호가 표시되는 경우도 있습니다.

8. 디바이스가 코드를 새로 고칠 때까지 30초 동안 기다린 다음 MFA code 2(MFA 코드 2) 상자에 다음 6자리 번호를 입력합니다. 다시 디바이스 전면의 버튼을 눌러야 두 번째 번호가 표시되는 경우도 있습니다.
9. Assign MFA(MFA 할당)을 선택합니다. 이제 MFA 디바이스가 AWS 계정과 연결되었습니다.

   Important

   인증 코드를 생성한 후 바로 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화 (p. 138)할 수 있습니다.

   다음에 루트 사용자 자격 증명을 사용하여 로그인할 때도 MFA 디바이스의 코드를 입력해야 합니다.

물리적 MFA 디바이스 교체 또는 "회전"

한 사용자에게는 한 번에 하나의 MFA 디바이스만 할당할 수 있습니다. 사용자가 디바이스를 분실하거나 이유를 불문하고 교체할 필요가 있을 경우, 먼저 기존 디바이스를 비활성화해야 합니다. 그런 다음, 해당 사용자를 위한 새 디바이스를 추가할 수 있습니다.

- 현재 어떤 사용자와 연결되어 있는 디바이스를 비활성화하는 방법은 MFA 디바이스 비활성화 (p. 142) 단원을 참조하십시오.
- IAM 사용자용 교체 하드웨어 MFA 디바이스를 추가하려면, 이 주제 앞부분의 다른 IAM 사용자에 대해 하드웨어 MFA 디바이스 활성(콘솔) (p. 132) 절차에 나오는 단계를 따르십시오.
- AWS 계정 루트 사용자용 교체 가상 MFA 디바이스를 추가하려면 이 주제 앞부분의 AWS 계정 루트 사용자용 하드웨어 MFA 디바이스 활성화(콘솔) (p. 133) 절차에 나오는 단계를 따르십시오.

미리 보기 – SMS 문자 메시지 MFA 디바이스 활성화

AWS는 곧 SMS 멀티 팩터 인증(MFA) 지원을 종료할 예정입니다. 신규 고객은 이 기능을 미리 볼 수 없습니다. 기존 고객은 다음의 MFA 대체 방법 중 하나로 전환하는 것이 좋습니다.

- 가상(소프트웨어 기반) (p. 122) MFA 디바이스
- U2F 보안 키 (p. 125)
- 하드웨어 기반 (p. 130) MFA 디바이스

도움말

계정의 사용자 중에서 SMS MFA 디바이스가 할당된 사용자를 볼 수 있습니다. IAM 콘솔의 탐색 창에서 사용자를 선택하고 표의 MFA 열에서 SMS가 표시된 사용자를 찾습니다.

SMS(문자 서비스) MFA 디바이스는 표준 SMS 문자 메시지를 받을 수 있는 전화번호를 사용하는 모든 모바일 디바이스일 수 있습니다. MFA 코드가 필요한 경우 AWS가 IAM 사용자에 대해 구성된 전화번호로 해당 코드를 보냅니다.

Note

SMS MFA는 IAM 사용자만 사용할 수 있습니다. AWS 계정 루트 사용자에서는 사용할 수 없습니다. MFA로 루트 사용자를 보호하려면 가상 MFA 디바이스, U2F 보안 키 또는 하드웨어 MFA 디바이스를 사용해야 합니다.

IAM 사용자의 SMS MFA 디바이스 활성화(콘솔)

AWS Management 콘솔에서 IAM을 사용하여 IAM 사용자를 전화번호로 구성함으로써 SMS MFA를 활성화할 수 있습니다.

Note

현재, AWS Management 콘솔에서만 SMS MFA를 관리할 수 있습니다.

IAM 사용자의 SMS MFA를 활성화하려면(콘솔)

1. AWS 계정 ID나 계정 별칭, IAM 사용자 이름 및 암호를 사용하여 IAM 콘솔에 로그인합니다.

   Note

   사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 이전에 다른 사용자로 로그인한 경우 페이지 하단 근처의 Sign in to a different account(다른 계정에 로그인)를 선택하여 기본 로그인 페이지로 돌아갑니다. 여기서 AWS 계정 ID 또는 계정 별칭을 입력하면 계정의 IAM 사용자 로그인 페이지로 리디렉션됩니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 사용자 이름 목록에서 원하는 MFA 사용자의 이름(확인란 아님)을 선택합니다.
4. Security credentials(보안 자격 증명) 탭을 선택합니다. Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.
5. Manage MFA Device(MFA 디바이스 관리) 마법사에서 An SMS MFA device(SMS MFA 디바이스)를 선택한 다음 계속을 선택합니다.
6. 이 IAM 사용자에게 MFA 코드를 보낼 전화번호를 입력한 다음 계속을 선택합니다.
7. 확인을 위해 이 지정된 전화번호로 6자리 인증 코드가 즉시 전송됩니다. 6자리 코드를 입력한 후 계속을 선택합니다. 적절한 시간 안에 코드를 받지 못한 경우 코드 재전송(Resend Code)을 선택합니다. SMS 서비스는 전송 시간을 보장하지 않습니다.

8. AWS에서 코드를 확인하면 마법사가 종료됩니다. 종료되지 않으면 마침을 선택하여 마법사를 닫습니다.

IAM 사용자의 SMS MFA 전화번호 변경

IAM 사용자에게 할당된 SMS MFA 디바이스의 전화번호를 변경하려면 현재 MFA 디바이스를 삭제해야 합니다. 그런 다음 새 전화 번호로 새 디바이스를 만들어야 합니다. 디바이스를 삭제하는 방법은 MFA 디바이스 비활성화 (p. 142) 단원을 참조하십시오.

가상 MFA 디바이스 활성화 및 관리(AWS CLI 또는 AWS API)

AWS CLI 명령 또는 AWS API 작업을 사용하여 IAM 사용자를 위한 가상 MFA 디바이스를 활성화할 수 있습니다. AWS CLI, AWS API, Windows PowerShell용 도구 또는 기타 다른 명령줄 도구를 사용하면 AWS 계정 루트 사용자에 대해 MFA 디바이스를 활성화할 수 없습니다. 하지만 AWS Management 콘솔을 사용하여 루트 사용자에 대해 MFA 디바이스를 활성화할 수 있습니다.

AWS Management 콘솔에서 MFA 디바이스를 활성화할 때 콘솔이 사용자를 대신해 여러 단계를 수행합니다. 대신 AWS CLI, Windows PowerShell용 도구 또는 AWS API를 사용해 가상 디바이스를 생성한다면 수동으로 올바른 순서에 따라 단계들을 수행해야 합니다. 예를 들어 가상 MFA 디바이스를 생성하려면 IAM 객체를 생성하고, 코드를 문자열이나 QR 코드 그래픽으로 추출합니다. 그런 다음 디바이스를 동기화하여 IAM 사용자와 연결합니다. 자세한 정보는 New-IAMVirtualMFADevice의 Examples 단원을 참조하십시오. 물리적 디바이스를 위해서는 생성 단계를 건너뛰고 디바이스를 동기화하고 사용자에게 직접 연결합니다.

IAM에서 가상 디바이스 개체를 생성하여 가상 MFA 디바이스를 나타내려면

이러한 명령은 다음 명령의 많은 일련 번호 대신 사용되는 디바이스에 ARN을 제공합니다.

- AWS CLI: `aws iam create-virtual-mfa-device`
- AWS API: `CreateVirtualMFADevice`

AWS에서 사용할 목적으로 MFA 디바이스를 활성화하려면

다음 명령은 디바이스와 AWS를 동기화하여 사용자 또는 루트 사용자에 연결합니다. 디바이스가 가상이라면 가상 디바이스의 ARN을 일련 번호로 사용합니다.

> **Important**
>
> 인증 코드를 생성한 후 바로 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 아래에서 설명하는 명령을 사용하여 디바이스를 재동기화할 수 있습니다.

- AWS CLI: `aws iam enable-mfa-device`
- AWS API: `EnableMFADevice`

디바이스를 비활성화하려면

다음 명령을 사용하여 디바이스를 사용자에게서 분리하고 비활성화합니다. 디바이스가 가상이라면 가상 디바이스의 ARN을 일련 번호로 사용합니다. 별도로 가상 디바이스 개체를 삭제해야 합니다.

- AWS CLI: `aws iam deactivate-mfa-device`
- AWS API: `DeactivateMFADevice`

가상 MFA 디바이스 개체를 표시하려면

다음 명령을 사용하여 가상 MFA 디바이스 개체의 목록을 봅니다.

- AWS CLI: `aws iam list-virtual-mfa-devices`

- AWS API: `ListVirtualMFADevices`

MFA 디바이스를 다시 동기화하려면

디바이스가 AWS에서 허용하지 않는 코드를 생성하는 경우 이러한 명령을 사용하십시오. 디바이스가 가상이라면 가상 디바이스의 ARN을 일련 번호로 사용합니다.

- AWS CLI: `aws iam resync-mfa-device`
- AWS API: `ResyncMFADevice`

IAM에서 가상 MFA 디바이스 엔터티를 삭제하려면

디바이스가 사용자로부터 분리된 후에 디바이스 개체를 삭제할 수 있습니다.

- AWS CLI: `aws iam delete-virtual-mfa-device`
- AWS API: `DeleteVirtualMFADevice`

분실되었거나 작동하지 않는 가상 MFA 디바이스를 복구하는 방법

간혹 가상 MFA 앱이 호스팅된 IAM 사용자의 디바이스가 분실 또는 교체되었거나 작동하지 않는 경우가 있을 수 있습니다. 이러한 경우가 발생하면 사용자는 스스로 디바이스를 복구할 수 없습니다. IAM 사용자는 관리자에게 연락하여 해당 디바이스를 비활성화해야 합니다. 자세한 정보는 MFA 디바이스 분실 또는 작동 중단 시 문제 해결 (p. 144) 단원을 참조하십시오.

MFA 상태 확인

IAM 콘솔을 사용하여 AWS 계정 루트 사용자 또는 IAM 사용자가 유효한 MFA 디바이스를 활성화했는지를 확인할 수 있습니다.

루트 사용자의 MFA 상태를 확인하려면

1. 루트 사용자 자격 증명으로 AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 보안 상태(Security Status) 아래에서 MFA의 활성화 여부를 확인합니다. MFA가 활성화되지 않은 경우, 알림 기호( )가 Activate MFA on your 루트 사용자(루트 사용자에서 MFA 활성화) 옆에 표시됩니다.

계정에 대해 MFA를 활성화하고 싶다면 다음 중 하나를 참조하십시오.

- AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) (p. 123)
- AWS 계정 루트 사용자에 대한 U2F 보안 키 활성화(콘솔) (p. 128)
- AWS 계정 루트 사용자용 하드웨어 MFA 디바이스 활성화(콘솔) (p. 133)

IAM 사용자의 MFA 상태를 확인하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 필요할 경우 다음 단계를 통해 사용자 테이블에 MFA 열을 추가합니다.
   a. 테이블 위 맨 오른쪽에서 설정 아이콘( )을 선택합니다.
   b. 열 관리(Manage Columns)에서 MFA를 선택합니다.
   c. (선택 사항) 필요할 경우 사용자 테이블에 표시하지 않으려는 열이 있으면 해당 열의 확인란 선택을 취소하면 됩니다.

d. 닫기를 선택하여 사용자 목록으로 돌아갑니다.

4. MFA 열에는 활성화된 MFA 디바이스가 표시됩니다. 사용자에게 활성화되어 있는 MFA 디바이스가 없으면 콘솔에서 활성화되지 않음이라고 표시합니다. 사용자에게 활성화된 MFA 디바이스가 있으면 MFA 열에 활성화된 디바이스의 유형이 가상, U2F Security Key(U2F 보안 키), Hardware(하드웨어) 또는 SMS 값으로 표시됩니다.
5. 사용자의 MFA 디바이스에 대한 추가 정보를 보려면 MFA 상태를 확인하려는 사용자의 이름을 선택합니다. 그런 다음 보안 자격 증명(Security credentials) 탭을 선택합니다.
6. 사용자에게 활성화되어 있는 MFA 디바이스가 없으면 콘솔에서 할당된 MFA 디바이스(Assigned MFA device) 옆에 아니요가 표시됩니다. 반대로 활성화되어 있는 MFA 디바이스가 있으면 할당된 MFA 디바이스(Assigned MFA device) 항목에 디바이스 값이 표시됩니다.

   - 하드웨어 디바이스의 디바이스 일련 번호(일반적으로 디바이스 후면의 숫자)(예: `GAHT12345678`)
   - SMS 디바이스의 AWS의 ARN(예: `arn:aws:iam::123456789012:sms-mfa/username`)
   - 가상 디바이스의 AWS의 ARN(예: `arn:aws:iam::123456789012:mfa/username`)

현재 설정을 변경하려면 Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.

MFA 활성화에 대한 자세한 내용은 다음을 참조하십시오.

- 가상 멀티 팩터 인증(MFA) 디바이스 활성화(콘솔) (p. 122)
- U2F 보안 키 활성화(콘솔) (p. 125)
- 하드웨어 MFA 디바이스 활성화(콘솔) (p. 130)
- 미리 보기 – SMS 문자 메시지 MFA 디바이스 활성화 (p. 135)

가상 및 하드웨어 MFA 디바이스 재동기화

AWS를 사용하여 가상 및 하드웨어 멀티 팩터 인증(MFA) 디바이스를 다시 동기화할 수 있습니다. 디바이스를 사용하려고 할 때 디바이스가 동기화되지 않으면 로그인 시도가 실패하고 디바이스를 다시 동기화하라는 메시지가 IAM에 표시됩니다.

> Note
>
> U2F 보안 키는 항상 동기화됩니다. U2F 보안 키를 분실했거나 도난당한 경우 비활성화할 수 있습니다. 모든 MFA 디바이스 유형의 비활성화에 대한 지침은 다른 IAM 사용자에 대해 MFA 디바이스를 비활성화하려면(콘솔) (p. 143) 단원을 참조하십시오.

AWS 관리자로서 IAM 사용자의 가상 및 하드웨어 MFA 디바이스가 동기화 상태를 벗어난 경우 이를 재동기화할 수 있습니다.

AWS 계정 루트 사용자 MFA 디바이스가 작동하지 않는 경우 로그인 프로세스 완료 여부와 관계없이 IAM 콘솔을 사용하여 디바이스를 재동기화할 수 있습니다.

주제

- 필요한 권한 (p. 138)
- 가상 및 하드웨어 MFA 디바이스 재동기화(IAM 콘솔) (p. 139)
- 가상 및 하드웨어 MFA 디바이스 재동기화(AWS CLI) (p. 142)
- 가상 및 하드웨어 MFA 디바이스 재동기화(AWS API) (p. 142)

필요한 권한

자신의 IAM 사용자에 대한 가상 또는 하드웨어 MFA 디바이스를 다시 동기화하려면 다음 정책에 따른 권한이 있어야 합니다. 이 정책은 디바이스 생성 또는 비활성화를 허용하지 않습니다

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListActions",
            "Effect": "Allow",
            "Action": [
                "iam:ListVirtualMFADevices"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUserToViewAndManageTheirOwnUserMFA",
            "Effect": "Allow",
            "Action": [
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "BlockAllExceptListedIfNoMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:ListMFADevices",
                "iam:ListVirtualMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

가상 및 하드웨어 MFA 디바이스 재동기화(IAM 콘솔)

IAM 콘솔을 사용하여 가상 및 하드웨어 MFA 디바이스를 재동기화할 수 있습니다.

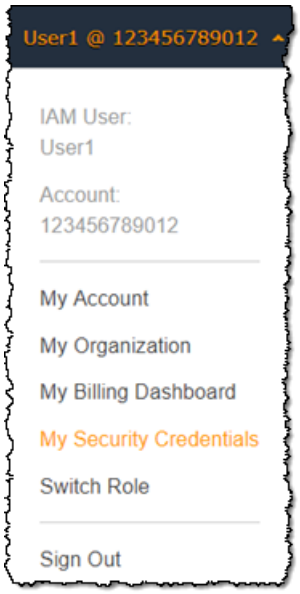
자신의 IAM 사용자에 대한 가상 또는 하드웨어 MFA 디바이스를 다시 동기화하려면(콘솔)

1. AWS 계정 ID나 계정 별칭, IAM 사용자 이름 및 암호를 사용하여 IAM 콘솔에 로그인합니다.

   Note

   사용자 편의를 위해 AWS 로그인 페이지는 브라우저 쿠키를 사용하여 IAM 사용자 이름 및 계정 정보를 기억합니다. 이전에 다른 사용자로 로그인한 경우 페이지 하단 근처의 Sign in to a different account(다른 계정에 로그인)를 선택하여 기본 로그인 페이지로 돌아갑니다. 여기서 AWS 계정 ID 또는 계정 별칭을 입력하면 계정의 IAM 사용자 로그인 페이지로 리디렉션됩니다.

   AWS 계정 ID를 받으려면 관리자에게 문의하십시오.
2. 오른쪽 상단의 탐색 모음에서 사용자 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)를 선택합니다.



3. AWS IAM credentials(AWS IAM 자격 증명) 탭의 Multi-factor authentication(멀티 팩터 인증) 섹션에서 Manage MFA device(내 MFA 디바이스 관리)를 선택합니다.
4. Manage MFA device(MFA 디바이스 관리) 마법사에서 Resync(재동기화)를 선택한 다음 Continue(계속)를 선택합니다.
5. 디바이스에서 순차적으로 생성된 다음 2개의 코드를 MFA code 1(MFA 코드 1) 및 MFA code 2(MFA 코드 2)에 입력합니다. 그런 다음 [Continue]를 선택합니다.

   Important

   코드를 생성한 후 즉시 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 요청이 처리되는 것으로 보이지만 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다.

다른 IAM 사용자에 대한 가상 및 하드웨어 MFA 디바이스를 다시 동기화하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택한 다음 MFA 디바이스를 재동기화해야 할 사용자의 이름을 선택합니다.
3. Security credentials(보안 자격 증명) 탭을 선택합니다. Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.
4. Manage MFA device(MFA 디바이스 관리) 마법사에서 Resync(재동기화)를 선택한 다음 Continue(계속)를 선택합니다.
5. 디바이스에서 순차적으로 생성된 다음 2개의 코드를 MFA code 1(MFA 코드 1) 및 MFA code 2(MFA 코드 2)에 입력합니다. 그런 다음 [Continue]를 선택합니다.

   Important

   코드를 생성한 후 즉시 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 요청이 처리되는 것으로 보이지만 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다.

로그인 전에 루트 사용자 MFA를 재동기화하려면(콘솔)

1. Amazon Web Services Sign In With Authentication Device(인증 디바이스로 Amazon Web Services 로그인) 페이지에서 다음을 선택합니다. Having problems with your authentication device?(인증 디바이스에 문제가 있습니까?) Click here.]를 선택합니다.

   Note

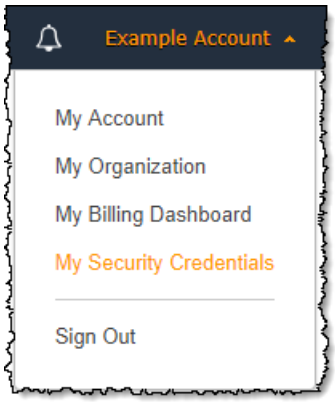
   MFA를 사용하여 로그인 및 인증 디바이스 문제 해결과 같은 다른 텍스트가 나타날 수 있습니다. 그러나 동일한 기능이 제공됩니다.
2. Re-Sync With Our Servers(서버를 통한 재동기화) 섹션에서 디바이스에서 순차적으로 생성된 다음 2개의 코드를 MFA code 1(MFA 코드 1) 및 MFA code 2(MFA 코드 2)에 입력합니다. 그런 다음 인증 디바이스 재동기화(Re-sync authentication device)를 선택합니다.
3. 필요할 경우 암호를 다시 입력하고 로그인을 선택합니다. 그런 다음 MFA 디바이스를 사용하여 로그인을 완료합니다.

로그인 이후 루트 사용자 MFA 디바이스를 재동기화하려면(콘솔)

1. AWS 계정 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 AWS 계정 루트 사용자로 로그인합니다.

   Note

   텍스트 상자가 세 개 표시되면 이전에 IAM 사용자 자격 증명으로 콘솔에 로그인한 것입니다. 브라우저에서 이 기본 설정을 기억하고 로그인할 때마다 이 계정별 로그인 페이지를 열 수 있습니다. IAM 사용자 로그인 페이지에서는 계정 소유자로 로그인할 수 없습니다. IAM 사용자 로그인 페이지가 표시되면 페이지 하단에 있는 Sign in using 루트 사용자 email(이메일을 사용하여 로그인)을 선택하여 기본 로그인 페이지로 돌아갑니다. 기본 로그인 페이지에서 AWS 계정 이메일 주소와 암호를 입력하여 루트 사용자로 로그인합니다.
2. 탐색 모음의 오른쪽에서 계정 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)을 선택합니다. 필요한 경우 보안 자격 증명으로 계속(Continue to Security Credentials)을 선택합니다.



3. 페이지의 Multi-factor authentication (MFA)(멀티 팩터 인증(MFA)) 섹션을 확장합니다.
4. 활성 MFA 디바이스 옆에 있는 Resync(재동기화)를 선택합니다.
5. Manage MFA Device(MFA 디바이스 관리) 대화 상자에서 디바이스에서 순차적으로 생성된 다음 2개의 코드를 MFA code 1(MFA 코드 1) 및 MFA code 2(MFA 코드 2)에 입력합니다. 그런 다음 [Continue]를 선택합니다.

   Important

   코드를 생성한 후 즉시 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다.

가상 및 하드웨어 MFA 디바이스 재동기화(AWS CLI)

AWS CLI에서 가상 및 하드웨어 MFA 디바이스를 재동기화할 수 있습니다.

IAM 사용자에 대한 가상 및 하드웨어 MFA 디바이스를 재동기화하려면(AWS CLI)

명령 프롬프트에서 `aws iam resync-mfa-device` 명령을 내립니다.

- 가상 MFA 디바이스: 디바이스의 Amazon 리소스 이름(ARN)을 일련 번호로 지정합니다.

```
$ aws iam resync-mfa-device --user-name Richard --serial-number
 arn:aws:iam::123456789012:mfa/RichardsMFA --authentication-code-1 123456 --
authentication-code-2 987654
```

- 하드웨어 MFA 디바이스: 하드웨어 디바이스의 일련 번호를 일련 번호로 지정합니다. 형식은 공급업체에 따라 다릅니다. 예를 들어 Amazon에서는 gemalto 토큰을 구매할 수 있습니다. 이 토큰의 일련 번호는 일반적으로 문자 4개이며 그 뒤로 숫자 4개가 이어집니다.

```
$ aws iam resync-mfa-device --user-name Richard --serial-number ABCD12345678 --
authentication-code-1 123456 --authentication-code-2 987654
```

> **Important**
>
> 코드를 생성한 후 즉시 요청을 제출하십시오. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 잠시 후 코드가 만료되기 때문에 요청이 실패합니다.

가상 및 하드웨어 MFA 디바이스 재동기화(AWS API)

IAM에는 동기화를 실행하는 API 호출이 있습니다. 이러한 경우 가상 및 하드웨어 MFA 사용자에게 API 호출에 액세스할 수 있는 권한을 부여하는 것이 좋습니다. 이때 사용자가 필요할 때마다 디바이스를 재동기화할 수 있도록 API 호출 기반 도구를 구축해야 합니다.

IAM 사용자에 대한 가상 및 하드웨어 MFA 디바이스를 재동기화하려면(AWS API)

- `ResyncMFADevice` 요청을 보냅니다.

MFA 디바이스 비활성화

멀티 팩터 인증(MFA) 디바이스를 사용하여 IAM 사용자로 로그인하는 데 문제가 있는 경우 관리자에게 문의하여 도움을 받으십시오.

관리자는 다른 IAM 사용자에 대해 디바이스를 비활성화할 수 있습니다. 이 방법을 사용하면 MFA를 사용하지 않고 로그인할 수 있습니다. MFA 디바이스가 교체되는 중이거나 디바이스가 일시적으로 사용 불가능할 때 이 방법을 임시 해결 방법으로 사용할 수 있습니다. 그러나 최대한 빨리 사용자를 위한 새 디바이스를 활성화하는 것이 좋습니다. 새 MFA 디바이스를 활성화 하는 방법에 대한 자세한 내용은 the section called “MFA 디바이스 활성화” (p. 120)를 참조하십시오.

> **Note**
>
> API 또는 AWS CLI를 사용하여 AWS 계정에서 사용자를 삭제하는 경우 사용자의 MFA 디바이스를 비활성화 또는 삭제해야 합니다. 이 변경 사항을 사용자 제거 과정의 일부로 활용합니다. 사용자 삭제에 대한 자세한 내용은 IAM사용자 관리 (p. 92) 단원을 참조하십시오.

주제

MFA 디바이스 비활성화(콘솔)

다른 IAM 사용자에 대해 MFA 디바이스를 비활성화하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Users(사용자)를 선택합니다.
3. 사용자의 MFA 디바이스를 비활성화하려면 MFA를 제거하려는 사용자의 이름을 선택합니다.
4. Security credentials(보안 자격 증명) 탭을 선택합니다. Assigned MFA device(할당된 MFA 디바이스) 옆의 관리를 선택합니다.
5. Manage MFA device(MFA 디바이스 관리) 마법사에서 Deactivate MFA device(MFA 디바이스 비활성화)를 선택한 다음 Continue(계속)을 선택합니다.

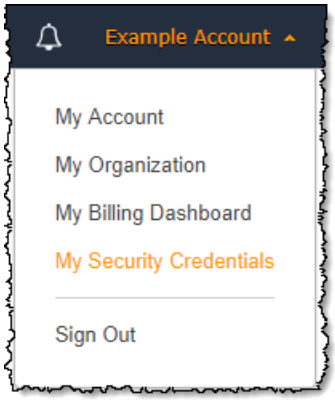
   디바이스가 AWS에서 제거됩니다. 디바이스는 다시 활성화되어 AWS 사용자 또는 AWS 계정 루트 사용자에 연결될 때까지는 로그인 또는 요청 인증에 사용할 수 없습니다.

AWS 계정 루트 사용자의 MFA 디바이스를 비활성화하려면(콘솔)

1. AWS 계정 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 AWS 계정 루트 사용자로 로그인합니다.

   Note

   텍스트 상자가 세 개 표시되면 이전에 IAM 사용자 자격 증명으로 콘솔에 로그인한 것입니다. 브라우저에서 이 기본 설정을 기억하고 로그인할 때마다 이 계정별 로그인 페이지를 열 수 있습니다. IAM 사용자 로그인 페이지에서는 계정 소유자로 로그인할 수 없습니다. IAM 사용자 로그인 페이지가 표시되면 페이지 하단에 있는 Sign in using 루트 사용자 email(이메일을 사용하여 로그인)을 선택하여 기본 로그인 페이지로 돌아갑니다. 기본 로그인 페이지에서 AWS 계정 이메일 주소와 암호를 입력하여 루트 사용자로 로그인합니다.
2. 탐색 모음의 오른쪽에서 계정 이름을 선택한 다음 My Security Credentials(내 보안 자격 증명)을 선택합니다. 필요한 경우 보안 자격 증명으로 계속(Continue to Security Credentials)을 선택합니다.



3. Multi-factor authentication (MFA)(멀티 팩터 인증(MFA)) 섹션을 확장합니다.
4. 비활성화하려는 MFA 디바이스의 행에서 비활성화를 선택합니다.

AWS 계정의 MFA 디바이스가 비활성화됩니다.

MFA 디바이스 비활성화(AWS CLI)

IAM 사용자에 대해 MFA 디바이스를 비활성화하려면(AWS CLI)

- 다음 명령을 실행합니다. `aws iam deactivate-mfa-device`

MFA 디바이스 비활성화(AWS API)

IAM 사용자에 대해 MFA 디바이스를 비활성화하려면(AWS API)

- 다음 연산을 호출합니다. `DeactivateMFADevice`

MFA 디바이스 분실 또는 작동 중단 시 문제 해결

가상 MFA 디바이스 (p. 122) 또는 하드웨어 MFA 디바이스 (p. 130)가 정상적으로 작동하는 것처럼 같지만, 이것을 사용하여 AWS 리소스에 액세스하지 못하는 경우에는 AWS와 동기화되지 않는 것이 원인일 수 있습니다. 가상 MFA 디바이스 또는 하드웨어 MFA 디바이스의 동기화에 대한 자세한 내용은 가상 및 하드웨어 MFA 디바이스 재동기화 (p. 138) 단원을 참조하십시오. U2F 보안 키 (p. 125)는 항상 동기화되어 있습니다.

AWS 계정 루트 사용자 Multi-Factor Authentication(MFA) 디바이스 (p. 119)가 분실, 손상 또는 작동하지 않는 경우 계정에 대한 액세스를 복구할 수 있습니다. IAM 사용자는 관리자에 문의하여 디바이스를 비활성화해야 합니다.

루트 사용자 MFA 디바이스 복구

AWS 계정 루트 사용자 멀티 팩터 인증(MFA) 디바이스 (p. 119) 분실, 손상 또는 고장 시에는 다른 인증 방법을 사용하여 로그인할 수 있습니다. 다시 말해, MFA 디바이스로 로그인할 수 없는 경우에 사용자 계정으로 등록된 이메일 및 전화로 사용자 ID를 확인하여 로그인할 수 있습니다.

다른 인증 요소를 사용하여 루트 사용자 로그인하기 전에 계정과 연결된 이메일과 전화번호에 액세스할 수 있는지 확인하십시오. 더 이상 이메일 또는 전화에 액세스할 수 없는 경우 AWS Support에 문의해야 합니다. AWS Support에서는 사용자가 로그인하여 새 디바이스를 추가할 수 있도록 사용자의 MFA 디바이스를 비활성화할 수 있습니다.

AWS 계정 루트 사용자로 다른 인증 요소를 사용하여 로그인하려면

1. AWS 계정 이메일 주소와 비밀번호를 사용해 AWS Management 콘솔에 AWS 계정 루트 사용자로 로그인합니다.
2. Amazon Web Services Sign In Using MFA(MFA를 사용한 Amazon Web Services 로그인) 페이지에서 Having problems with your authentication device?(인증 디바이스에 문제가 있습니까?)를 선택합니다. Click here.]를 선택합니다.

   Note

   MFA를 사용하여 로그인 및 인증 디바이스 문제 해결과 같은 다른 텍스트가 나타날 수 있습니다. 그러나 동일한 기능이 제공됩니다. 어느 경우든 다른 인증 요소를 사용하여 계정 이메일 주소 및 전화 번호를 확인할 수 없는 경우 AWS Support에 문의하여 MFA 디바이스를 비활성화하십시오.
3. 필요할 경우 암호를 다시 입력하고 로그인을 선택합니다.
4. 대체 인증 팩터를 사용하여 로그인(Sign In Using Alternative Factors of Authentication) 섹션에서 대체 팩터를 사용하여 로그인(Sign in using alternative factors)을 선택합니다.
5. 이메일 주소를 확인하여 계정을 인증하려면 확인 이메일 전송(Send verification email)을 선택합니다.
6. AWS 계정과 연결된 이메일에서 Amazon Web Services의 메시지를 확인합니다(no-reply-aws@amazon.com). 이메일 지침을 따릅니다.

   계정에 이메일이 없는 경우에는 스팸 폴더를 확인하거나 브라우저로 돌아가 이메일 재전송(Resend the email)을 선택합니다.
7. 이메일 주소를 확인한 후에 계정 인증을 계속 진행할 수 있습니다. 전화 번호를 확인하려면 지금 전화하기(Call me now)를 선택합니다.
8. AWS 전화를 받고, 요구에 따라 AWS 웹사이트의 6자리 숫자를 전화 키패드에 입력합니다.

AWS에서 전화가 오지 않을 경우에는 로그인을 선택하여 콘솔에 다시 로그인하고 처음부터 다시 시작합니다. 또는 AWS Support를 선택하여 지원 부서로 문의합니다.

9. 전화 번호를 확인한 후에는 콘솔에 로그인(Sign in to the console)을 선택하여 계정에 로그인할 수 있습니다.
10. 다음 단계는 사용 중인 MFA의 유형에 따라 다릅니다.

    - 가상 MFA 디바이스의 경우, 디바이스에서 계정을 제거합니다. 그런 다음 AWS 보안 자격 증명(AWS Security Credentials) 페이지로 이동하여 기존 MFA 가상 디바이스 개체를 삭제한 다음 새 개체를 생성하십시오.
    - U2F 보안 키의 경우, AWS 보안 자격 증명(AWS Security Credentials) 페이지로 이동하여 기존 U2F 키를 비활성화한 다음 새 키를 활성화하십시오.
    - 하드웨어 MFA 디바이스의 경우, 타사 공급업체에 연락해 디바이스 수리 또는 교체를 위한 도움을 받습니다. 새 디바이스를 받기 전까지 다른 인증 요소를 사용하여 계속 로그인할 수 있습니다. 하드웨어 MFA 디바이스를 새로 받은 후에는 AWS 보안 자격 증명(AWS Security Credentials) 페이지로 이동하여 기존 MFA 하드웨어 디바이스 개체를 삭제한 다음 새 개체를 생성하십시오.

    Note

    잃어버렸거나 도난당한 MFA 디바이스를 동일한 유형의 디바이스로 대체해야 하는 것은 아닙니다. 예를 들어, U2F 보안 키가 망가져 새로 주문한 경우, 새로운 U2F 보안 키를 받을 때까지는 가상 MFA 또는 하드웨어 MFA 디바이스를 사용할 수 있습니다.
11. MFA 디바이스가 없거나 도난당한 경우에는 인증 디바이스를 훔친 공격자가 현재 암호를 알 수 있으므로 AWS 비밀번호도 변경하십시오 (p. 100).

IAM 사용자 MFA 디바이스 복구

디바이스가 분실 또는 작동 중지된 경우 IAM 사용자는 직접 복구할 수 없습니다. 해당 사용자는 관리자에 문의하여 디바이스를 비활성화해야 합니다. 그러면 새 디바이스를 활성화할 수 있습니다.

IAM 사용자로 MFA 디바이스 도움을 받으려면

1. AWS 관리자나 그 밖에 IAM 사용자의 사용자 이름 및 암호를 제공한 담당자에게 문의합니다. MFA 디바이스 비활성화 (p. 142) 설명대로 관리자가 MFA 디바이스를 비활성화해야 로그인할 수 있습니다.
2. 다음 단계는 사용 중인 MFA의 유형에 따라 다릅니다.

    - 가상 MFA 디바이스의 경우, 디바이스에서 계정을 제거합니다. 그런 다음 가상 멀티 팩터 인증(MFA) 디바이스 활성화(콘솔) (p. 122) 설명대로 가상 디바이스를 활성화합니다.
    - U2F 보안 키의 경우, 타사 공급업체에 연락해 디바이스 교체를 위한 도움을 받습니다. 새로운 U2F 보안 키를 받은 경우, U2F 보안 키 활성화(콘솔) (p. 125)에 설명된 대로 활성화합니다.
    - 하드웨어 MFA 디바이스의 경우, 타사 공급업체에 연락해 디바이스 수리 또는 교체를 위한 도움을 받습니다. 물리적 MFA 디바이스를 새로 받은 후에는 하드웨어 MFA 디바이스 활성화(콘솔) (p. 130) 설명대로 디바이스를 활성화합니다.

    Note

    잃어버렸거나 도난당한 MFA 디바이스를 동일한 유형의 디바이스로 대체해야 하는 것은 아닙니다. 예를 들어, U2F 보안 키가 망가져 새로 주문한 경우, 새로운 U2F 보안 키를 받을 때까지는 가상 MFA 또는 하드웨어 MFA 디바이스를 사용할 수 있습니다.
3. MFA 디바이스가 없거나 도난당한 경우에는 인증 디바이스를 훔친 공격자가 현재 암호를 알 수 있으므로 비밀번호도 변경하십시오 (p. 110).

MFA 보호 API 액세스 구성

사용자가 호출할 수 있는 API 작업을 IAM 정책을 사용해 지정할 수 있습니다. 어떤 경우에는 사용자가 특히 중요한 작업을 수행할 수 있게 허용하기 전에 AWS 멀티 팩터 인증(MFA)으로 인증을 받도록 요구하는 추가 보안이 필요할 수 있습니다.

예를 들어 사용자가 Amazon EC2 `RunInstances`, `DescribeInstances` 및 `StopInstances` 작업을 수행하도록 허용하는 정책이 있을 수 있습니다. 하지만 `TerminateInstances`처럼 안전하지 않은 작업의 경우 이를 제한해 사용자가 AWS MFA 디바이스에서 인증할 때만 작업을 수행하도록 해야 할 필요가 있을 수 있습니다.

주제

개요

API 작업에 MFA 보호를 추가하려면 다음과 같은 작업이 필요합니다.

1. 관리자는 MFA 인증이 필요한 API 요청을 해야 하는 각 사용자에 대해 AWS MFA 디바이스를 구성합니다. 이 프로세스는 MFA 디바이스 활성화 (p. 120)에 설명되어 있습니다.
2. 관리자는 사용자가 AWS MFA 디바이스로 인증했는지 여부를 확인하는 `Condition` 요소가 포함된 사용자 정책을 생성합니다.
3. 나중에 설명할 MFA 보호에 관한 시나리오에 따라 사용자는 MFA 파라미터를 지원하는 AWS STS API 작업인 AssumeRole 또는 GetSessionToken 중 하나를 호출합니다. 사용자는 사용자와 연결된 디바이스의 디바이스 식별자를 호출에 포함시킵니다. 또한 사용자는 디바이스에 생성하는 시간 기반 일회용 암호(TOTP)도 포함시킵니다. 각각의 경우, 사용자는 AWS에 추가 요청하는 데 사용하기 위해 임시 보안 자격 증명을 다시 가져옵니다.

   Note

   서비스의 API 작업에 대한 MFA 보호 기능은 해당 서비스에서 임시 보안 자격 증명을 지원하는 경우에만 사용 가능합니다. 이러한 서비스 목록은 임시 보안 자격 증명을 사용하여 AWS에 액세스 단원을 참조하십시오.

권한 부여에 실패한 경우 AWS는 "액세스가 거부되었습니다."라는 오류 메시지를 반환합니다(무단 액세스의 경우와 동일). MFA 보호 API 정책이 적용되는 경우, 사용자가 유효한 MFA 인증 없이 API 작업을 호출하려 하면 AWS에서는 정책에 지정된 API 작업에 대한 액세스를 거부합니다. API 작업 요청의 타임스탬프가 정책에 지정된 허용 범위를 벗어난 경우에도 작업이 거부됩니다. 사용자는 MFA 코드와 디바이스 일련 번호로 새 임시 보안 자격 증명을 요청하여 MFA 인증을 다시 해야 합니다.

MFA 조건이 포함된 IAM 정책

MFA 조건이 포함된 정책은 다음에 연결할 수 있습니다.

- IAM 사용자 또는 그룹
- Amazon S3 버킷, Amazon SQS 대기열 또는 Amazon SNS 주제 등의 리소스
- 사용자가 수임할 수 있는 IAM 역할의 신뢰 정책

정책의 MFA 조건을 사용해 다음과 같은 속성을 확인할 수 있습니다.

- 존재 - 사용자가 MFA로 인증했는지 간단히 확인하려면 `aws:MultiFactorAuthPresent` 키가 `Bool` 조건에서 `True`인지 확인합니다. 사용자가 단기 자격 증명으로 인증하는 경우에만 키가 있습니다. 액세스 키와 같은 장기 자격 증명에는 이 키가 포함되어 있지 않습니다.
- 기간 - MFA 인증 이후 지정된 시간 내에서만 액세스 권한을 부여하고 싶은 경우, 숫자 조건 유형을 사용하여 `aws:MultiFactorAuthAge` 키의 나이와 값(예: 3,600초)을 비교합니다. MFA가 사용되지 않는 경우 `aws:MultiFactorAuthAge` 키가 없습니다.

다음 예는 MFA 조건을 포함해 MFA 인증이 있는지 테스트하는 IAM 역할의 신뢰 정책을 보여 줍니다. 이 정책을 통해 `Principal` 요소(`ACCOUNT-B-ID`를 유효한 AWS 계정 ID로 대체)에 지정된 AWS 계정의 사용자는 이 정책이 연결된 역할을 수임할 수 있습니다. 그러나 이러한 사용자는 MFA를 사용하여 인증을 받은 경우에만 역할을 수임할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"AWS": "ACCOUNT-B-ID"},
    "Action": "sts:AssumeRole",
    "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
  }
}
```

MFA의 조건 유형에 대한 자세한 내용은 AWS 전역 조건 컨텍스트 키 (p. 650), 숫자 조건 연산자 (p. 603) 및 조건 키의 존재를 확인하는 조건 연산자 (p. 608) 단원을 참조하십시오.

GetSessionToken과 AssumeRole 중에서 선택하기

AWS STS에서는 사용자가 MFA 정보를 전달할 수 있도록 `GetSessionToken`과 `AssumeRole`이라는 두 가지 API 작업을 제공합니다. 사용자가 임시 보안 자격 증명을 가져오기 위해 호출하는 API 작업은 다음 시나리오 중 어떤 것이 적용되느냐에 따라 달라집니다.

다음 시나리오에는 **`GetSessionToken`**을 사용합니다.

- 요청을 수행하는 IAM 사용자와 동일한 AWS 계정의 리소스에 액세스하는 API 작업을 호출합니다. `GetSessionToken` 요청에서 얻는 임시 자격 증명은, 자격 증명 요청에 MFA 정보를 포함하는 경우에 한해, IAM 및 AWS STS API 작업에 액세스할 수 있다는 점에 유의하십시오. `GetSessionToken`에서 반환하는 임시 자격 증명에 MFA 정보가 포함되어 있으므로 자격 증명에서 수행하는 개별 API 작업에서 MFA를 확인할 수 있습니다.
- MFA 조건이 포함된 리소스 기반 정책으로 보호되는 리소스에 액세스.

`GetSessionToken` 작업의 목적은 MFA를 사용하는 사용자를 인증하는 것입니다. 정책을 사용하여 인증 작업을 제어할 수는 없습니다.

다음 시나리오에는 **`AssumeRole`**을 사용합니다.

- 같은 또는 다른 AWS 계정의 리소스에 액세스하는 API 작업을 호출합니다. API 호출은 모든 IAM 또는 AWS STS API를 포함할 수 있습니다. 액세스를 보호하기 위해 사용자가 역할을 수임하는 시각에 MFA를 적용한다는 것에 유의하십시오. `AssumeRole`에서 반환하는 임시 자격 증명은 컨텍스트에 MFA 정보를 포함하고 있지 않으므로 MFA에 대한 개별 API 작업을 확인할 수 없습니다. 이것이 바로 `GetSessionToken`을 사용해 리소스 기반 정책에 의해 보호되는 리소스에 대한 액세스를 제한해야 하는 이유입니다.

이러한 시나리오가 구현되는 방식에 대한 세부 정보는 이 문서의 후반부에 나와 있습니다.

MFA 보호 API 액세스에 대한 중요 사항

API 작업에 대한 MFA 보호가 지닌 다음과 같은 측면을 이해하는 것이 중요합니다.

- MFA 보호는 임시 보안 자격 증명을 사용하는 경우에만 제공되며, 임시 보안 자격 증명은 `AssumeRole` 또는 `GetSessionToken`을 사용해 얻어야 합니다.
- AWS 계정 루트 사용자 자격 증명으로는 MFA 보호 API 액세스를 사용할 수 없습니다.
- U2F 보안 키로는 MFA 보호 API 액세스를 사용할 수 없습니다.
- 연동 사용자는 AWS 서비스에 사용할 MFA 디바이스를 할당받을 수 없으므로, MFA에서 제어하는 AWS 리소스에 액세스할 수 없습니다. (다음 참조.)
- 임시 자격 증명을 반환하는 다른 AWS STS API 작업에서는 MFA를 지원하지 않습니다. `AssumeRoleWithWebIdentity` 및 `AssumeRoleWithSAML`의 경우 사용자는 외부 공급자에 의해 인증되며 AWS에서는 그 공급자가 MFA를 요구했는지 여부를 확인할 수 없습니다. `GetFederationToken`의 경우 MFA가 특정 사용자와 반드시 연결되는 것은 아닙니다.
- 이와 마찬가지로 장기 자격 증명(IAM 사용자 액세스 키 및 루트 사용자 액세스 키)은 만료되지 않기 때문에 MFA 보호 API 액세스를 통해 사용할 수 없습니다.
- 또한, `AssumeRole` 및 `GetSessionToken`은 MFA 정보 없이도 호출할 수 있습니다. 이 경우 호출자는 임시 보안 자격 증명을 다시 가져오지만, 그러한 임시 자격 증명의 세션 정보에는 사용자가 MFA로 인증했는지 나타나지 않습니다.
- API 작업에 대해 MFA 보호를 설정하려면 정책에 MFA 조건을 추가하면 됩니다. MFA 사용을 적용하기 위해 정책에는 `aws:MultiFactorAuthPresent` 조건 키가 포함되어 있어야 합니다. 교차 계정 위임을 위해 역할의 신뢰 정책에는 조건 키가 포함되어 있어야 합니다.
- 다른 AWS 계정이 내 계정의 리소스에 액세스하도록 허용하는 경우, 리소스의 보안은 신뢰할 수 있는 계정, 즉 다른 계정(내 계정이 아님)의 구성에 따라 달라집니다. 이것은 멀티 팩터 인증이 필요할 때도 마찬가지입니다. 가상 MFA 디바이스를 생성할 권한이 있는 신뢰할 수 있는 계정 내의 어떤 자격 증명도 MFA 클레임을 생성하여 역할의 신뢰 정책의 해당 부분을 충족할 수 있습니다. 멀티 팩터 인증을 요구하는 AWS 리소스에 대한 액세스를 다른 계정의 멤버에게 허용하기 전에 신뢰할 수 있는 계정의 소유자가 보안 모범 사례를 따르도록 해야 합니다. 예를 들어 신뢰할 수 있는 계정에서는 MFA 디바이스 관리 API 작업과 같은 중요 API 작업에 대한 액세스를 신뢰할 수 있는 특정 자격 증명으로 제한해야 합니다.
- 정책에 MFA 조건이 포함된 경우, 사용자가 MFA에 인증되지 않거나 잘못된 MFA 디바이스 식별자 또는 잘못된 TOTP를 제공하는 경우 요청이 거부됩니다.

시나리오: 교차 계정 위임에 대한 MFA 보호

이 시나리오에서는 다른 계정의 IAM 사용자에게 액세스 권한을 위임하려고 합니다. 단 해당 사용자가 AWS MFA 디바이스로 인증된 경우에 한합니다. (교차 계정 위임에 대한 자세한 내용은 역할 용어 및 개념 (p. 175) 단원을 참조하십시오.)

계정 A(액세스할 리소스를 소유한 신뢰하는 계정)에 관리자 권한이 있는 IAM 사용자 Anaya가 있다고 가정해 봅시다. 그녀는 계정 B(신뢰할 수 있는 계정)의 사용자 Richard에게 액세스 권한을 부여하고 싶지만, Richard가 MFA에 인증되었는지 확인한 후에 그가 역할을 수임하기를 원합니다.

1. 신뢰하는 계정 A에서 Anaya는 `CrossAccountRole`이라는 IAM 역할을 생성하고 해당 역할의 신뢰 정책에서 보안 주체를 계정 B의 계정 ID로 설정합니다. 이 신뢰 정책은 AWS STS `AssumeRole` 작업에 권한을 부여합니다. 또한 Anaya는 다음 예와 같이 신뢰 정책에 MFA 조건을 추가합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"AWS": "ACCOUNT-B-ID"},
    "Action": "sts:AssumeRole",
    "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
  }
}
```

2. Anaya는 역할이 수행할 수 있는 작업을 지정하는 역할에 권한 정책을 추가합니다. MFA 보호 기능이 포함된 역할의 권한 정책은 다른 역할 권한 정책과 다르지 않습니다. 다음 예제에서는 Anaya가 역할에 추

가하는 정책을 보여 줍니다. 역할을 맡은 사용자는 이 정책을 통해 계정 A의 `Books` 테이블에서 Amazon DynamoDB 작업을 수행할 수 있고, 아울러 콘솔에서 작업을 수행할 때 필요한 `dynamodb:ListTables` 작업을 할 수 있습니다.

> **Note**
>
> 권한 정책은 MFA 조건을 포함하지 않습니다. MFA 인증은 사용자가 역할을 수임할 수 있는지 여부를 결정하는 데에만 사용된다는 점을 알아두십시오. 사용자가 역할을 수임하면 MFA 검사가 추가로 수행되지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TableActions",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:*:ACCOUNT-A-ID:table/Books"
        },
        {
            "Sid": "ListTable",
            "Effect": "Allow",
            "Action": "dynamodb:ListTable",
            "Resource": "*"
        }
    ]
}
```

3. 신뢰할 수 있는 계정 B에서 관리자는 IAM 사용자 Richard가 AWS MFA 디바이스로 구성되었는지, 그리고 그가 이 디바이스의 ID를 알고 있는지 확인합니다. 디바이스 ID란 하드웨어 MFA 디바이스의 경우 일련 번호이며, 가상 MFA 디바이스의 경우 해당 디바이스의 ARN입니다.
4. 계정 B에서 관리자는 사용자 Richard(또는 그가 소속된 그룹)에게 `AssumeRole` 작업을 호출할 수 있도록 허용하는 다음과 같은 정책을 연결합니다. 리소스는 Anaya가 1단계에서 생성한 역할의 ARN으로 설정됩니다. 이 정책에는 MFA 조건이 포함되어 있지 않습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["sts:AssumeRole"],
    "Resource": ["arn:aws:iam::ACCOUNT-A-ID:role/CrossAccountRole"]
  }]
}
```

5. 계정 B에서 Richard(또는 Richard가 실행하는 애플리케이션)는 `AssumeRole`을 호출합니다. API 호출에는 위임할 역할의 ARN(`arn:aws:iam::ACCOUNT-A-ID:role/CrossAccountRole`), MFA 디바이스의 ID 및 Richard가 자신의 디바이스에서 가져오는 현재 TOTP가 포함되어 있습니다.

   Richard가 `AssumeRole`을 호출하면, AWS에서 그가 MFA에 대한 요건을 포함해 유효한 자격 증명을 갖고 있는지 여부를 확인합니다. 만일 Richard가 유효한 자격 증명을 갖고 있다면 성공적으로 역할을 수임해 역할의 임시 자격 증명을 사용함과 동시에 계정 A에서 `Books`라는 테이블에 대해 어떤 DynamoDB 작업도 수행할 수 있습니다.

   `AssumeRole`을 호출하는 프로그램의 예는 MFA 인증이 포함된 AssumeRole 호출하기(Python) (p. 153) 단원을 참조하십시오.

시나리오: 현재 계정의 API 작업에 대한 액세스의 MFA 보호

이 시나리오에서는 AWS 계정의 사용자가 AWS MFA 디바이스를 사용해 인증받은 경우에만 중요한 API 작업에 액세스할 수 있는지 확인해야 합니다.

계정 A에 EC2 인스턴스로 작업해야 하는 개발자 그룹이 있다고 가정해 봅시다. 일반적인 개발자들은 이 인스턴스를 사용할 수 있지만, `ec2:StopInstances` 또는 `ec2:TerminateInstances` 작업에 대한 권한은 없습니다. 그와 같은 "안전하지 않은" 권한이 있는 작업을 몇몇 신뢰할 수 있는 사용자만 액세스할 수 있게 제한하고자 하여, 이러한 민감한 Amazon EC2 작업을 허용하는 정책에 MFA 보호를 추가합니다.

이 시나리오에서 신뢰할 수 있는 사용자 중 한 명은 사용자 Sofía입니다. 사용자 Anaya는 계정 A의 관리자입니다.

1. Anaya는 Sofia가 AWS MFA 디바이스로 구성되었는지, 그리고 Sofia가 이 디바이스의 ID를 알고 있는지 확인합니다. 디바이스 ID란 하드웨어 MFA 디바이스의 경우 일련 번호이며, 가상 MFA 디바이스의 경우 해당 디바이스의 ARN입니다.
2. Anaya는 `EC2-Admins`라는 그룹을 생성하고 이 그룹에 사용자 Sofía를 추가합니다.
3. Anaya는 `EC2-Admins` 그룹에 다음과 같은 정책을 연결합니다. 이 정책은 사용자에게 Amazon EC2 `StopInstances` 및 `TerminateInstances` 작업을 호출할 권한을 부여하는데, 단 이 사용자가 MFA를 사용하여 인증되었을 경우에 한합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Resource": ["*"],
    "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
  }]
}
```

4. **Note**

   이 정책의 효력이 발생하려면 사용자는 먼저 로그아웃한 한 후 다시 로그인해야 합니다.

   사용자 Sofía가 Amazon EC2 인스턴스를 중지하거나 종료해야 하는 경우, Sofia(또는 Sofia가 실행하는 애플리케이션)는 `GetSessionToken`을 호출합니다. 이 API 작업에서는 MFA 디바이스의 ID와 Sofia가 자신의 디바이스에서 가져오는 현재 TOTP를 전달합니다.
5. 사용자 Sofía(또는 Sofía가 사용하는 애플리케이션)은 `GetSessionToken`에서 제공하는 임시 자격 증명을 사용하여 Amazon EC2 `StopInstances` 또는 `TerminateInstances` 작업을 호출합니다.

   `GetSessionToken`을 호출하는 프로그램의 예는 이 문서의 후반부에 있는 MFA 인증이 포함된 GetSessionToken 호출하기(Python 및 C#) (p. 151) 단원을 참조하십시오.

시나리오: 리소스 기반 정책이 있는 리소스에 대한 MFA 보호

이 시나리오에서는 S3 버킷, SQS 대기열 또는 SNS 주제의 소유자입니다. 리소스에 액세스하는 모든 AWS 계정 사용자가 AWS MFA 디바이스로 인증되었는지 확인하려고 합니다.

이 시나리오는 사용자가 역할을 먼저 수임하지 않고도 교차 계정 MFA 보호를 제공하는 방법을 설명합니다. 이 경우 사용자는 세 가지 조건이 충족되면 리소스에 액세스할 수 있습니다. 즉 사용자는 MFA로 인증을 받아야 하고, `GetSessionToken`에서 임시 보안 자격 증명을 가져올 수 있어야 하며, 리소스의 정책에서 신뢰하는 계정에 로그인해 있어야 합니다.

계정 A에 속해 있고 S3 버킷을 생성한다고 가정해 봅시다. 여러 AWS 계정에 속한 사용자에게 이 버킷에 대한 액세스를 부여하되, 사용자가 MFA로 인증한 경우에 한하고자 합니다.

이 시나리오에서 사용자 Anaya는 계정 A의 관리자입니다. 사용자 Nikhil은 계정 C의 IAM 사용자입니다.

1. 계정 A에서 Anaya는 `Account-A-bucket`이라는 버킷을 생성합니다.

2. Anaya는 이 버킷에 버킷 정책을 추가합니다. 이 정책은 계정 A, 계정 B 또는 계정 C의 모든 사용자가 이 버킷에서 Amazon S3 `PutObject` 및 `DeleteObject` 작업을 수행하도록 허용합니다. 이 정책에는 MFA 조건이 포함되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {"AWS": [
      "ACCOUNT-A-ID",
      "ACCOUNT-B-ID",
      "ACCOUNT-C-ID"
    ]},
    "Action": [
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": ["arn:aws:s3:::ACCOUNT-A-BUCKET-NAME/*"],
    "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
  }]
}
```

   Note

   Amazon S3는 루트 계정 액세스에 대해(서만) MFA Delete 기능을 제공합니다. 버킷의 버전 관리 상태를 설정할 때 Amazon S3 MFA Delete를 활성화할 수 있습니다. Amazon S3 MFA Delete는 IAM 사용자에게 적용되지 않으며, MFA 보호 API 액세스에서 독립적으로 관리됩니다. 버킷을 삭제할 권한이 있는 IAM 사용자도 Amazon S3 MFA 삭제 기능이 활성화된 버킷은 삭제할 수 없습니다. Amazon S3 MFA Delete에 대한 자세한 내용은 MFA Delete 단원을 참조하십시오.

3. 계정 C에서 관리자는 사용자 Nikhil이 AWS MFA 디바이스로 구성되었는지, 그리고 그가 이 디바이스의 ID를 알고 있는지 확인합니다. 디바이스 ID란 하드웨어 MFA 디바이스의 경우 일련 번호이며, 가상 MFA 디바이스의 경우 해당 디바이스의 ARN입니다.
4. 계정 C에서 Nikhil(또는 그가 실행하는 애플리케이션)은 `GetSessionToken`을 호출합니다. 이 호출에는 MFA 디바이스의 ID 또는 ARN과 Nikhil이 자신의 디바이스에서 가져오는 현재 TOTP가 포함되어 있습니다.
5. Nikhil(또는 그가 사용하는 애플리케이션)은 `GetSessionToken`에서 반환하는 임시 자격 증명을 사용하여 `PutObject`으로 파일을 업로드하는 Amazon S3 `Account-A-bucket` 작업을 호출합니다.

   `GetSessionToken`을 호출하는 프로그램의 예는 이 문서의 후반부에 있는 MFA 인증이 포함된 GetSessionToken 호출하기(Python 및 C#) (p. 151) 단원을 참조하십시오.

   Note

   `AssumeRole`이 반환하는 임시 자격 증명은 이 경우에는 유효하지 않습니다. 사용자는 역할 수임을 위해 MFA 정보를 제공할 수 있지만 `AssumeRole`에서 반환하는 임시 자격 증명에는 MFA 정보가 포함되어 있지 않습니다. 이 정보는 정책의 MFA 조건을 충족하기 위해 필요합니다.

샘플 코드: 멀티 팩터 인증이 포함된 자격 증명 요청하기

다음 예에서는 `GetSessionToken` 및 `AssumeRole` 작업을 호출하고 MFA 인증 파라미터를 전달하는 방법을 보여줍니다. 권한이 없어도 `GetSessionToken`을 호출할 수 있지만, `AssumeRole`을 호출할 수 있게 허용하는 정책이 있어야 합니다. 반환된 자격 증명은 계정 내 모든 S3 버킷의 목록을 나열하는 데 사용됩니다.

MFA 인증이 포함된 GetSessionToken 호출하기(Python 및 C#)

AWS SDK for Python (Boto) 및 .NET용 AWS SDK를 토대로 작성된 다음 예는 `GetSessionToken`을 호출하고 MFA 인증 정보를 전달하는 방법을 보여 줍니다. `GetSessionToken` 작업에서 반환하는 임시 보안 자격 증명은 이어서 계정 내 모든 S3 버킷의 목록을 나열하는 데 사용됩니다.

이 코드를 실행하는 사용자(또는 사용자가 속한 그룹)에게 연결된 정책에서는 반환된 임시 자격 증명에 대한 권한을 제공합니다. 이 예의 경우 정책에서 사용자에게 Amazon S3 `ListBuckets` 작업을 요청할 수 있는 권한을 부여해야 합니다.

Python 사용하기

```
import boto
from boto.s3.connection import S3Connection
from boto.sts import STSConnection

# Prompt for MFA time-based one-time password (TOTP)
mfa_TOTP = raw_input("Enter the MFA code: ")

# The calls to AWS STS GetSessionToken must be signed with the access key ID and secret
# access key of an IAM user. The credentials can be in environment variables or in
# a configuration file and will be discovered automatically
# by the STSConnection() function. For more information, see the Python SDK
# documentation: http://boto.readthedocs.org/en/latest/boto_config_tut.html

sts_connection = STSConnection()

# Use the appropriate device ID (serial number for hardware device or ARN for virtual
 device).
# Replace ACCOUNT-NUMBER-WITHOUT-HYPHENS and MFA-DEVICE-ID with appropriate values.

tempCredentials = sts_connection.get_session_token(
    duration=3600,
    mfa_serial_number="&region-arn;iam::ACCOUNT-NUMBER-WITHOUT-HYPHENS:mfa/MFA-DEVICE-ID",
    mfa_token=mfa_TOTP
)

# Use the temporary credentials to list the contents of an S3 bucket
s3_connection = S3Connection(
    aws_access_key_id=tempCredentials.access_key,
    aws_secret_access_key=tempCredentials.secret_key,
    security_token=tempCredentials.session_token
)

# Replace BUCKET-NAME with an appropriate value.
bucket = s3_connection.get_bucket(bucket_name="BUCKET-NAME")
objectlist = bucket.list()
for obj in objectlist:
    print obj.name
```

C# 사용하기

```
Console.Write("Enter MFA code: ");
string mfaTOTP = Console.ReadLine(); // Get string from user

/* The calls to AWS STS GetSessionToken must be signed using the access key ID and secret
   access key of an IAM user. The credentials can be in environment variables or in
   a configuration file and will be discovered automatically
   by the AmazonSecurityTokenServiceClient constructor. For more information, see
   https://docs.aws.amazon.com/sdk-for-net/v2/developer-guide/net-dg-config-creds.html
*/
AmazonSecurityTokenServiceClient stsClient =
    new AmazonSecurityTokenServiceClient();
GetSessionTokenRequest getSessionTokenRequest = new GetSessionTokenRequest();
getSessionTokenRequest.DurationSeconds = 3600;

// Replace ACCOUNT-NUMBER-WITHOUT-HYPHENS and MFA-DEVICE-ID with appropriate values
getSessionTokenRequest.SerialNumber = "arn:aws:iam::ACCOUNT-NUMBER-WITHOUT-HYPHENS:mfa/MFA-
DEVICE-ID";
```

```
getSessionTokenRequest.TokenCode = mfaTOTP;

GetSessionTokenResponse getSessionTokenResponse =
    stsClient.GetSessionToken(getSessionTokenRequest);

// Extract temporary credentials from result of GetSessionToken call
GetSessionTokenResult getSessionTokenResult =
    getSessionTokenResponse.GetSessionTokenResult;
string tempAccessKeyId = getSessionTokenResult.Credentials.AccessKeyId;
string tempSessionToken = getSessionTokenResult.Credentials.SessionToken;
string tempSecretAccessKey = getSessionTokenResult.Credentials.SecretAccessKey;
SessionAWSCredentials tempCredentials = new SessionAWSCredentials(tempAccessKeyId,
    tempSecretAccessKey, tempSessionToken);

// Use the temporary credentials to list the contents of an S3 bucket
// Replace BUCKET-NAME with an appropriate value
ListObjectsRequest S3ListObjectsRequest = new ListObjectsRequest();
S3ListObjectsRequest.BucketName = "BUCKET-NAME";
S3Client = AWSClientFactory.CreateAmazonS3Client(tempCredentials);
ListObjectsResponse S3ListObjectsResponse =
    S3Client.ListObjects(S3ListObjectsRequest);
foreach (S3Object s3Object in S3ListObjectsResponse.S3Objects)
{
    Console.WriteLine(s3Object.Key);
}
```

MFA 인증이 포함된 AssumeRole 호출하기(Python)

AWS SDK for Python (Boto)을 토대로 작성된 다음 예는 `AssumeRole`을 호출하고 MFA 인증 정보를 전달하는 방법을 보여 줍니다. `AssumeRole`에서 반환한 임시 보안 자격 증명은 계정의 모든 Amazon S3 버킷을 나열하는 데 사용됩니다.

이 시나리오에 대한 자세한 내용은 시나리오: 교차 계정 위임에 대한 MFA 보호 (p. 148)를 참조하십시오.

```
import boto
from boto.s3.connection import S3Connection
from boto.sts import STSConnection

# Prompt for MFA time-based one-time password (TOTP)
mfa_TOTP = raw_input("Enter the MFA code: ")

# The calls to AWS STS AssumeRole must be signed with the access key ID and secret
# access key of an IAM user. (The AssumeRole API operation can also be called using
 temporary
# credentials, but this example does not show that scenario.)
# The IAM user credentials can be in environment variables or in
# a configuration file and will be discovered automatically
# by the STSConnection() function. For more information, see the Python SDK
# documentation: http://boto.readthedocs.org/en/latest/boto_config_tut.html

sts_connection = STSConnection()

# Use appropriate device ID (serial number for hardware device or ARN for virtual device)
# Replace ACCOUNT-NUMBER-WITHOUT-HYPHENS, ROLE-NAME, and MFA-DEVICE-ID with appropriate
 values
tempCredentials = sts_connection.assume_role(
    role_arn="arn:aws:iam::ACCOUNT-NUMBER-WITHOUT-HYPHENS:role/ROLE-NAME",
    role_session_name="AssumeRoleSession1",
    mfa_serial_number="arn:aws:iam::ACCOUNT-NUMBER-WITHOUT-HYPHENS:mfa/MFA-DEVICE-ID",
    mfa_token=mfa_TOTP
)

# Use the temporary credentials to list the contents of an S3 bucket
s3_connection = S3Connection(
```

```
    aws_access_key_id=tempCredentials.credentials.access_key,
    aws_secret_access_key=tempCredentials.credentials.secret_key,
    security_token=tempCredentials.credentials.session_token
)

# Replace BUCKET-NAME with a real bucket name
bucket = s3_connection.get_bucket(bucket_name="BUCKET-NAME")
objectlist = bucket.list()
for obj in objectlist:
    print obj.name
```

미사용 자격 증명 찾기

AWS 계정의 보안을 강화하려면 필요 없는 IAM 사용자 자격 증명(암호화 액세스 키)을 삭제합니다. 예를 들어, 사용자가 조직을 떠나거나 AWS 액세스가 더 이상 필요하지 않은 경우 해당 자격 증명을 찾아서 더 이상 작동하지 않도록 해야 합니다. 더 이상 필요 없는 자격 증명을 삭제하는 것이 가장 좋습니다. 나중에 필요한 경우가 생기면 언제든지 다시 생성할 수 있습니다. 적어도 암호를 변경하거나 액세스 키를 비활성화하여 이전 사용자가 더 이상 액세스할 수 없게 해야 합니다.

미사용은 이와는 다른 것으로 보통 특정 기간 동안 사용되지 않은 자격 증명을 뜻합니다.

미사용 암호 찾기

AWS Management 콘솔을 사용하여 사용자의 암호 사용 정보를 볼 수 있습니다. 사용자 수가 많을 경우 콘솔을 사용하여 각 사용자가 자신의 콘솔 암호를 사용한 최종 시각에 대한 정보가 담긴 자격 증명 보고서를 다운로드할 수 있습니다. AWS CLI 또는 IAM API에서 그 정보에 액세스할 수도 있습니다.

미사용 암호를 확인하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 필요할 경우 사용자 테이블에 Console last sign-in(콘솔 마지막 로그인) 열을 추가합니다.
   a. 테이블 위 맨 오른쪽에서 설정 아이콘( )을 선택합니다.
   b. Manage Columns(열 관리)에서 Console last sign-in(콘솔 마지막 로그인)을 선택합니다.
   c. 닫기를 선택하여 사용자 목록으로 돌아갑니다.
4. Console last sign-in(콘솔 마지막 로그인) 열에는 사용자가 콘솔을 통해 마지막으로 AWS에 로그인한 날짜부터 경과한 일수가 표시됩니다. 이 정보를 통해 지정된 기간 이상 동안 암호를 사용하여 로그인하지 않은 사용자를 확인할 수 있습니다. 암호 사용자 중 로그인한 적이 없는 사용자는 이 열에 없음이라고 표시됩니다. 없음은 암호가 없는 사용자를 나타냅니다. 최근에 사용된 적이 없는 암호는 삭제해야 할 자격 증명을 식별하기 위한 좋은 기준이 될 수 있습니다.

   Important

   서비스 문제로 인해 암호가 마지막으로 사용된 데이터에 2018년 5월 3일 22:50 PDT ~ 2018년 5월 23일 14:08 PDT 사이의 암호 사용이 포함되어 있지 않습니다. 이는 IAM 콘솔에 표시되는 마지막 로그인 날짜, IAM 자격 증명 보고서의 암호가 마지막으로 사용된 날짜와 GetUser API 연산에 의해 반환되는 암호가 마지막으로 사용된 날짜에 영향을 줍니다. 사용자가 해당 기간에 로그인한 경우 반환되는 암호가 마지막으로 사용된 날짜는 사용자가 2018년 5월 3일 이전에 마지막으로 로그인한 날짜입니다. 사용자가 2018년 5월 23일 14:08 PDT 이후에 로그인한 경우 반환되는 암호가 마지막으로 사용된 날짜는 정확합니다.
   암호가 마지막으로 사용된 정보를 사용하여 삭제할 사용되지 않은 자격 증명을 식별할 경우(예: 지난 90일 동안 AWS에 로그인하지 않은 사용자 삭제) 2018년 5월 23일 이후의 날짜를 포함하도록 평가 기간을 조정하는 것이 좋습니다. 또는 사용자가 액세스 키를 사용하여 AWS에 프로그래밍 방식으로 액세스하는 경우 액세스 키가 마지막으로 사용된 정보가 모든 날짜에 대해 정확하므로 해당 정보를 참조할 수 있습니다.

자격 증명 보고서를 다운로드하여 미사용 암호를 찾으려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Credential Report(자격 증명 보고서)를 선택합니다.
3. 보고서 다운로드를 선택하여 `status_reports_<date>T<time>.csv`라는 쉼표 구분 값(CSV) 파일을 다운로드합니다. 5번째 열에는 날짜가 있는 `password_last_used` 열 또는 다음 중 하나가 있습니다.
   - 해당 사항 없음 – 할당된 암호가 전혀 없는 사용자
   - no_information – IAM이 2014년 10월 20일 암호 수명을 추적하기 시작한 이후 암호를 사용하지 않은 사용자들

미사용 암호를 찾으려면(AWS CLI)

미사용 암호를 찾으려면 다음 명령을 실행합니다.

- `aws iam list-users`는 각자 `PasswordLastUsed` 값이 있는 사용자 목록을 반환합니다. 값이 비어 있는 경우 사용자가 암호가 없거나 2014년 10월 20일 IAM이 암호 수명을 추적하기 시작한 이후 암호가 사용되지 않은 것입니다.

미사용 암호를 찾으려면(AWS API)

미사용 암호를 찾으려면 다음 연산을 호출합니다.

- `ListUsers`는 각각 `<PasswordLastUsed>` 값이 있는 사용자의 집합을 반환합니다. 값이 비어 있는 경우 사용자가 암호가 없거나 2014년 10월 20일 IAM이 암호 수명을 추적하기 시작한 이후 암호가 사용되지 않은 것입니다.

자격 증명 보고서를 다운로드하기 위한 명령어에 대한 자세한 내용은 자격 증명 보고서 가져오기(AWS CLI) (p. 160)단원을 참조하십시오.

미사용 액세스 키 찾기

AWS Management 콘솔을 사용하여 사용자의 액세스 키 사용 정보를 볼 수 있습니다. 사용자 수가 많을 경우 콘솔을 사용하여 자격 증명 보고서를 다운로드하여 각 사용자가 자신의 액세스 키를 마지막으로 사용한 때를 알 수 있습니다. AWS CLI 또는 IAM API에서 그 정보에 액세스할 수도 있습니다.

미사용 액세스 키를 확인하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 필요할 경우 사용자 테이블에 Access key last used(마지막으로 사용한 액세스 키) 열을 추가합니다.
   a. 테이블 위 맨 오른쪽에서 설정 아이콘( )을 선택합니다.
   b. Manage Columns(열 관리)에서 Access key last used(마지막으로 사용한 액세스 키)를 선택합니다.
   c. 닫기를 선택하여 사용자 목록으로 돌아갑니다.
4. Access key last used(마지막으로 사용한 액세스 키) 열에는 사용자가 프로그래밍 방식으로 AWS에 마지막으로 액세스한 때부터 경과한 일수가 표시됩니다. 이 정보를 통해 지정된 기간 이상 동안 액세스 키를 사용하지 않은 사용자를 확인할 수 있습니다. 액세스 키가 없는 사용자는 이 열에 없음이라고 표시됩니다. 최근에 사용된 적이 없는 액세스 키는 삭제해야 할 자격 증명을 식별하기 위한 좋은 기준이 될 수 있습니다.

자격 증명 보고서를 다운로드하여 미사용 액세스 키를 찾으려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Credential Report(자격 증명 보고서)를 선택합니다.
3. 보고서 다운로드를 선택하여 `status_reports_<date>T<time>.csv`라는 쉼표 구분 값(CSV) 파일을 다운로드합니다. 열 11부터 13에는 액세스 키 1의 마지막 사용 날짜, 리전 및 서비스 정보가 표시됩니다. 열 16부터 18에는 액세스 키 2에 대해 동일한 정보가 표시됩니다. 값이 해당 사항 없음으로 되어 있는 것은 사용자에게 액세스 키가 없거나 2015년 4월 22일 IAM이 액세스 키 수명을 추적하기 시작한 이후 사용자가 액세스 키를 사용하지 않았다는 것입니다.

미사용 액세스 키를 확인하려면(AWS CLI)

미사용 액세스 키를 찾으려면 다음 명령을 실행합니다.

- `aws iam list-access-keys`는 `AccessKeyID`를 포함해 사용자의 액세스 키에 대한 정보를 반환합니다.
- `aws iam get-access-key-last-used`는 액세스 키 ID를 받아들여 `LastUsedDate` 액세스 키의 마지막 사용 및 `Region` 마지막으로 요청된 서비스의 `ServiceName`을 포함하는 출력을 반환합니다. `LastUsedDate`가 없는 경우 2015년 4월 22일 IAM이 액세스 키 수명을 추적하기 시작한 이후 액세스 키가 사용되지 않은 것입니다.

미사용 액세스 키를 확인하려면(AWS API)

미사용 액세스 키를 찾으려면 다음 연산을 호출합니다.

- `ListAccessKeys`는 지정된 사용자와 연결된 액세스 키에 대한 `AccessKeyID` 값의 목록을 반환합니다.
- `GetAccessKeyLastUsed`는 액세스 키 ID를 받아들여 값의 집합을 반환합니다. `LastUsedDate`, 액세스 키가 마지막으로 사용된 `Region` 및 마지막으로 요청된 서비스의 `ServiceName`이 포함되어 있습니다. 값이 비어 있는 경우 사용자가 액세스 키가 없거나 2015년 4월 22일 IAM이 액세스 키 수명을 추적하기 시작한 이후 액세스 키가 사용되지 않은 것입니다.

자격 증명 보고서를 다운로드하기 위한 명령어에 대한 자세한 내용은 자격 증명 보고서 가져오기(AWS CLI) (p. 160)단원을 참조하십시오.

AWS 계정의 자격 증명 보고서 가져오기

계정의 모든 사용자와 암호, 액세스 키, MFA 디바이스 등 이들의 자격 증명 상태를 나열하는 자격 증명 보고서를 생성하고 다운로드할 수 있습니다. AWS Management 콘솔, AWS SDK 및 명령줄 도구 또는 IAM API에서 자격 증명 보고서를 가져올 수 있습니다.

자격 증명 보고서를 사용하면 감사 및 규정 준수에 도움이 됩니다. 이 보고서를 통해 암호, 액세스 키 교체 등 자격 증명의 수명 주기 요구 사항이 어떤 영향을 주는지 감사할 수 있습니다. 외부 감사자에게 이 보고서를 제공하거나 보고서를 직접 다운로드할 권한을 감사자에게 부여할 수 있습니다.

최소 네 시간에 한 번씩 자격 증명 보고서를 생성할 수 있습니다. 보고서를 요청하면 IAM은 먼저 해당 AWS 계정의 보고서가 4시간 이내에 생성되었는지 여부를 확인합니다. 네 시간 이내에 생성된 경우 최신 보고서를 다운로드하고, 계정의 최신 보고서가 생성된 지 네 시간이 넘었거나 해당 계정에 대한 이전 보고서가 없는 경우 IAM에서 새 보고서를 생성하여 이를 다운로드합니다.

주제

- 자격 증명 보고서 가져오기(AWS API) (p. 160)

필요한 권한

보고서를 생성하고 다운로드하려면 다음 권한이 필요합니다.

- 자격 증명 보고서를 생성하려면 `GenerateCredentialReport`
- 보고서를 다운로드하려면 `GetCredentialReport`

보고서 형식 이해하기

자격 증명 보고서는 CSV(쉼표로 구분된 값) 파일 형식으로 되어 있습니다. 공통 스프레드시트 소프트웨어로 CSV 파일을 열어 분석을 수행하거나 CSV 파일을 프로그래밍 방식으로 사용하고 사용자 지정 분석을 수행하는 애플리케이션을 구축할 수 있습니다.

CSV 파일에는 다음 열이 포함되어 있습니다:

사용자

사용자의 표시 이름입니다.

arn

사용자의 Amazon 리소스 이름(ARN)입니다. ARN에 대한 자세한 내용은 IAM ARN (p. 564) 단원을 참조하십시오.

user_creation_time

사용자가 생성된 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다.

password_enabled

사용자에게 암호가 있는 경우 이 값은 `TRUE`입니다. 그렇지 않으면 `FALSE`입니다. AWS 계정 루트 사용자 값은 항상 `not_supported`입니다.

password_last_used

AWS 웹 사이트에 로그인하는 데 AWS 계정 루트 사용자 또는 IAM 사용자의 암호가 마지막으로 사용된 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다. 사용자의 마지막 로그인 시간을 캡처하는 AWS 웹 사이트는 AWS Management 콘솔, AWS 토론 포럼 및 AWS Marketplace입니다. 암호가 5분 내에 두 번 이상 사용된 경우, 첫 번째 사용만 이 필드에 기록됩니다.

- 다음과 같은 경우 이 필드의 값은 `no_information`입니다.
  - 사용자의 암호가 사용된 적이 없는 경우.
  - 암호와 관련된 로그인 데이터가 없는 경우, 예를 들어 IAM에서 2014년 10월 20일에 이 정보를 추적하기 시작한 이후로 사용자의 암호가 사용되지 않은 경우.
- 사용자에게 암호가 없는 경우, 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

Important

서비스 문제로 인해 암호가 마지막으로 사용된 데이터에 2018년 5월 3일 22:50 PDT ~ 2018년 5월 23일 14:08 PDT 사이의 암호 사용이 포함되어 있지 않습니다. 이는 IAM 콘솔에 표시되는 마지막 로그인 날짜, IAM 자격 증명 보고서의 암호가 마지막으로 사용된 날짜와 GetUser API 연산에 의해 반환되는 암호가 마지막으로 사용된 날짜에 영향을 줍니다. 사용자가 해당 기간에 로그인한 경우 반환되는 암호가 마지막으로 사용된 날짜는 사용자가 2018년 5월 3일 이전에 마지막으로 로그인한 날짜입니다. 사용자가 2018년 5월 23일 14:08 PDT 이후에 로그인한 경우 반환되는 암호가 마지막으로 사용된 날짜는 정확합니다.
암호가 마지막으로 사용된 정보를 사용하여 삭제할 사용되지 않은 자격 증명을 식별할 경우(예: 지난 90일 동안 AWS에 로그인하지 않은 사용자 삭제) 2018년 5월 23일 이후의 날짜를 포함하도록 평

가 기간을 조정하는 것이 좋습니다. 또는 사용자가 액세스 키를 사용하여 AWS에 프로그래밍 방식으로 액세스하는 경우 액세스 키가 마지막으로 사용된 정보가 모든 날짜에 대해 정확하므로 해당 정보를 참조할 수 있습니다.

password_last_changed

사용자의 암호가 마지막으로 설정된 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다. 사용자에게 암호가 없는 경우, 이 필드의 값은 `N/A`(해당 사항 없음)입니다. AWS 계정(루트)의 값은 항상 `not_supported`입니다.

password_next_rotation

계정에 암호 교체를 요구하는 암호 정책이 있는 경우, 사용자가 새 암호를 설정해야 할 때 이 필드에 날짜 및 시간(ISO 8601 날짜-시간 형식)이 포함됩니다. AWS 계정(루트)의 값은 항상 `not_supported`입니다.

mfa_active

사용자에 대해 멀티 팩터 인증 (p. 119)(MFA) 디바이스를 사용하도록 설정된 경우, 이 값은 `TRUE`입니다. 그렇지 않은 경우 이 값은 `FALSE`입니다.

access_key_1_active

사용자에게 액세스 키가 있고 액세스 키의 상태가 `Active`이면, 이 값은 `TRUE`입니다. 그렇지 않은 경우 이 값은 `FALSE`입니다.

access_key_1_last_rotated

사용자의 액세스 키가 생성되었거나 마지막으로 변경된 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다. 사용자에게 활성 상태의 액세스 키가 없는 경우, 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

access_key_1_last_used_date

사용자의 액세스 키를 AWS API 요청 서명에 마지막으로 사용한 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다. 액세스 키가 15분 내에 두 번 이상 사용된 경우, 첫 번째 사용만 이 필드에 기록됩니다.

다음과 같은 경우 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

- 사용자에게 액세스 키가 없는 경우.
- 액세스 키가 사용된 적이 없는 경우.
- IAM에서 2015년 4월 22일에 이 정보를 추적하기 시작한 이후로 액세스 키가 사용되지 않은 경우.

access_key_1_last_used_region

액세스 키가 마지막으로 사용된 AWS 리전입니다. 액세스 키가 15분 내에 두 번 이상 사용된 경우, 첫 번째 사용만 이 필드에 기록됩니다.

다음과 같은 경우 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

- 사용자에게 액세스 키가 없는 경우.
- 액세스 키가 사용된 적이 없는 경우.
- IAM에서 2015년 4월 22일에 이 정보의 추적을 시작하기 전에 액세스 키가 마지막으로 사용된 경우.
- 마지막으로 사용한 서비스가 리전 전용이 아닌 경우(예: Amazon S3).

access_key_1_last_used_service

액세스 키로 가장 최근에 액세스한 AWS 제품입니다. 이 필드의 값은 서비스의 네임스페이스를 사용합니다. 예를 들어 —Amazon S3의 경우 `s3`, Amazon EC2의 경우 `ec2`입니다. 액세스 키가 15분 내에 두 번 이상 사용된 경우, 첫 번째 사용만 이 필드에 기록됩니다.

다음과 같은 경우 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

- 사용자에게 액세스 키가 없는 경우.
- 액세스 키가 사용된 적이 없는 경우.
- IAM에서 2015년 4월 22일에 이 정보의 추적을 시작하기 전에 액세스 키가 마지막으로 사용된 경우.

access_key_2_active

사용자에게 두 번째 액세스 키가 있고 두 번째 키의 상태가 `Active`이면, 이 값은 `TRUE`입니다. 그렇지 않은 경우 이 값은 `FALSE`입니다.

Note

사용자는 교체하기 쉽도록 최대 두 개의 액세스 키를 보유할 수 있습니다. 액세스 키 교체에 대한 자세한 내용은 액세스 키 교체 (p. 115) 단원을 참조하십시오.

access_key_2_last_rotated

사용자의 두 번째 액세스 키가 생성되었거나 마지막으로 변경된 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다. 사용자에게 활성 상태의 두 번째 액세스 키가 있는 경우, 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

access_key_2_last_used_date

AWS API 요청에 서명하는 데 사용자의 두 번째 액세스 키가 마지막으로 사용된 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다. 액세스 키가 15분 내에 두 번 이상 사용된 경우, 첫 번째 사용만 이 필드에 기록됩니다.

다음과 같은 경우 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

- 사용자에게 두 번째 액세스 키가 없는 경우.
- 사용자의 두 번째 액세스 키가 사용된 적이 없는 경우.
- IAM에서 2015년 4월 22일에 이 정보의 추적을 시작하기 전에 사용자의 두 번째 액세스 키가 마지막으로 사용된 경우.

access_key_2_last_used_region

사용자의 두 번째 액세스 키가 마지막으로 사용된 AWS 리전입니다. 액세스 키가 15분 내에 두 번 이상 사용된 경우, 첫 번째 사용만 이 필드에 기록됩니다. 다음과 같은 경우 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

- 사용자에게 두 번째 액세스 키가 없는 경우.
- 사용자의 두 번째 액세스 키가 사용된 적이 없는 경우.
- IAM에서 2015년 4월 22일에 이 정보의 추적을 시작하기 전에 사용자의 두 번째 액세스 키가 마지막으로 사용된 경우.
- 마지막으로 사용한 서비스가 리전 전용이 아닌 경우(예: Amazon S3).

access_key_2_last_used_service

사용자의 두 번째 액세스 키로 가장 최근에 액세스한 AWS 서비스입니다. 이 필드의 값은 서비스의 네임스페이스를 사용합니다. 예를 들어 Amazon S3의 경우 `s3`, Amazon EC2의 경우 `ec2`입니다. 액세스 키가 15분 내에 두 번 이상 사용된 경우, 첫 번째 사용만 이 필드에 기록됩니다. 다음과 같은 경우 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

- 사용자에게 두 번째 액세스 키가 없는 경우.
- 사용자의 두 번째 액세스 키가 사용된 적이 없는 경우.
- IAM에서 2015년 4월 22일에 이 정보의 추적을 시작하기 전에 사용자의 두 번째 액세스 키가 마지막으로 사용된 경우.

cert_1_active

사용자에게 X.509 서명 인증서가 있고 해당 인증서의 상태가 `Active`인 경우, 이 값은 `TRUE`입니다. 그렇지 않은 경우 이 값은 `FALSE`입니다.

cert_1_last_rotated

사용자의 서명 인증서가 생성되었거나 마지막으로 변경된 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다. 사용자에게 활성 상태의 서명 인증서가 있는 경우, 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

cert_2_active

사용자에게 두 번째 X.509 서명 인증서가 있고 해당 인증서의 상태가 `Active`인 경우, 이 값은 `TRUE`입니다. 그렇지 않은 경우 이 값은 `FALSE`입니다.

Note

사용자는 인증서 교체가 쉽도록 최대 두 개의 X.509 서명 인증서를 보유할 수 있습니다.

cert_2_last_rotated

사용자의 두 번째 서명 인증서가 생성되었거나 마지막으로 변경된 날짜 및 시간(ISO 8601 날짜-시간 형식)입니다. 사용자에게 활성 상태의 두 번째 서명 인증서가 있는 경우, 이 필드의 값은 `N/A`(해당 사항 없음)입니다.

자격 증명 보고서 가져오기(콘솔)

AWS Management 콘솔을 사용하여 자격 증명 보고서를 CSV(쉼표로 구분된 값) 파일로 다운로드할 수 있습니다.

자격 증명 보고서를 다운로드하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 자격 증명 보고서를 선택합니다.
3. 보고서 다운로드를 선택합니다.

자격 증명 보고서 가져오기(AWS CLI)

다음 명령을 실행합니다:

- 자격 증명 보고서를 생성하려면: `aws iam generate-credential-report`
- 자격 증명 보고서를 가져오려면: `aws iam get-credential-report`

자격 증명 보고서 가져오기(AWS API)

다음 연산을 호출합니다.

- 자격 증명 보고서를 생성하려면: `GenerateCredentialReport`
- 자격 증명 보고서를 가져오려면: `GetCredentialReport`

IAM과 CodeCommit를 함께 사용: Git 자격 증명, SSH 키 및 AWS 액세스 키

CodeCommit는 AWS 클라우드에서 프라이빗 Git 리포지토리를 호스팅하는 관리형 버전 관리 서비스입니다. CodeCommit을 사용하려면 CodeCommit 리포지토리와 통신하도록 Git 클라이언트를 구성합니다. 이 구성의 일환으로 CodeCommit에서 사용자 인증에 사용할 수 있는 IAM 자격 증명을 제공합니다. IAM에서는 세 가지 유형의 자격 증명으로 CodeCommit를 지원합니다.

- Git 자격 증명: HTTPS를 통해 CodeCommit 리포지토리와 통신하는 데 사용할 수 있는 IAM; 생성 사용자 이름 및 암호 페어입니다.
- SSH 키: SSH를 통해 CodeCommit 리포지토리와 통신하기 위해 IAM 사용자와 연결할 수 있는 로컬로 생성된 퍼블릭-프라이빗 키 페어입니다.
- AWS 액세스 키 (p. 111): HTTPS를 통해 CodeCommit 리포지토리와 통신하기 위해 AWS CLI에 포함된 자격 증명 헬퍼와 함께 사용할 수 있습니다.

각 옵션에 대한 자세한 내용은 다음 단원을 참조하십시오.

CodeCommit에 Git 자격 증명 및 HTTPS 사용(권장)

Git 자격 증명을 사용하여 IAM 사용자에 대한 정적 사용자 이름 및 암호 페어를 생성한 다음 HTTPS 연결에 이러한 자격 증명을 사용합니다. 정적 Git 자격 증명을 지원하는 타사 도구 또는 IDE(통합 개발 환경)에서도 이러한 자격 증명을 사용할 수 있습니다.

이러한 자격 증명은 모든 지원되는 운영 체제에 공통적이고 대부분의 자격 증명 관리 시스템, 개발 환경 및 기타 소프트웨어 개발 도구와 호환되므로 이는 권장되는 방법입니다. 언제든지 Git 자격 증명에 대한 암호를 재설정할 수 있습니다. 또한 자격 증명이 더 이상 필요하지 않은 경우 자격 증명을 비활성화하거나 삭제할 수 있습니다.

> Note
>
> Git 자격 증명에 대해 본인의 사용자 이름 또는 암호를 선택할 수 없습니다. IAM에서는 사용자가 AWS에 대한 보안 표준을 준수하고 CodeCommit에서 리포지토리를 보호하도록 돕기 위해 이러한 자격 증명을 생성합니다. 자격 증명은 생성될 때 한 번만 다운로드할 수 있습니다. 따라서 자격 증명을 안전한 장소에 보관하십시오. 필요한 경우 언제든지 암호를 재설정할 수 있지만, 그러면 이전 암호를 사용하여 구성된 연결은 무효화됩니다. 새 암호를 사용하여 연결하려면 연결을 다시 구성해야 합니다.

자세한 내용은 다음 주제 단원을 참조하십시오.

- IAM 사용자를 만들려면 AWS 계정의 IAM 사용자 생성 (p. 87) 단원을 참조하십시오.
- CodeCommit에서 Git 자격 증명을 생성하여 사용하려면 AWS CodeCommit 사용 설명서의 Git 자격 증명을 사용하는 HTTPS 사용자의 경우 단원을 참조하십시오.

> Note
>
> Git 자격 증명을 생성한 이후에 IAM 사용자의 이름을 변경할 경우 Git 자격 증명의 사용자 이름은 변경되지 않습니다. 사용자 이름과 암호는 동일하게 유지되고 계속 유효합니다.

서비스별 자격 증명을 회전하려면

1. 현재 사용 중인 서비스별 자격 증명 세트 이외에 두 번째 세트를 만듭니다.
2. 새 자격 증명 세트를 사용하도록 모든 애플리케이션을 업데이트하고 애플리케이션이 작동하는지 확인합니다.
3. 원래 자격 증명의 상태를 "Inactive"로 변경합니다.
4. 모든 애플리케이션이 계속 작동하는지 확인합니다.
5. 비활성 서버별 자격 증명을 삭제합니다.

CodeCommit에 SSH 키 및 SSH 사용

SSH 연결을 사용하여 Git 및 CodeCommit에서 SSH 인증에 사용하는 퍼블릭 및 프라이빗 키 파일을 로컬 시스템에서 만듭니다. 퍼블릭 키를 IAM 사용자와 연결하고 프라이빗 키를 로컬 시스템에 저장합니다. 자세한 내용은 다음 주제 단원을 참조하십시오.

- IAM 사용자를 만들려면 AWS 계정의 IAM 사용자 생성 (p. 87) 단원을 참조하십시오.
- SSH 퍼블릭 키를 만들어 IAM 사용자와 연결하려면 AWS CodeCommit 사용 설명서의 Linux, macOS, or Unix에서 SSH 연결 또는 Windows에서 SSH 연결 단원을 참조하십시오.

> Note
>
> 퍼블릭 키는 ssh-rsa 형식 또는 PEM 형식으로 인코딩해야 합니다. 퍼블릭 키의 최소 비트 길이는 2048비트이고 최대 길이는 16384비트입니다. 이것은 업로드하는 파일의 크기와는 별개입니다. 예

를 들어 2048비트 키를 생성할 수 있으며 결과 PEM 파일의 길이는 1679바이트입니다. 퍼블릭 키를 다른 형식 또는 크기로 제공하면 키 형식이 잘못되었다는 오류 메시지가 표시됩니다.

AWS CLI 자격 증명 헬퍼 및 CodeCommit에 HTTPS 사용

Git 자격 증명을 사용한 HTTPS 연결의 대안으로, Git에서 CodeCommit 리포지토리와 상호 작용하기 위해 AWS에 인증해야 할 때마다 암호화 방식으로 서명된 IAM 사용자 자격 증명 또는 Amazon EC2 인스턴스 역할을 사용하도록 허용할 수 있습니다. 이는 IAM 사용자가 필요하지 않은 CodeCommit 리포지토리에 연결하는 유일한 방법입니다. 또한 연동된 액세스 및 임시 자격 증명으로 작동되는 유일한 방법입니다. 비즈니스에 연동된 액세스 또는 임시 자격 증명을 반드시 사용해야 하는 경우를 제외하고 IAM 사용자를 만들어 액세스에 사용하는 것이 좋습니다. 자세한 내용은 다음 주제 단원을 참조하십시오.

- 연동된 액세스에 대한 자세한 내용은 자격 증명 공급자 및 연동 (p. 183) 및 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동) (p. 181) 단원을 참조하십시오.
- 임시 자격 증명에 대한 자세한 내용은 임시 보안 자격 증명 (p. 302) 및 CodeCommit 리포지토리에 대한 임시 액세스 단원을 참조하십시오.

AWS CLI Credential Helper는 Keychain Access, Windows Credential Management 등과 같은 다른 자격 증명 헬퍼 시스템과 호환되지 않습니다. HTTPS를 통한 자격 증명 헬퍼 연결을 구성할 때 고려해야 할 추가 사항이 있습니다. 자세한 내용은 AWS CodeCommit 사용 설명서의 Linux, macOS, or Unix 자격 증명 헬퍼를 사용하여 AWS CLI에서 HTTPS 연결 또는 AWS CLI 자격 증명 헬퍼를 사용하여 Windows에서 HTTPS 연결 단원을 참조하십시오.

Amazon Managed Apache Cassandra Service와 함께 IAM 사용

Amazon Managed Apache Cassandra Service는 확장 가능하고 가용성이 뛰어난 관리형 Apache Cassandra 호환 데이터베이스 서비스입니다. AWS Management 콘솔를 사용하거나, `cqlsh` 클라이언트를 실행하거나 , Apache 2.0 라이선스를 획득한 Cassandra 드라이버를 사용하여 MCS에 액세스할 수 있습니다.

> Note
>
> 콘솔을 통해서만 MCS와 상호 작용하려는 경우에는 서비스별 자격 증명을 생성할 필요가 없습니다. 자세한 내용은 Amazon Managed Apache Cassandra Service 개발자 안내서의 콘솔을 사용한 Amazon Managed Apache Cassandra Service 액세스를 참조하십시오.

사용자가 `cqlsh` 또는 Apache 2.0 라이선스를 획득한 Cassandra 드라이버를 사용하여 MCS에 액세스할 수 있도록 하려면 서비스별 자격 증명을 생성해야 합니다. 서비스별 자격 증명에서는 IAM 사용자가 하나의 AWS 서비스와 상호 작용할 수 있지만 다른 서비스와는 상호 작용할 수 없습니다.

MCS에 액세스하는 데 필요한 권한에 대한 자세한 내용은 Amazon Managed Apache Cassandra Service 개발자 안내서의 서비스별 자격 증명 생성을 참조하십시오.

MCS 자격 증명 생성(콘솔)

AWS Management 콘솔를 사용하여 IAM 사용자에 대한 Amazon Managed Apache Cassandra Service(MCS) 자격 증명을 생성할 수 있습니다.

MCS 서비스별 자격 증명을 생성하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택한 다음 자격 증명이 필요한 사용자의 이름을 선택합니다.

3. Credentials for Amazon Managed Apache Cassandra Service (MCS)(Amazon Managed Apache Cassandra Service(MCS)를 위한 자격 증명) 아래의 Security Credentials(보안 자격 증명) 탭에서 Generate credentials(자격 증명 생성)를 선택합니다.
4. 이제 서비스별 자격 증명을 사용할 수 있습니다. 이 때가 암호를 보거나 다운로드 할 수 있는 유일한 시간입니다. 나중에 복구할 수 없습니다. 그러나 언제든지 암호를 재설정할 수 있습니다. 나중에 필요하므로 사용자와 암호를 안전한 위치에 저장하십시오.

MCS 자격 증명 생성(AWS CLI)

AWS CLI를 사용하여 IAM 사용자에 대한 Amazon Managed Apache Cassandra Service(MCS) 자격 증명을 생성할 수 있습니다.

MCS 서비스별 자격 증명을 생성하려면(AWS CLI)

- 다음 명령을 사용합니다.
  - aws iam create-service-specific-credential

MCS 자격 증명 생성(AWS API)

AWS API를 사용하여 IAM 사용자에 대한 Amazon Managed Apache Cassandra Service(MCS) 자격 증명을 생성할 수 있습니다.

MCS 서비스별 자격 증명을 생성하려면(AWS API)

- 다음 작업을 완료합니다.
  - CreateServiceSpecificCredential

서버 인증서 작업

AWS에서 웹 사이트나 애플리케이션에 대한 HTTPS 연결을 활성화하려면 SSL/TLS 서버 인증서가 필요합니다. AWS Certificate Manager(ACM)에서 지원되는 리전에서 사용되는 인증서의 경우, ACM을 사용하여 서버 인증서를 프로비저닝, 관리 및 배포하는 것이 좋습니다. 지원되지 않는 리전에서는 IAM을 인증서 관리자로 사용해야 합니다. ACM에서 지원하는 리전을 알아보려면 AWS General Reference의 AWS Certificate Manager Certificate Manager 리전 및 엔드포인트를 참조하십시오.

ACM은 서버 인증서를 프로비저닝 및 관리하고 배포하는 데 선호하는 도구입니다. ACM을 사용하면 인증서를 요청하거나 기존 ACM 또는 외부 인증서를 AWS 리소스에 배포할 수 있습니다. ACM이 제공하는 인증서는 무료이고 자동으로 갱신됩니다. 지원되는 리전에서는 ACM을 사용하여 콘솔에서 또는 프로그래밍 방식으로 서버 인증서를 관리할 수 있습니다. ACM 사용에 대한 자세한 정보는 AWS Certificate Manager 사용 설명서를 참조하십시오. ACM 인증서 요청에 대한 자세한 정보는 AWS Certificate Manager 사용 설명서의 퍼블릭 인증서 요청 또는 프라이빗 인증서 요청 단원을 참조하십시오. 타사 인증서를 ACM으로 가져오는 작업에 대한 자세한 정보는 AWS Certificate Manager 사용 설명서의 인증서 가져오기 단원을 참조하십시오.

ACM에서 지원되지 않는 리전에서 HTTPS 연결을 지원해야 하는 경우에만 IAM을 인증서 관리자로 사용합니다. IAM은 프라이빗 키를 안전하게 암호화하고 암호화된 버전을 IAM SSL 인증서 스토리지에 저장합니다. IAM은 모든 리전에서 서버 인증서 배포를 지원하지만 외부 공급자로부터 AWS에서 사용할 인증서를 얻어야 합니다. ACM 인증서는 IAM에 업로드할 수 없습니다. 또한 인증서는 IAM 콘솔에서 관리할 수 없습니다.

타사 인증서를 IAM에 업로드하는 방법에 대한 자세한 정보는 다음 주제를 참조하십시오.

주제

서버 인증서 업로드(AWS API)

IAM에 서버 인증서를 업로드하려면 인증서와 함께 그에 딸린 프라이빗 키를 제공해야 합니다. 인증서에 자체 서명이 되어 있지 않은 경우, 인증서 체인도 제공해야 합니다. (자체 서명된 인증서를 업로드하는 경우에는 인증서 체인이 필요하지 않습니다). 인증서를 업로드하기 전에 이 모든 항목이 있는지, 있다면 각 항목이 다음 기준을 충족하는지 확인하십시오.

- 인증서는 업로드 시점에 유효해야 합니다. 유효 기간이 시작되기 전(인증서의 `NotBefore` 날짜) 또는 만료된 후(인증서의 `NotAfter` 날짜)에는 인증서를 업로드할 수 없습니다.
- 프라이빗 키는 암호화되지 않은 것이어야 합니다. 패스워드나 패스프레이즈로 보호된 프라이빗 키는 업로드할 수 없습니다. 암호화된 프라이빗 키의 해독에 대한 도움말은 문제 해결 (p. 166) 단원을 참조하십시오.
- 인증서, 프라이빗 키 및 인증서 체인은 모두 PEM 인코딩되어야 합니다. 이 항목들을 PEM 형식으로 변환하는 작업에 대한 도움말은 문제 해결 (p. 166) 단원을 참조하십시오.

IAM API를 사용하여 인증서를 업로드하려면 UploadServerCertificate 요청을 전송하십시오. 다음 예에서는 AWS Command Line Interface(AWS CLI)에서 이 작업을 수행하는 방법을 보여줍니다. 이 예시에서는 다음과 같이 가정합니다.

- PEM 인코딩된 인증서가 `Certificate.pem`이라는 파일에 저장되어 있다.
- PEM 인코딩된 인증서 체인이 `CertificateChain.pem`이라는 파일에 저장되어 있다.
- PEM 인코딩된 비암호화 프라이빗 키가 `PrivateKey.pem`이라는 파일에 저장되어 있다.

다음 예시 명령을 사용하려면 이 파일들의 이름을 바꾸고 *`ExampleCertificate`*을 업로드된 인증서의 이름으로 대체해야 합니다. 하나의 연속선에 명령을 입력합니다. 다음 예시에는 가독성을 높여주는 줄바꿈과 추가 공백이 포함되어 있습니다.

```
$ aws iam upload-server-certificate --server-certificate-name ExampleCertificate
                                    --certificate-body file://Certificate.pem
                                    --certificate-chain file://CertificateChain.pem
                                    --private-key file://PrivateKey.pem
```

선행 명령은 성공적으로 실행되는 경우 Amazon Resource Name(ARN) (p. 564), 표시 이름, 식별자(ID), 만료 날짜 등 업로드된 인증서에 대한 메타데이터를 반환합니다.

> **Note**
>
> Amazon CloudFront에서 사용할 서버 인증서를 업로드하는 경우, `--path` 옵션을 사용하여 경로를 지정해야 합니다. 경로는 `/cloudfront`로 시작해야 하고 후행 슬래시를 포함해야 합니다(예: `/cloudfront/test/`).

Windows PowerShell용 AWS 도구를 사용하여 인증서를 업로드하려면 Publish-IAMServerCertificate를 사용하십시오.

서버 인증서 가져오기(AWS API)

IAM API를 사용하여 인증서를 조회하려면 GetServerCertificate 요청을 전송하십시오. 다음 예에서는 AWS CLI에서 이 작업을 수행하는 방법을 보여줍니다. *`ExampleCertificate`*을 조회할 인증서의 이름으로 대체합니다.

```
$ aws iam get-server-certificate --server-certificate-name ExampleCertificate
```

선행 명령은 성공적으로 실행되는 경우 인증서, 인증서 체인(업로드된 경우) 및 인증서 관련 메타데이터를 반환합니다.

Note

업로드 후에는 IAM에서 프라이빗 키를 다운로드하거나 조회할 수 없습니다.

Windows PowerShell용 AWS 도구을(를) 사용하여 인증서를 조회하려면 Get-IAMServerCertificate을 사용하십시오.

서버 인증서 목록 조회(AWS API)

IAM API를 사용하여 업로드한 서버 인증서의 목록을 조회하려면 ListServerCertificates 요청을 전송하십시오. 다음 예에서는 AWS CLI에서 이 작업을 수행하는 방법을 보여줍니다.

```
$ aws iam list-server-certificates
```

선행 명령은 성공적으로 실행되는 경우 각 인증서 관련 메타데이터가 담긴 목록을 반환합니다.

Windows PowerShell용 AWS 도구를 사용하여 업로드한 서버 인증서의 목록을 조회하려면 Get-IAMServerCertificates를 사용하십시오.

서비스 인증서 이름 변경 또는 경로 업데이트(AWS API)

IAM API를 사용하여 서버 인증서의 이름을 변경하거나 경로를 업데이트하려면 UpdateServerCertificate 요청을 전송하십시오. 다음 예에서는 AWS CLI에서 이 작업을 수행하는 방법을 보여줍니다.

다음 예시 명령을 사용하려면 기존 및 신규 인증서의 이름과 인증서 경로를 바꾸고 명령을 하나의 연속선에 입력해야 합니다. 다음 예시에는 가독성을 높여주는 줄바꿈과 추가 공백이 포함되어 있습니다.

```
$ aws iam update-server-certificate --server-certificate-name ExampleCertificate
                                    --new-server-certificate-name CloudFrontCertificate
                                    --new-path /cloudfront/
```

선행 명령은 성공적으로 실행되는 경우 메타데이터를 반환하지 않습니다.

Windows PowerShell용 AWS 도구을(를) 사용하여 서버 인증서의 이름을 변경하거나 경로를 업데이트하려면 Update-IAMServerCertificate을 사용하십시오.

서버 인증서 삭제(AWS API)

IAM API를 사용하여 서버 인증서를 삭제하려면 DeleteServerCertificate 요청을 전송하십시오. 다음 예에서는 AWS CLI에서 이 작업을 수행하는 방법을 보여줍니다.

다음 예시 명령을 사용하려면 *ExampleCertificate*을 삭제할 인증서의 이름으로 대체해야 합니다.

```
$ aws iam delete-server-certificate --server-certificate-name ExampleCertificate
```

선행 명령은 성공적으로 실행되는 경우 메타데이터를 반환하지 않습니다.

Windows PowerShell용 AWS 도구을 사용하여 서버 인증서를 삭제하려면 Remove-IAMServerCertificate을 사용하십시오.

문제 해결

IAM에 인증서를 업로드하려면 인증서, 프라이빗 키 및 인증서 체인이 모두 PEM 인코딩되어 있어야 합니다. 또한 프라이빗 키가 암호화되지 않은 것이어야 합니다. 다음 예시를 참조하십시오.

Example PEM 인코딩된 인증서

```
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

Example PEM 인코딩된 비암호화 프라이빗 키

```
-----BEGIN RSA PRIVATE KEY-----
Base64-encoded private key
-----END RSA PRIVATE KEY-----
```

Example PEM 인코딩된 인증서 체인

인증서 체인에는 한 개 이상의 인증서가 포함되어 있습니다. 텍스트 편집기, Windows의 copy 명령 또는 Linux의 cat 명령을 사용하여 여러 인증서 파일을 하나의 체인으로 연결할 수 있습니다. 여러 개의 인증서를 포함하는 경우 각 인증서가 앞에 지정된 인증서를 인증해야 합니다. 루트 CA 인증서를 포함하여 인증서를 연결함으로써 이를 달성합니다.

다음 예시의 경우에는 세 개의 인증서가 포함되어 있지만, 사용자에 따라 인증서 체인에 포함된 인증서가 그보다 많거나 적을 수 있습니다.

```
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

이 항목들이 IAM에 업로드하기에 적합한 형식이 아닌 경우, OpenSSL을 사용하여 적합한 형식으로 변환할 수 있습니다.

인증서 또는 인증서 체인을 DER에서 PEM으로 변환하려면

다음 예시와 같이 OpenSSL x509 명령을 사용합니다. 다음 예시 명령에서 *Certificate.der*을 DER 인코딩된 인증서가 포함된 파일의 이름으로 대체합니다. *Certificate.pem*을, PEM 인코딩된 인증서를 포함할 출력 파일에 지정하려는 이름으로 바꿉니다.

```
$ openssl x509 -inform DER -in Certificate.der -outform PEM -out Certificate.pem
```

프라이빗 키를 DER에서 PEM으로 변환하려면

다음 예시와 같이 OpenSSL rsa 명령을 사용합니다. 다음 예시 명령에서 *PrivateKey.der*을 DER 인코딩된 프라이빗 키가 포함된 파일의 이름으로 대체해야 합니다. *PrivateKey.pem*을, PEM 인코딩된 프라이빗 키를 포함할 출력 파일에 지정하려는 이름으로 바꿉니다.

```
$ openssl rsa -inform DER -in PrivateKey.der -outform PEM -out PrivateKey.pem
```

암호화된 프라이빗 키를 해독하려면(패스워드나 패스프레이즈 제거)

다음 예시와 같이 OpenSSL rsa 명령을 사용합니다. 다음 예시 명령을 사용하려면 *EncryptedPrivateKey.pem*을 암호화된 프라이빗 키가 포함된 파일의 이름으로 대체해야 합니다. *PrivateKey.pem*을, PEM 인코딩된 비암호화 프라이빗 키를 포함할 출력 파일에 지정하려는 이름으로 바꿉니다.

```
$ openssl rsa -in EncryptedPrivateKey.pem -out PrivateKey.pem
```

인증서 번들을 PKCS#12(PFX)에서 PEM으로 변환하려면

다음 예시와 같이 OpenSSL pkcs12 명령을 사용합니다. 다음 예시 명령에서 *CertificateBundle.p12*를 PKCS#12 인코딩된 인증서 번들이 포함된 파일의 이름으로 대체합니다. *CertificateBundle.pem*을, PEM 인코딩된 인증서 번들을 포함할 출력 파일에 지정하려는 이름으로 대체합니다.

```
$ openssl pkcs12 -in CertificateBundle.p12 -out CertificateBundle.pem -nodes
```

인증서 번들을 PKCS#7에서 PEM으로 변환하려면

다음 예시와 같이 OpenSSL pkcs7 명령을 사용합니다. 다음 예시 명령에서 *CertificateBundle.p7b*를 PKCS#7 인코딩된 인증서 번들이 포함된 파일의 이름으로 대체합니다. *CertificateBundle.pem*을, PEM 인코딩된 인증서 번들을 포함할 출력 파일에 지정하려는 이름으로 대체합니다.

```
$ openssl pkcs7 -in CertificateBundle.p7b -print_certs -out CertificateBundle.pem
```

IAM 그룹

IAM 그룹 (p. 167)은 IAM 사용자들의 집합입니다. 그룹을 활용하면 다수의 사용자들에 대한 권한을 지정함으로써 해당 사용자들에 대한 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 Admins라는 그룹을 만들어 일반적으로 관리자에게 필요한 유형의 권한을 부여할 수 있습니다. 이 그룹에 할당된 권한이 이 그룹에 속하는 모든 사용자에게 자동으로 부여됩니다. 관리자 권한을 필요로 하는 새로운 사용자가 조직에 들어올 경우 해당 사용자를 이 그룹에 추가하여 적절한 권한을 할당할 수 있습니다. 마찬가지로 조직에서 직원의 업무가 바뀌면 해당 사용자의 권한을 편집하는 대신 이전 그룹에서 해당 사용자를 제거한 후 적절한 새 그룹에 추가하면 됩니다.

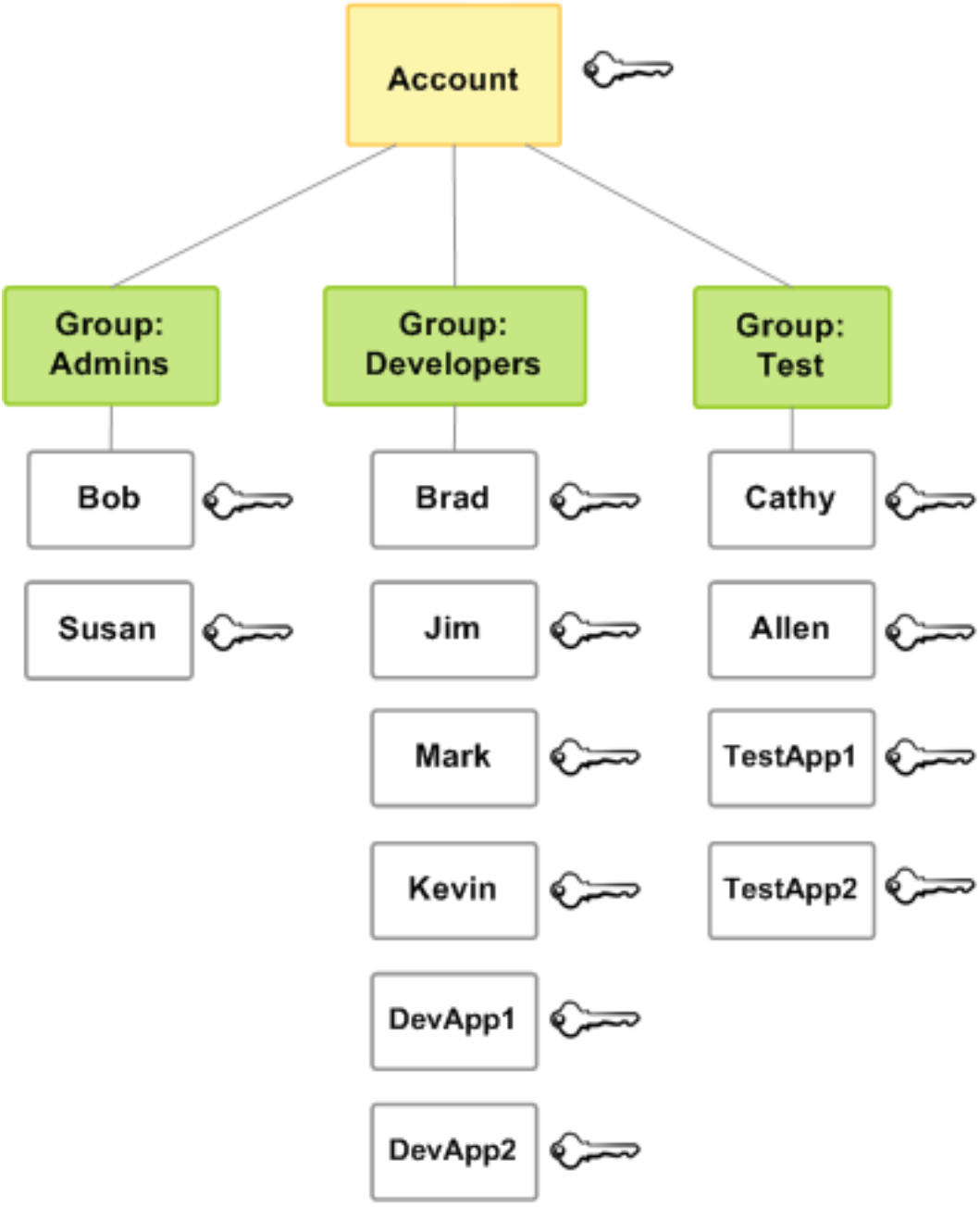
그룹은 권한 정책에서 `Principal`로 식별될 수 없기 때문에 IAM에서는 진정한 '자격 증명'이 아니라는 점에 유의하십시오. 그것은 다수의 사용자들에게 한 번에 정책을 연결하는 방법일 뿐입니다.

다음은 그룹이 갖는 몇 가지 중요한 특징입니다.

- 한 그룹에 여러 사용자가 포함될 수 있으며 한 사용자가 다중 그룹에 속할 수 있습니다.
- 그룹은 중첩될 수 없습니다. 즉, 그룹은 사용자만 포함할 수 있으며 다른 그룹은 포함할 수 없습니다.
- AWS 계정의 모든 사용자를 자동으로 포함하는 기본 그룹은 없습니다. 이러한 그룹이 필요한 경우 하나 만들어 새로운 사용자를 각각 해당 그룹에 할당해야 합니다.
- 보유할 수 있는 그룹의 수와 사용자가 속할 수 있는 그룹의 수에는 제한이 있습니다. 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

다음 다이어그램에서는 어느 작은 회사의 간단한 예제를 보여줍니다. 회사 소유주는 `Admins` 그룹을 생성해 회사가 성장함에 따라 사용자들이 다른 사용자들을 생성하고 관리하도록 합니다. `Admins` 그룹은 `Developers` 그룹과 `Test` 그룹을 생성합니다. 이러한 각 그룹은 AWS와 상호 작용하는 사용자(사람 및 애

플리케이션: Jim, Brad, DevApp1 등)들로 구성됩니다. 사용자마다 개별적인 보안 자격 증명 세트가 있습니다. 이 예제에서는 각 사용자가 단일 그룹에 속합니다. 하지만 사용자는 다중 그룹에 속할 수 있습니다.



IAM 그룹 생성

그룹을 설정하려면 그룹을 생성해야 합니다. 그런 다음 그룹 내 사용자가 할 수 있는 작업 유형에 따라 권한을 부여해야 합니다. 마지막으로 그룹에 사용자를 추가합니다.

그룹을 만들기 위해 필요한 권한에 대한 자세한 내용은 IAM 리소스에 액세스하는 데 필요한 권한 (p. 507) 단원을 참조하십시오.

IAM 그룹을 만들어 정책을 연결하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 그룹을 클릭한 다음 Create New Group(새 그룹 생성)을 클릭합니다.
3. 그룹 이름 상자에 그룹 이름을 입력한 다음 다음 단계를 클릭합니다.

   Note

   그룹 이름에는 최대 64개의 문자, 숫자 및 더하기(+), 등호(=), 쉼표(,), 마침표(.), 앳(@), 밑줄(_) 및 하이픈(-) 조합을 사용할 수 있습니다. 이름은 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어 이름이 **ADMINS** 및 **admins**, 두 가지로 지정된 그룹을 만들 수는 없습니다. IAM 엔터티 관련 제한에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.
4. 정책 목록에서 그룹 멤버 전체에 적용하고자 하는 정책 이름마다 확인란을 선택합니다. 그런 다음 다음 단계를 클릭합니다.
5. [Create Group]을 클릭합니다.

`Administrators` 그룹을 설정하는 방법의 예는 첫 번째 IAM 관리자 및 그룹 생성 (p. 20)을 참조하십시오.

IAM 그룹(AWS CLI 또는 AWS API)을 생성하려면

다음 중 하나를 사용하십시오.

- AWS CLI: aws iam create-group
- AWS API: CreateGroup

IAM 그룹 관리

Amazon Web Services는 IAM 그룹 관리를 위한 다양한 도구를 제공합니다. 그룹에서 사용자를 추가 및 제거하는 데 필요한 권한에 대한 자세한 내용은 IAM 리소스에 액세스하는 데 필요한 권한 (p. 507)을 참조하십시오.

주제

- IAM 그룹 표시 (p. 169)
- IAM 그룹에서 사용자 추가 및 제거 (p. 170)
- IAM 그룹에 정책 연결 (p. 171)
- IAM 그룹 이름 바꾸기 (p. 172)
- IAM 그룹 삭제 (p. 172)

IAM 그룹 표시

계정의 모든 그룹, 그룹에 속한 사용자 및 한 사용자가 속한 그룹의 목록을 조회할 수 있습니다. AWS CLI 또는 AWS API를 사용하는 경우 특정 경로 접두사를 사용해 전체 그룹의 목록을 조회할 수 있습니다.

계정에 속한 모든 그룹을 표시하는 방법

다음을 수행하십시오.

- AWS Management 콘솔: 탐색 창에서 그룹을 선택합니다.
- AWS CLI: aws iam list-groups

- AWS API: ListGroups

특정 그룹에 속한 사용자를 표시하려면

다음을 수행하십시오.

- AWS Management 콘솔: 탐색 창에서 그룹을 선택하고, 그룹 이름을 선택한 후 사용자 탭을 선택합니다.
- AWS CLI: aws iam get-group
- AWS API: GetGroup

사용자가 속한 모든 그룹을 표시하려면

다음을 수행하십시오.

- AWS Management 콘솔: 탐색 창에서 사용자를 선택하고, 사용자 이름을 선택한 후 그룹 탭을 선택합니다.
- AWS CLI: aws iam list-groups-for-user
- AWS API: ListGroupsForUser

IAM 그룹에서 사용자 추가 및 제거

그룹을 사용하여 한 번에 여러 사용자에게 동일한 권한 정책을 적용합니다. 그런 다음 IAM 그룹에서 사용자를 추가하거나 제거할 수 있습니다. 이 기능은 사람들이 조직에 들어오거나 조직을 떠날 때 유용합니다.

정책 액세스 보기

정책에 대한 권한을 변경하기 전에 최근 서비스 수준 활동을 검토해야 합니다. 이 기능은 사용 중인 보안 주체(사람 또는 애플리케이션)의 액세스 권한을 제거하지 않으려는 경우 중요합니다. 서비스에서 마지막으로 액세스한 데이터 보기에 대한 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

그룹에서 사용자 추가 또는 제거(콘솔)

AWS Management 콘솔을 사용하여 그룹에서 사용자를 추가 또는 제거할 수 있습니다.

IAM 그룹에 사용자를 추가하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 그룹을 선택한 다음 그룹 이름을 선택합니다.
3. [Users] 탭을 선택한 후 [Add Users to Group]를 선택합니다. 추가할 사용자 옆에 있는 확인란을 선택합니다.
4. 사용자 추가를 선택합니다.

IAM 그룹에서 사용자를 제거하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 그룹을 선택한 다음 그룹 이름을 선택합니다.
3. 사용자 탭을 선택한 후 Remove Users from Group(그룹에서 사용자 제거)를 선택합니다. 제거할 사용자 옆에 있는 확인란을 선택합니다.

4. 사용자 제거를 선택합니다.

그룹에서 사용자 추가 또는 제거(AWS CLI)

AWS CLI을 사용하여 그룹에서 사용자를 추가 또는 제거할 수 있습니다.

IAM 그룹에 사용자를 추가하려면(AWS CLI)

- 다음 명령을 사용합니다.
  - aws iam add-user-to-group

IAM 그룹에서 사용자를 제거하려면(AWS CLI)

- 다음 명령을 사용합니다.
  - aws iam remove-user-from-group

그룹에서 사용자 추가 또는 제거(AWS API)

AWS API를 사용하여 그룹에서 사용자를 추가 또는 제거할 수 있습니다.

IAM 그룹에 사용자를 추가하려면(AWS API)

- 다음 작업을 완료합니다.
  - AddUserToGroup

IAM 그룹에서 사용자를 제거하려면(AWS API)

- 다음 작업을 완료합니다.
  - RemoveUserFromGroup

IAM 그룹에 정책 연결

다음 단계에 설명된 대로 그룹에 AWS 관리형 정책 (p. 357)—즉, AWS가 제공하는 미리 작성된 정책—을 연결할 수 있습니다. 고객 관리형 정책, 즉 생성하는 사용자 지정 권한이 있는 정책을 연결하려면 먼저 정책을 만들어야 합니다. 고객 관리형 정책 만들기에 대한 자세한 내용은 IAM 정책 만들기 (p. 435) 단원을 참조하십시오.

권한 및 정책에 대한 자세한 내용은 액세스 관리 (p. 348)을 참조하십시오.

그룹에 정책을 연결하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 연결할 정책 이름 옆의 확인란을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. Policy actions(정책 작업)와 연결을 차례로 클릭합니다.
5. 필터에서 모든 유형을 선택한 다음 그룹을 클릭합니다.

6. 정책을 연결할 그룹 이름 옆의 확인란을 선택한 다음 정책 연결을 클릭합니다.

그룹(AWS CLI 또는 AWS API)에 정책을 연결하려면

다음 중 하나를 수행하십시오.

- AWS CLI: aws iam attach-group-policy
- AWS API: AttachGroupPolicy

IAM 그룹 이름 바꾸기

그룹의 이름 또는 경로를 변경하면 진행됩니다.

- 그룹에 연결된 정책은 이름이 변경되어도 계속 유지됩니다.
- 그룹의 모든 사용자도 이름이 변경되어도 계속 유지됩니다.
- 그룹의 고유 ID는 변동 없이 유지됩니다. 고유 ID에 대한 자세한 내용은 고유 식별자 (p. 567) 단원을 참조하십시오.

IAM에서는 새 이름을 사용하기 위해 이러한 그룹을 리소스로 참조하는 정책을 자동으로 업데이트하지 않기 때문에 그룹의 이름을 바꿀 때 주의해야 합니다. 그룹의 이름을 바꾸기 전에 모든 정책을 수동으로 확인해 해당 그룹이 이름으로 언급된 모든 정책을 찾아야 합니다. Bob이라는 직원이 회사의 테스트 부서 관리자인 경우를 예로 들어 보겠습니다. Bob에게는 테스트 그룹의 사용자를 추가 및 제거할 수 있는 IAM 사용자에 연결된 정책이 있습니다. 관리자가 그룹의 이름을 변경하거나 그룹 경로를 변경하는 경우, 관리자는 Bob에게 연결된 정책도 업데이트하여 새 이름 또는 새 경로를 사용하도록 해야 합니다. 그렇지 않은 경우 Bob은 그룹에 사용자를 추가할 수도 그룹에서 사용자를 제거할 수도 없습니다.

그룹을 리소스로 참조하는 정책을 찾으려면:

1. IAM 콘솔의 탐색 창에서 정책을 선택합니다.
2. 정책 유형 드롭다운 목록에서 고객 관리형을 선택하여 사용자 지정 정책만 표시하도록 정책을 필터링합니다.
3. 각 정책 이름 옆에 있는 화살표를 선택해 정책 요약을 확장합니다.
4. 서비스 목록에 IAM이 있으면 선택합니다.
5. 리소스 열에서 그룹의 이름을 찾습니다.
6. 정책 편집을 선택하여 정책에서 그룹 이름을 변경합니다.

IAM 그룹의 이름을 변경하려면

다음을 수행하십시오.

- AWS Management 콘솔: 탐색 창에서 그룹을 선택한 후 그룹 이름 옆에 있는 확인란을 선택합니다. 페이지 상단의 그룹 작업 목록에서 그룹 이름 편집을 선택합니다. 새 그룹 이름을 입력한 후 예, 편집합니다를 선택합니다.
- AWS CLI: aws iam update-group
- AWS API: UpdateGroup

IAM 그룹 삭제

AWS Management 콘솔에서 그룹을 삭제하면 콘솔은 모든 그룹 구성원을 자동으로 제거하고 연결된 모든 관리형 정책을 분리하며, 모든 인라인 정책들을 삭제합니다. 그러나 IAM은 이러한 그룹을 리소스로 참조하

는 정책을 자동으로 삭제하지 않기 때문에 그룹을 삭제할 때 주의해야 합니다. 그룹을 삭제하기 전에 모든 정책을 수동으로 확인하여 해당 그룹이 이름으로 언급된 모든 정책을 찾아야 합니다. John이라는 직원이 회사의 테스트 부서 관리자인 경우를 예로 들어 보겠습니다. John에게는 테스트 그룹의 사용자를 추가 및 제거할 수 있는 IAM 사용자에 연결된 정책이 있습니다. 관리자는 그룹을 삭제할 경우 John에게 연결된 정책도 삭제해야 합니다.

그룹을 리소스로 참조하는 정책을 찾으려면

1. IAM 콘솔의 탐색 창에서 정책을 선택합니다.
2. 정책 유형 드롭다운 목록에서 고객 관리형을 선택하여 사용자 지정 정책만 표시하도록 정책을 필터링합니다.
3. 각 정책 이름 옆에 있는 화살표를 선택해 정책 요약을 확장합니다.
4. 서비스 목록에 IAM이 있으면 선택합니다.
5. 리소스 열에서 그룹의 이름을 찾습니다.
6. 정책 삭제를 선택하여 정책을 삭제합니다.

반면에, AWS CLI, Windows PowerShell용 도구 또는 AWS API를 사용하여 그룹을 삭제할 경우에는 먼저 그룹의 사용자를 제거해야 합니다. 그런 다음 이 그룹에 포함된 인라인 정책을 삭제합니다. 그런 다음 그룹에 연결된 관리형 정책을 모두 분리합니다. 이렇게 해야만 그룹을 삭제할 수 있습니다.

IAM 그룹 삭제(콘솔)

AWS Management 콘솔에서 IAM 그룹을 삭제할 수 있습니다.

IAM 그룹을 삭제하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 [Groups]를 선택합니다.
3. 그룹 목록에서 삭제할 그룹 이름 옆의 확인란을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. Group Actions(그룹 작업)을 클릭한 다음 그룹 삭제를 클릭합니다.
5. 확인 상자에서 Yes, Delete(예, 삭제합니다)를 클릭합니다.

IAM 그룹(AWS CLI) 삭제

AWS CLI에서 IAM 그룹을 삭제할 수 있습니다.

IAM 그룹(AWS CLI)을 삭제하려면

1. 그룹에서 모든 사용자를 제거합니다.
   - aws iam get-group(그룹의 사용자 목록을 가져오는 방법), aws iam remove-user-from-group(그룹에서 사용자를 제거하는 방법)
2. 그룹에 삽입된 인라인 정책을 모두 삭제합니다.
   - aws iam list-group-policies(그룹의 인라인 정책 목록을 가져오는 방법), aws iam delete-group-policy(그룹의 인라인 정책을 삭제하는 방법)
3. 그룹에 추가된 관리형 정책을 모두 분리합니다.
   - aws iam list-attached-group-policies(그룹에 추가된 관리형 정책 목록을 가져오는 방법), aws iam detach-group-policy(그룹에서 관리형 정책을 분리하는 방법)
4. 그룹을 삭제합니다.

- aws iam delete-group

IAM 그룹(AWS API) 삭제

AWS API를 사용하여 IAM 그룹을 삭제할 수 있습니다.

IAM 그룹(AWS API)을 삭제하려면

1. 그룹에서 모든 사용자를 제거합니다.
   - GetGroup(그룹의 사용자 목록 확인) 및 RemoveUserFromGroup(그룹에서 사용자 제거)
2. 그룹에 삽입된 인라인 정책을 모두 삭제합니다.
   - ListGroupPolicies(그룹의 인라인 정책 목록 확인) 및 DeleteGroupPolicy(그룹의 인라인 정책 삭제)
3. 그룹에 추가된 관리형 정책을 모두 분리합니다.
   - ListAttachedGroupPolicies(그룹에 연결된 관리형 정책의 목록 확인) 및 DetachGroupPolicy(그룹에서 관리형 정책 연결 분리)
4. 그룹을 삭제합니다.
   - DeleteGroup

IAM역할

IAM 역할은 특정 권한을 가진 계정에 생성할 수 있는 IAM 자격 증명입니다. AWS에서 자격 증명이 할 수 있는 것과 없는 것을 결정하는 권한 정책을 갖춘 AWS 자격 증명이라는 점에서, IAM 역할은 IAM 사용자와 유사합니다. 그러나 역할은 한 사람과만 연관되지 않고 그 역할이 필요한 사람이면 누구든지 맡을 수 있도록 고안되었습니다. 또한 역할에는 그와 연관된 암호 또는 액세스 키와 같은 표준 장기 자격 증명이 없습니다. 그 대신, 역할을 수임하면 역할 세션을 위한 임시 보안 자격 증명을 제공합니다.

역할을 사용하여 일반적으로 AWS 리소스에 액세스할 수 없는 사용자, 애플리케이션 또는 서비스에 액세스 권한을 위임할 수 있습니다. 예를 들어 AWS 계정의 사용자에게 이들이 대개 권한이 없는 리소스에 대한 액세스 권한을 부여하거나 한 AWS 계정의 사용자에게 다른 계정의 리소스에 대한 액세스 권한을 부여해야 할 경우가 있습니다. 또는 모바일 앱에서 AWS 리소스를 사용할 수 있도록 하되 앱에 AWS 키를 내장(교체하기 어렵고 사용자가 추출할 가능성이 있음)하길 원치 않는 경우도 있습니다. 때로는 기업 디렉토리에서처럼 AWS 외부에 정의된 자격 증명을 이미 보유하고 있는 사용자에게 AWS 액세스 권한을 부여해야 하는 경우도 있습니다. 또는 타사에 계정에 대한 액세스 권한을 부여하여 리소스에 대한 감사를 수행할 수 있도록 해야 할 경우도 있을 수 있습니다.

이러한 경우 IAM 역할을 사용하여 AWS 리소스에 대한 액세스 권한을 위임할 수 있습니다. 이 단원에서는 역할 및 역할을 사용할 수 있는 여러 가지 방법, 다양한 접근 방식을 선택하는 경우와 방법, 역할을 생성, 관리, 전환(또는 수임) 및 삭제하는 방법을 소개합니다.

주제

역할 용어 및 개념

아래는 역할을 시작하는 데 도움이 되는 몇 가지 기본 용어들입니다.

역할

특정 권한을 가진 계정에 생성할 수 있는 IAM 자격 증명. IAM 역할은 IAM 사용자와 몇 가지 점에서 유사합니다. 역할과 사용자 모두 AWS에서 자격 증명으로 할 수 있는 것과 할 수 없는 것을 결정하는 권한 정책을 포함하는 AWS 자격 증명입니다. 그러나 역할은 한 사람과만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다. 또한 역할에는 그와 연관된 암호 또는 액세스 키와 같은 표준 장기 자격 증명이 없습니다. 그 대신, 역할을 수임하면 역할 세션을 위한 임시 보안 자격 증명을 제공합니다.

역할은 다음의 주체들이 사용할 수 있습니다.

- 동일한 AWS 계정의 IAM 사용자
- 역할과 다른 AWS 계정의 IAM 사용자
- Amazon Elastic Compute Cloud(Amazon EC2)와 같은 AWS가 제공하는 웹 서비스
- SAML 2.0, OpenID Connect 또는 사용자 지정 구축 자격 증명 브로커와 호환되는 외부 자격 증명 공급자(IdP) 서비스에 의해 인증된 외부 사용자

AWS 서비스 역할

서비스가 사용자를 대신하여 사용자 계정에서 작업을 수행하기 위해 수임한 역할입니다. 일부 AWS 서비스 환경을 설정할 때, 서비스에서 맡을 역할을 정의해야 합니다. 이 서비스 역할에는 서비스가 AWS 리소스에 액세스하는 데 필요한 모든 권한이 포함되어야 합니다. 서비스 역할은 서비스마다 다르지만, 해당 서비스에 대한 문서화된 요구 사항을 충족하는 한 대부분의 경우 권한을 선택할 수 있습니다. 서비스 역할은 해당 계정 내에서만 액세스를 제공하며 다른 계정의 서비스에 대한 액세스를 부여하는 데 사용할 수 없습니다. IAM 내에서 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다.

EC2 인스턴스의 AWS 서비스 역할

Amazon EC2 인스턴스에서 실행 중인 애플리케이션이 계정에서 작업을 수행하기 위해 맡을 수 있는 특수한 유형의 서비스 역할 이 역할은 시작된 EC2 인스턴스에 할당됩니다. 해당 인스턴스에서 실행 중인 애플리케이션은 임시 보안 자격 증명을 검색하고 역할이 허용하는 작업을 수행할 수 있습니다. EC2 인스턴스의 서비스 역할 사용에 대한 세부 정보는 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265)를 참조하십시오.

AWS 서비스 연결 역할

AWS 서비스에 직접 연결된 고유한 유형의 서비스 역할입니다. 서비스 연결 역할은 해당 서비스에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다. 또한 연결된 서비스는 서비스 연결 역할을 만들고 수정하며 삭제하는 방법을 정의합니다. 서비스는 역할을 자동으로 만들거나 삭제할 수 있습니다. 서비스의 프로세스나 마법사를 사용하여 사용자가 역할을 만들거나 수정하거나 삭제하도록 허용할 수도 있습니다. 또는 사용자가 IAM을 사용하여 역할을 만들거나 삭제하도록 요구할 수도 있습니다. 방법이 어떻든, 서비스 연결 역할은 필요한 권한을 수동으로 추가할 필요가 없으므로 서비스를 더 쉽게 설정할 수 있습니다.

Note

서비스 연결 역할 지원을 시작할 때 이미 서비스를 사용하는 중이라면 계정의 새 역할에 대해 알려주는 이메일을 받게 될 수 있습니다. 이 경우 서비스에서 계정에 서비스 연결 역할을 자동으로 생성합니다. 이 역할을 지원하기 위해 어떤 작업도 수행할 필요가 없으며, 이 역할을 수동으로 삭제할 수 없습니다. 자세한 내용은 내 AWS 계정에 표시되는 새 역할 (p. 553) 단원을 참조하십시오.

서비스 연결 역할의 사용을 지원하는 서비스에 대한 자세한 내용은 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [Yes] 링크를 선택합니다. 서비스에 서비스 연결 역할 만들기, 수정 또는 삭제에 대한 설명서가 포함되어 있지 않으면 IAM 콘솔, AWS CLI 또는 API를 사용하면 됩니다. 자세한 내용은 서비스 연결 역할 사용 (p. 218) 단원을 참조하십시오.

역할 함께 묶기

역할 함께 묶기는 AWS CLI 또는 API를 통해 역할을 사용하여 두 번째 역할을 수임하는 경우 발생합니다. 예를 들어, `User1`에게 `RoleA` 및 `RoleB`를 맡을 권한이 있다고 가정해 보겠습니다. 또한 `RoleA`에는 `RoleB`를 맡을 권한이 있습니다. `AssumeRole` API 작업에서 `User1`의 장기 사용자 자격 증명을 사용하여 `RoleA`를 맡을 수 있습니다. 이 작업은 `RoleA`의 단기 자격 증명을 반환합니다. 역할 체인에 참여하기 위해 `RoleA`의 단기 자격 증명을 사용하여 `RoleB`를 맡을 수 있습니다.

역할을 맡을 때 세션 태그를 전달하고 태그를 전이적으로 설정할 수 있습니다. 전이적 세션 태그는 역할 체인의 모든 후속 세션에 전달됩니다. 세션 태그에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

역할 체인을 사용하면 AWS CLI 또는 AWS API 역할 세션이 최대 1시간으로 제한됩니다. AssumeRole API 작업을 사용하여 역할을 수임할 때 `DurationSeconds` 파라미터를 사용하여 역할 세션 길이를 지정할 수 있습니다. 역할에 대한 최대 세션 기간 설정 (p. 251)에 따라 파라미터 값을 최대 43200초(12시간)까지 지정할 수 있습니다. 그러나 역할 함께 묶기를 사용해 역할을 수임하고 1시간보다 큰 `DurationSeconds` 파라미터 값을 지정하면 작업이 실패합니다.

AWS에서는 역할을 사용하여 EC2 인스턴스에서 실행되는 애플리케이션에 권한을 부여 (p. 265)하는 것을 역할 함께 묶기로 간주하지 않습니다.

위임

제어하는 리소스에 대한 액세스를 허용하는 권한을 누군가에게 부여하는 것입니다. 위임은 두 계정 간에 신뢰를 설정하는 것을 포함합니다. 첫 번째는 리소스를 소유한 계정입니다(신뢰하는 계정). 두 번째는 리소스에 액세스해야 하는 사용자가 포함된 계정입니다(신뢰되는 계정). 신뢰받는 계정과 신뢰하는 계정은 다음 중 하나가 될 수 있습니다.

- 동일 계정
- 조직에서 통제하는 별도의 계정
- 서로 다른 조직이 소유한 2개의 계정

리소스에 대한 액세스 권한을 위임하려면, 2개의 정책 (p. 177)이 연결되어 있는 IAM 역할을 생성 (p. 226)합니다. 권한 정책은 역할 사용자에게 리소스에 대해 의도한 작업을 수행하는 데 필요한 권한을 부여합니다. 신뢰 정책은 역할을 위임하도록 허용된 신뢰할 수 있는 계정 멤버를 지정합니다.

신뢰 정책을 생성할 때 와일드카드(*)를 보안 주체로 지정할 수 없습니다. 신뢰 정책은 신뢰하는 계정의 역할에 연결되어 있고 권한의 절반에 해당합니다. 나머지 절반은 사용자에게 역할 전환 또는 위임을 허용하는 (p. 252) 신뢰받는 계정의 사용자에게 연결된 권한 정책입니다. 임시로 역할을 위임하는 사용자는 자신의 고유 권한을 포기하고 대신 해당 역할의 권한을 위임합니다. 사용자가 역할을 끝내거나 역할 사용을 중지하면 원래 사용자 권한이 자동으로 회복됩니다. 외부 ID (p. 229)라 불리는 부가적인 파라미터는 동일한 조직에 의해 제어되지 않는 계정 사이에서 역할을 안전하게 사용하도록 하는 데 도움이 됩니다.

연동

외부 자격 증명 공급자와 AWS 사이에 신뢰 관계를 생성하는 것입니다. 사용자들은 Login with Amazon, Facebook, Google 또는 OpenID Connect(OIDC)와 호환되는 IdP 등의 웹 자격 증명 공급자에 로그인할 수 있습니다. 또한, 사용자는 Microsoft Active Directory 연동 서비스와 같은 Security Assertion Markup Language(SAML) 2.0과 호환되는 엔터프라이즈 자격 증명 시스템에 로그인할 수 있습니다. OIDC 및 SAML 2.0을 사용해 이 외부 자격 증명 공급자와 AWS 사이에 신뢰 관계를 구성할 때, 사용자에게는 IAM 역할이 할당됩니다. 사용자는 임시 보안 자격 증명을 부여받아 AWS 리소스에 대한 액세스가 가능합니다.

연합된 사용자

IAM 사용자를 만드는 대신 AWS Directory Service의 기존 자격 증명, 엔터프라이즈 사용자 디렉터리 또는 웹 자격 증명 공급자를 사용할 수 있습니다. 이 사용자를 연합된 사용자라고 합니다. AWS에서는 자격 증명 공급자 (p. 183)를 통해 액세스가 요청되면 연합된 사용자에게 역할을 할당합니다. 연합된 사용자에 대한 자세한 내용은 IAM 사용 설명서의 연합된 사용자 및 역할 (p. 12)을 참조하십시오.

신뢰 정책

역할을 맡기 위해 신뢰할 보안 주체를 정의하는 JSON 정책 문서 (p. 637)입니다. 역할 신뢰 정책은 IAM의 역할에 연결된 필수 리소스 기반 정책 (p. 350)입니다. 신뢰 정책에서 지정할 수 있는 보안 주체 (p. 589)에는 사용자, 역할, 계정 및 서비스가 포함됩니다.

권한 정책

JSON 형식의 권한 문서로, 역할이 사용할 수 있는 리소스와 작업을 정의합니다. 이 문서는 IAM 정책 언어 (p. 586)의 규칙에 따라 작성됩니다.

권한 경계

자격 증명 기반 정책이 역할에 부여할 수 있는 최대 권한을 제한하는 정책을 사용하는 고급 기능입니다. 서비스 연결 역할에 권한 경계를 적용할 수 없습니다. 자세한 내용은 IAM 엔터티에 대한 권한 경계 (p. 363) 단원을 참조하십시오.

Principal

작업을 수행하고 리소스에 액세스할 수 있는 AWS의 개체입니다. 보안 주체는 AWS 계정 루트 사용자, IAM 사용자 또는 역할입니다. 리소스에 액세스할 수 있는 권한을 다음 두 가지 중 한 가지 방식으로 부여할 수 있습니다.

- 권한 정책을 사용자에게(직접 또는 그룹을 통해 간접적으로) 또는 역할에게 연결할 수 있습니다.
- 리소스 기반 정책 (p. 12)을 지원하는 서비스의 경우 해당 리소스에 연결된 정책의 `Principal` 요소에서 보안 주체를 식별할 수 있습니다.

AWS 계정을 보안 주체로 참조하는 경우 그 보안 주체는 일반적으로 해당 계정 내에서 정의된 모든 보안 주체를 의미합니다.

Note

역할의 신뢰 정책에서 `Principal` 요소에 와일드카드(*)를 사용할 수 없습니다.

교차 계정 액세스를 위한 역할

한 계정의 리소스에 대한 액세스 권한을 다른 계정의 신뢰할 수 있는 보안 주체에 부여하는 역할. 역할은 교차 계정 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 제품을 사용하면 (역할을 프록시로 사용하는 대신) 리소스에 직접 정책을 연결할 수 있습니다. 이를 리소스 기반 정책이라고 하며, 이 정책을 사용하여 다른 AWS 계정의 보안 주체에게 리소스에 대한 액세스 권한을 부여할 수 있습니다. 이러한 리소스에는 Amazon Simple Storage Service(S3) 버킷, S3 Glacier 볼트, Amazon Simple Notification Service(SNS) 주제 및 Amazon Simple Queue Service(SQS) 대기열이 포함됩니다. 리소스 기반 정책을 지원하는 서비스에 대한 자세한 내용은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 리소스 기반 정책에 대한 자세한 내용은 IAM 역할과 리소스 기반 정책의 차이 (p. 287) 단원을 참조하십시오.

역할에 대한 일반적인 시나리오: 사용자, 애플리케이션 및 서비스

대부분의 AWS 기능과 마찬가지로 역할 사용에는 일반적으로 2가지 방법이 있습니다. 즉, IAM 콘솔에서 대화식으로 사용하는 것 또는 AWS CLI, Windows PowerShell용 도구 또는 API에서 프로그래밍 방식으로 사용하는 것입니다.

- IAM 콘솔을 사용하는 계정의 IAM 사용자는 역할로 전환하여 콘솔에서 해당 역할의 권한을 임시로 사용할 수 있습니다. 사용자는 자신의 원래 권한을 포기하고 역할에 할당된 권한을 수임합니다. 사용자가 역할을 끝내면 원래 권한이 복원됩니다.
- AWS가 제공하는 애플리케이션 또는 서비스(예: Amazon EC2)에서 AWS에 프로그래밍 방식으로 요청하기 위한 역할에 대한 임시 보안 자격 증명을 요청하여 역할을 수임할 수 있습니다. 역할을 이러한 방식으로 사용함으로써 리소스에 액세스해야 하는 각 엔터티마다 장기 보안 자격 증명을 공유하거나 유지(예를 들면 IAM 사용자를 생성함으로써)할 필요가 없습니다.

> **Note**
>
> 이 안내서는 역할로 전환합니다와 역할을 수임합니다라는 표현을 서로 대치할 수 있는 동일한 의미로 사용합니다.

역할을 사용하는 가장 간단한 방법은 IAM 사용자에게 자신 또는 다른 AWS 계정에서 만든 역할로 전환할 권한을 부여하는 것입니다. IAM 사용자는 IAM 콘솔을 통해 역할을 쉽게 전환하여 일반적으로 부여받지 않은 권한을 사용할 수 있습니다. 이후 역할을 끝내 그러한 권한을 포기할 수 있습니다. 이를 통해 중요한 리소스에 잘못 액세스하거나 이를 수정하는 일을 방지할 수 있습니다.

애플리케이션 및 서비스 또는 연동된 외부 사용자에게 액세스 권한을 부여하는 등 역할을 한층 복잡한 방식으로 사용하기 위해 `AssumeRole` API를 호출할 수 있습니다. 이 API 호출은 애플리케이션이 이후의 API 호출에 사용할 수 있는 일련의 임시 자격 증명 세트를 반환합니다. 임시 자격 증명을 사용하여 시도하는 작업에는 연결된 역할에서 부여한 권한만 있습니다. 애플리케이션에서는 콘솔에서 사용자가 하듯이 역할을 "끝낼" 필요가 없습니다. 단지 애플리케이션에서 임시 자격 증명 사용을 중지하고 원래 자격 증명으로 호출을 재개합니다.

연동 사용자는 IdP(자격 증명 공급자)에서 제공하는 자격 증명을 사용하여 로그인합니다. 그 다음 AWS에서 신뢰받는 IdP에 임시 자격 증명을 제공하여 이후의 AWS 리소스 요청에 포함할 수 있도록 사용자에게 전달합니다. 그러한 자격 증명은 할당된 역할에 부여된 권한을 제공합니다.

이 섹션에서는 다음 시나리오의 개요를 제공합니다.

- 소유한 AWS 계정의 IAM 사용자에게 액세스를 제공함으로써 소유한 다른 계정의 리소스에 액세스하도록 하는 경우 (p. 178)
- 타사가 소유한 AWS 계정에 속한 IAM 사용자에게 액세스를 제공하는 경우 (p. 180)
- AWS가 제공하는 서비스를 위해 AWS 리소스에 대한 액세스 권한을 제공하는 경우 (p. 181)
- 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동) (p. 181)

자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공

IAM 사용자에게 AWS 계정 내에서 역할을 전환하거나 소유하고 있는 다른 AWS 계정에 정의된 역할로 전환할 수 있는 권한을 부여할 수 있습니다.

> **Note**
>
> 소유하지 않은 또는 제어하지 않는 계정에 대한 액세스 권한을 부여하고자 하는 경우, 이 주제 뒷부분의 타사가 소유한 AWS 계정에 대한 액세스 제공 (p. 180) 단원을 참조하십시오.

조직에 중요한 Amazon EC2 인스턴스가 있다고 가정해 봅시다. 사용자에게 인스턴스를 종료할 수 있는 권한을 직접 부여하지 않고, 이러한 권한이 있는 역할을 만들 수 있습니다. 그런 다음 관리자는 인스턴스를 종료해야 하는 경우 해당 역할로 전환할 수 있습니다. 그러면 이러한 인스턴스에 다음과 같은 보호 계층이 추가됩니다.

- 사용자에게 역할을 수임할 권한을 명시적으로 부여해야 합니다.
- 사용자는 AWS Management 콘솔을 사용하여 해당 역할로 능동적으로 전환하거나 AWS CLI 또는 AWS API를 사용하여 역할을 수임해야 합니다.
- 역할에 멀티 팩터 인증(MFA) 보호를 추가하여 MFA 디바이스로 로그인하는 사용자만 역할을 수임할 수 있도록 합니다. 역할을 수임한 사용자가 MFA(멀티 팩터 인증)를 사용하여 처음에 인증을 받도록 역할을 구성하는 방법을 알아보려면 MFA 보호 API 액세스 구성 (p. 146) 단원을 참조하십시오.

이 방법을 사용하여 최소 권한 원칙을 적용하는 것이 좋습니다. 다시 말해, 특정 작업이 필요한 경우에만 승격된 권한을 사용하도록 제한하는 것입니다. 역할을 사용하여 중요한 환경을 실수로 변경하는 일을 방지할

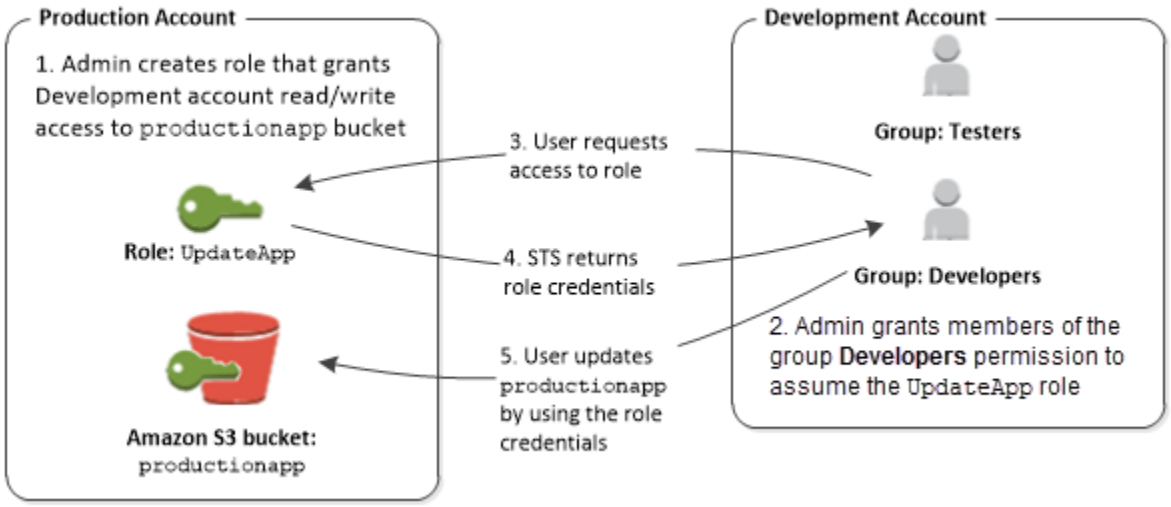
수 있습니다. 특히 필요할 때만 역할이 사용되는지 확인하기 위해 중요한 환경을 감사 (p. 334)와 결합하는 경우에 그렇습니다.

이러한 목적을 위해 역할을 만들려면 해당 역할의 신뢰 정책 `Principal` 요소에서 액세스가 필요한 사용자의 ID로 계정을 지정합니다. 그런 다음 이러한 다른 계정의 특정 사용자에게 해당 역할로 전환할 수 있는 권한을 부여할 수 있습니다. 해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

한 계정의 사용자는 동일한 또는 다른 계정의 역할로 전환할 수 있습니다. 사용자는 역할을 사용하는 동안 해당 작업만을 수행하고 해당 역할에서 허용한 리소스만 액세스할 수 있지만, 이들의 원래 사용자 권한은 일시 중지된 상태입니다. 사용자가 역할을 끝내면 원래 사용자 권한이 회복됩니다.

분리된 개발 및 프로덕션 계정을 사용한 예제 시나리오

프로덕션 환경에서 개발 환경을 격리하기 위해 조직이 여러 개의 AWS 계정을 갖고 있다고 가정합시다. 개발 계정의 사용자는 프로덕션 계정의 리소스에 액세스해야 하는 경우가 있습니다. 예를 들어, 개발 환경에서 프로덕션 환경으로 업데이트를 승격하려는 경우 교차 계정 액세스 권한이 필요할 수 있습니다. 두 계정을 모두 사용하는 사용자를 위해 별도의 자격 증명(및 암호)을 생성했다 해도 여러 계정에 대한 자격 증명을 관리할 경우 자격 증명 관리가 어려워집니다. 다음 그림을 보면 모든 사용자가 개발 계정에서 관리됩니다. 그러나 일부 개발자에게는 프로덕션 계정에 대한 제한된 액세스 권한이 필요합니다. 개발 계정에는 Testers와 Developers라는 두 개의 그룹이 있으며 각 그룹에는 고유의 정책이 있습니다.



1. 프로덕션 계정에서 관리자는 IAM을 사용하여 그 계정에 `UpdateApp` 역할을 만듭니다. 관리자는 그 역할에서 개발 계정을 `Principal`로 지정하는 신뢰 정책을 정의합니다. 이는 개발 계정의 권한이 있는 사용자는 `UpdateApp` 역할을 사용할 수 있다는 것을 뜻합니다. 또한, 관리자는 이 역할의 사용자가 `productionapp`이라는 Amazon S3 버킷에 대한 읽기 및 쓰기 권한을 보유하도록 지정하는 역할에 대한 권한 정책을 정의합니다.

   그런 다음 관리자는 적절한 정보를 이 역할을 수임해야 하는 대상과 공유합니다. 그러한 정보로는 계정 번호와 역할 이름(AWS 콘솔 사용자들에 대한) 또는 Amazon 리소스 이름(ARN)(AWS CLI 또는 AWS API 액세스용)이 있습니다. 이 역할의 ARN은 `arn:aws:iam::123456789012:role/UpdateApp`과 같은 형태를 띕니다. 여기에서 역할의 이름은 `UpdateApp`이고, 역할이 생성된 계정 번호는 123456789012입니다.

   > **Note**
   >
   > 관리자는 역할을 수임하는 사용자가 먼저 멀티 팩터 인증(MFA)을 사용하여 인증을 받도록 역할을 구성할 수도 있습니다. 자세한 내용은 MFA 보호 API 액세스 구성 (p. 146) 단원을 참조하십시오.

2. 개발 계정에서 관리자는 Developer 그룹의 구성원에게 이 역할로 전환할 수 있는 권한을 부여합니다. 이를 수행하려면 Developers 그룹에 `UpdateApp` 역할에 대한 AWS Security Token Service(AWS STS) `AssumeRole` API를 호출할 권한을 부여하면 됩니다. 이제 개발 계정의 Developers 그룹에 속한 모든 IAM 사용자는 프로덕션 계정의 `UpdateApp` 역할로 전환할 수 있습니다. Developer 그룹에 속하지 않은 다른 사용자는 이 역할로 전환할 수 있는 권한이 없으므로 프로덕션 계정의 S3 버킷에 액세스할 수 없습니다.
3. 사용자가 이 역할로의 전환을 요청:
   - AWS 콘솔: 탐색 표시줄에서 계정 이름을 선택하고 Switch Role(역할 전환)을 선택합니다. 계정 ID(또는 별칭) 및 역할 이름을 지정합니다. 아니면 사용자는 관리자가 이메일로 보낸 링크를 클릭해도 됩니다. 링크를 누르면 세부 정보가 이미 채워져 있는 Switch Role(역할 전환) 페이지로 이동합니다.
   - AWS API/AWS CLI: 개발 계정의 Developers 그룹에 속한 사용자는 `AssumeRole` 함수를 호출하여 `UpdateApp` 역할에 대한 자격 증명을 가져옵니다. `UpdateApp` 역할의 ARN을 이 호출의 일부로 지정합니다. Testers 그룹의 사용자가 동일한 요청을 하는 경우에는 요청이 실패하는데, 이는 Testers가 `AssumeRole` 역할 ARN을 위해 `UpdateApp`을 호출할 권한이 없기 때문입니다.
4. AWS STS는 임시 자격 증명을 반환합니다.
   - AWS 콘솔: AWS STS에서 그 요청이 신뢰할 수 있는 대상(개발 계정)에서 온 것인지 확인하기 위해 그 요청에 대해 역할의 신뢰 정책을 확인합니다. 확인 후 AWS STS에서 AWS 콘솔로 임시 보안 자격 증명을 반환합니다.
   - API/CLI: AWS STS에서 신뢰할 수 있는 대상(Development 계정)이 요청을 보낸 것인지 확인하기 위해 역할의 신뢰 정책에 대한 요청을 확인합니다. 확인 후 AWS STS에서 해당 애플리케이션으로 임시 보안 자격 증명을 반환합니다.
5. 임시 자격 증명은 AWS 리소스에 대한 액세스를 허용합니다.
   - AWS 콘솔: AWS 콘솔은 이후의 모든 콘솔 작업에서 사용자를 대신하여 임시 자격 증명을 사용합니다. 이 경우에 그 작업이란 `productionapp` 버킷에 대한 읽기 및 쓰기입니다. 이 콘솔은 프로덕션 계정의 다른 리소스에는 액세스할 수 없습니다. 사용자가 역할을 끝내면 사용자의 권한은 이 역할로 전환하기 전에 보유한 원래의 권한으로 돌아갑니다.
   - API/CLI: 이 애플리케이션에서는 임시 보안 자격 증명을 사용하여 `productionapp` 버킷을 업데이트합니다. 이 애플리케이션은 임시 보안 자격 증명을 통해 `productionapp` 버킷에 대한 읽기 및 쓰기만 할 수 있으며 프로덕션 계정의 다른 리소스에는 액세스할 수 없습니다. 애플리케이션은 역할을 종료하지 않아도 되지만 대신에 임시 자격 증명 사용을 중지하고 이후의 API 호출에서 다시 원래의 자격 증명을 사용합니다.

타사가 소유한 AWS 계정에 대한 액세스 제공

타사가 조직의 AWS 리소스에 액세스해야 하는 경우 역할을 사용하여 해당 사용자에게 그에 대한 액세스 권한을 위임할 수 있습니다. 예를 들어, 타사가 AWS 리소스를 관리하는 서비스를 제공할 경우 IAM 역할을 사용하면 AWS 보안 자격 증명을 공유하지 않고 외부 사용자에게 AWS 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 대신 제3자는 AWS 계정에서 생성한 역할을 수임하여 AWS 리소스에 액세스할 수 있습니다. 해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

해당 사용자가 수임할 수 있는 역할을 생성하려면 타사가 다음 정보를 제공해야 합니다.

- 타사의 AWS 계정 ID 역할에 대한 신뢰 정책을 정의할 때 AWS 계정 ID를 보안 주체로 지정합니다.
- 역할을 고유하게 연결하는 데 사용하는 외부 ID. 외부 ID는 여러분과 타사가 알고 있는 임의의 비밀 식별자일 수 있습니다. 예를 들어, 여러분과 타사가 사용하는 인보이스 ID를 사용할 수 있지만 타사의 이름이나 전화번호와 같이 추측 가능한 것은 사용하지 마십시오. 역할에 대한 신뢰 정책을 정의할 때 이 ID를 지정해야 합니다. 타사가 역할을 수임할 때 이 ID를 제공해야 합니다. 외부 ID에 대한 자세한 내용은 AWS 리소스에 대한 액세스를 타사에 부여할 때 외부 ID를 사용하는 방법 (p. 229)을 참조하십시오.
- 귀사의 AWS 리소스를 사용하기 위해 타사에게 필요한 권한. 역할의 권한 정책을 정의할 때 이러한 권한을 지정해야 합니다. 이 정책은 타사에서 수행할 수 있는 작업과 액세스할 수 있는 리소스를 정의합니다.

역할을 정의한 후에는 역할의 Amazon 리소스 이름(ARN)을 타사에 제공해야 합니다. 타사가 역할을 수임하려면 해당 역할의 ARN이 필요합니다.

타사에게 액세스 권한을 위임하는 역할을 생성하는 방법은 AWS 리소스에 대한 액세스를 타사에 부여할 때 외부 ID를 사용하는 방법 (p. 229)를 참조하십시오.

Important

타사에 AWS 리소스에 대한 액세스 권한을 부여하는 경우 타사는 여러분이 정책에서 지정하는 모든 리소스에 액세스할 수 있습니다. 타사의 리소스 사용에 대해서는 여러분에게 과금됩니다. 타사의 리소스 사용을 적절하게 제한해야 합니다.

AWS 서비스에 액세스 권한 제공

많은 AWS 서비스에서는 역할을 사용하여 해당 서비스가 액세스할 수 있는 대상을 제어해야 합니다. 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임한 역할을 서비스 역할 (p. 175)이라고 합니다. 역할이 서비스에 대해 특수한 목적을 수행하는 경우 EC2 인스턴스의 서비스 역할 (p. 175) 또는 서비스 연결 역할 (p. 175)로 분류할 수 있습니다. 서비스에서 역할을 사용하는지 여부와 서비스에서 사용할 역할을 할당하는 방법을 알아보려면 서비스별 AWS 문서를 참조하십시오.

역할을 생성해 AWS가 제공하는 서비스에 액세스 권한을 위임하는 것에 대한 자세한 내용은 AWS 서비스에 대한 권한을 위임할 역할 생성 (p. 233) 단원을 참조하십시오.

외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)

사용자는 이미 기업 디렉토리 등 AWS 외부에 자격 증명을 보유할 수 있습니다. 그러한 사용자가 AWS 리소스를 사용해야 하는 경우(또는 그러한 리소스에 액세스하는 애플리케이션을 사용해야 하는 경우), AWS 보안 자격 증명이 필요합니다. IAM 역할을 사용하여 자격 증명이 내 조직 또는 타사 IdP(자격 증명 공급자)로부터 연동되는 사용자에 대한 권한을 지정할 수 있습니다.

모바일 또는 웹 기반 앱 사용자들을 Amazon Cognito와 연동하기

AWS 리소스에 액세스하는 모바일 또는 웹 기반 앱을 만드는 경우, 이 앱에는 AWS에 프로그래밍 방식으로 요청하기 위해 보안 자격 증명이 필요합니다. 대부분의 모바일 애플리케이션 시나리오의 경우 Amazon Cognito 사용을 권장합니다. 이 서비스와 함께 iOS용 Mobile SDK, Android 및 Fire OS용 AWS Mobile SDK를 사용하여 사용자 고유 자격 증명을 만들고 AWS 리소스에 대한 보안 액세스를 인증할 수 있습니다. Amazon Cognito는 다음 단원에 나열한 것과 동일한 자격 증명 제공자를 지원하며 개발자 인증 자격 증명 및 인증되지 않은(게스트) 액세스도 지원합니다. Amazon Cognito는 디바이스를 바꿔 가며 이용해도 데이터를 보존하도록 사용자 데이터 동기화를 위한 API 작업도 제공합니다. 자세한 내용은 모바일 앱을 위한 Amazon Cognito 사용 (p. 184) 단원을 참조하십시오.

사용자를 퍼블릭 자격 증명 서비스 공급자 또는 OpenID Connect와 연동하기

가능한 경우에는 언제든지 모바일 및 웹 기반 애플리케이션 시나리오를 위해 Amazon Cognito를 사용하십시오. Amazon Cognito는 퍼블릭 자격 증명 공급자 서비스를 이용해 대부분의 백그라운드 작업을 수행합니다. 동일한 타사 서비스를 사용하며 익명 로그인을 지원하기도 합니다. 그러나 고급 시나리오의 경우에는 Login with Amazon, Facebook, Google, 또는 OpenID Connect(OIDC)와 호환되는 모든 IdP로 직접 작업할 수 있습니다. 이들 서비스 중 한 가지를 이용한 웹 자격 증명 연동에 대한 자세한 내용은 웹 자격 증명 연동에 대하여 (p. 183)을 참조하십시오.

SAML 2.0으로 사용자 연동하기

조직에서 SAML 2.0(Security Assertion Markup Language 2.0)을 지원하는 자격 증명 공급자 소프트웨어 패키지를 이미 사용하는 경우 IdP(자격 증명 공급자)인 조직과 서비스 공급자인 AWS 간에 신뢰를 형성할 수 있습니다. 그러면 SAML을 사용하여 사용자에게 AWS Management 콘솔에 대한 연동 SSO(Single-Sing On) 또는 AWS API 작업을 호출하기 위한 연동 액세스를 제공할 수 있습니다. 예를 들어 회사가 Microsoft Active Directory와 Active Directory Federation Services를 이용한다면, SAML 2.0을 사용해 연동할 수 있습니다. SAML 2.0를 이용한 사용자 연동에 대한 세부 정보는 SAML 2.0 기반 연동에 대하여 (p. 188)을 참조하십시오.

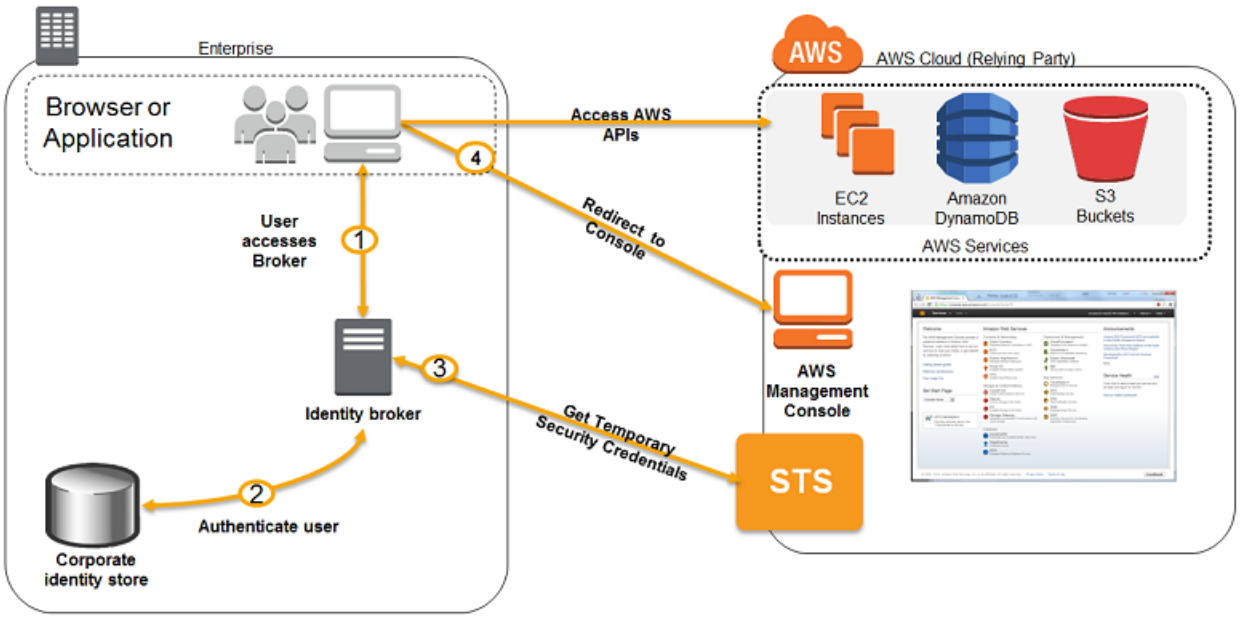
사용자 지정 자격 증명 브로커 애플리케이션 생성에 의한 사용자 연동

자격 증명 스토어가 SAML 2.0과 호환되지 않는다면, 사용자 지정 자격 증명 브로커 애플리케이션을 구축해 비슷한 기능을 수행할 수 있습니다. 브로커 애플리케이션이 사용자를 인증하고, AWS에게 사용자를 위한 임시 자격 증명을 요청한 다음, 이를 사용자에게 제공해 AWS 리소스에 액세스하도록 합니다.

예를 들어 Example Corp.에 회사의 AWS 리소스에 액세스하는 내부 애플리케이션을 실행해야 하는 직원들이 많다고 합시다. 직원들은 이미 회사 자격 증명 및 인증 시스템에서 자격 증명을 갖고 있어서 Example Corp.은 각 직원들에 대해 별도의 IAM 사용자를 생성하길 원하지 않습니다.

Example Corp의 개발자인 Bob은 내부 애플리케이션이 회사의 AWS 리소스에 액세스하도록 하기 위해 사용자 지정 자격 증명 브로커 애플리케이션을 개발합니다. 그 애플리케이션은 직원들이 기존 Example Corp. 자격 증명 및 인증 시스템에 로그인된 상태인지 확인하는데, 그 시스템은 LDAP, Active Directory, 또는 다른 시스템을 사용할 수 있습니다. 그 다음에 자격 증명 브로커 애플리케이션은 직원들에 대한 임시 보안 자격 증명을 획득합니다. 이 시나리오는 AWS 리소스에 접근할 필요가 있는 애플리케이션들이 모두 회사 네트워크 내에서 실행되고 그 회사는 기존 인증 시스템을 보유하고 있다는 점만 제외하면 이전 것(사용자 지정 인증 시스템을 사용하는 모바일 앱)과 유사합니다.

임시 보안 자격 증명을 얻기 위해 자격 증명 브로커 애플리케이션은 밥(Bob)이 사용자들에 대한 정책을 어떻게 관리하고자 하는지, 그리고 임시 자격 증명이 언제 만료되는지에 따라 `AssumeRole` 또는 `GetFederationToken`을 호출해 임시 보안 자격 증명을 획득합니다. (이러한 API 작업 간의 차이점을 보려면 임시 보안 자격 증명 (p. 302) 및 사용자 임시 보안 자격 증명에 대한 권한 제어 (p. 316)를 참조하십시오.) 호출은 AWS 액세스 키 ID, 보안 액세스 키, 세션 토큰으로 구성된 임시 보안 자격 증명을 반환합니다. 자격 증명 브로커 애플리케이션은 이 임시 보안 자격 증명을 내부 회사 애플리케이션에서도 사용할 수 있게 해줍니다. 그 앱은 그 임시 자격 증명을 사용해 AWS를 직접 호출할 수 있습니다. 그 앱은 자격 증명이 만료될 때까지 캐싱한 다음, 새로운 일련의 임시 자격 증명을 요청합니다. 다음은 이 시나리오를 설명한 그림입니다.



이 시나리오에는 다음과 같은 속성이 있습니다.

- 자격 증명 브로커 애플리케이션은 임시 보안 자격 증명을 만들 수 있도록 IAM의 보안 토큰 서비스(STS) API에 액세스할 수 있는 권한이 있습니다.
- 신원 증명 브로커 애플리케이션을 통해 기존 인증 시스템 내에서 직원이 인증되었는지 확인할 수 있습니다.
- 사용자에게 AWS Management Console에 액세스할 수 있는 임시 URL[Single-Sign-On(SSO)이라고 함]이 제공됩니다.

이 시나리오에 기술된 자격 증명 브로커 애플리케이션과 유사한 샘플 애플리케이션을 보려면, AWS Sample Code & Libraries의 Identity Federation Sample Application for an Active Directory Use Case를 참조하십시오. 임시 보안 자격 증명 생성에 대한 자세한 내용은 임시 보안 자격 증명 요청하기 (p. 304)를 참조하십시오 . AWS Management Console에 액세스하는 연동된 사용자에 대한 자세한 내용은 다음(SAML 2.0 연동 사용자가 AWS Management 콘솔에 액세스할 수 있게 하기 (p. 208))을 참조하십시오.

자격 증명 공급자 및 연동

AWS 외부의 사용자 자격 증명을 이미 관리하고 있는 경우 AWS 계정에서 IAM 사용자를 생성하는 대신 IAM 자격 증명 공급자를 사용할 수 있습니다. 자격 증명 공급자(IdP)를 사용하면 AWS 외부의 사용자 자격 증명을 관리할 수 있고 이 외부 사용자 자격 증명에 계정의 AWS 리소스에 대한 사용 권한을 부여할 수 있습니다. 기업 사용자 디렉터리처럼 조직 내에 이미 고유의 자격 증명 시스템이 있다면 이 방법이 유용합니다. 그 밖에 AWS 리소스에 액세스해야 하는 모바일 앱이나 웹 애플리케이션을 개발할 때도 효과적입니다.

IAM 자격 증명 공급자를 사용하면 사용자 지정 로그인 코드를 생성할 필요도, 그리고 자신의 사용자 자격 증명을 관리할 필요도 없습니다. IdP에서 이러한 작업을 대신 수행합니다. 외부 사용자는 Login with Amazon, Facebook 또는 Google과 같은 널리 알려진 IdP를 통해 로그인합니다. 사용자에게 계정의 AWS 리소스를 사용할 수 있는 외부 자격 증명 권한을 부여할 수 있습니다. IAM 자격 증명 공급자는 애플리케이션으로 액세스 키 같은 장기 보안 자격 증명을 배포하거나 포함할 필요가 없으므로 AWS 계정의 보안에 도움이 됩니다.

IdP를 사용하기 위해서는, 먼저 IAM 자격 증명 공급자 엔터티를 생성하여 AWS 계정과 IdP 사이에 신뢰 관계를 설정해야 합니다. IAM은 OpenID Connect(OIDC) 또는 SAML 2.0(Security Assertion Markup Language 2.0)과 호환되는 IdP를 지원합니다. AWS에서 해당 IdP 중 하나를 사용하는 것에 대한 자세한 정보는 다음을 참조하십시오.

- 웹 자격 증명 연동에 대하여 (p. 183)
- SAML 2.0 기반 연동에 대하여 (p. 188)

IAM 자격 증명 공급자 엔터티를 생성하여 호환되는 IdP와 AWS 사이에 신뢰 관계를 구축하는 방법에 대한 자세한 정보는 IAM 자격 증명 공급자 생성 (p. 192) 단원을 참조하십시오.

웹 자격 증명 연동에 대하여

모바일 디바이스에서 실행되고 Amazon S3 및 DynamoDB를 사용해 플레이어와 점수 정보를 저장하는 게임과 같은 AWS 리소스에 액세스하는 모바일 앱을 만들고 있다고 상상해 봅시다.

그런 앱을 만들 때 AWS 액세스 키로 서명해야 하는 AWS 서비스에 요청을 할 것입니다. 그러나 암호화된 스토어에서일지라도 사용자가 디바이스에 다운로드하는 앱으로 장기 AWS 자격 증명을 포함 또는 배포하지 말 것을 강력하게 권고합니다. 대신 앱을 구축해 웹 자격 증명 연동을 사용하여 필요시 동적으로 임시 AWS 보안 자격 증명을 요청할 수 있도록 하십시오. 제공된 임시 자격 증명은 모바일 앱에 필요한 작업을 수행하기 위해 필요한 권한만을 지닌 AWS 역할에 매핑됩니다.

웹 자격 증명 연동을 사용하면 사용자 지정 로그인 코드를 생성하거나 자신의 사용자 자격 증명을 관리할 필요가 없습니다. 대신에, 앱의 사용자는 Login with Amazon, Facebook, Google 또는 다른 OpenID Connect(OIDC) 호환 IdP와 같은 널리 알려진 외부 자격 증명 공급자(IdP)를 사용해 사용자가 로그인할 수 있습니다. 앱의 사용자는 인증 토큰을 받은 다음, AWS에서 이 토큰을 AWS 계정의 리소스를 사용할 수 있는 권한을 가진 IAM 역할에 매핑되는 임시 보안 자격 증명으로 바꿉니다. IdP를 사용하면 AWS 계정을 안전하게 보호할 수 있다는 이점이 있습니다. 애플리케이션으로 장기 보안 자격 증명을 포함하고 배포할 필요가 없기 때문입니다.

대부분의 시나리오에서 Amazon Cognito를 사용할 것을 권장하는 이유는 Amazon Cognito는 자격 증명 브로커의 역할을 하고 연동 작업의 대부분을 수행하기 때문입니다. 자세한 정보는 모바일 앱을 위한 Amazon Cognito 사용 (p. 184) 단원을 참조하십시오.

Amazon Cognito를 사용하지 않는다면 웹 IdP(예: Facebook, Google 또는 기타 OIDC 호환 IdP)와 상호작용하는 코드를 작성한 다음, `AssumeRoleWithWebIdentity` API를 호출해 그 IdP에서 얻는 인증 토큰을 AWS 임시 보안 자격 증명과 바꾸어야 합니다. 기존 앱에 대해 이러한 접근 방식을 이미 사용해왔다면 그것을 계속 사용할 수 있습니다.

주제

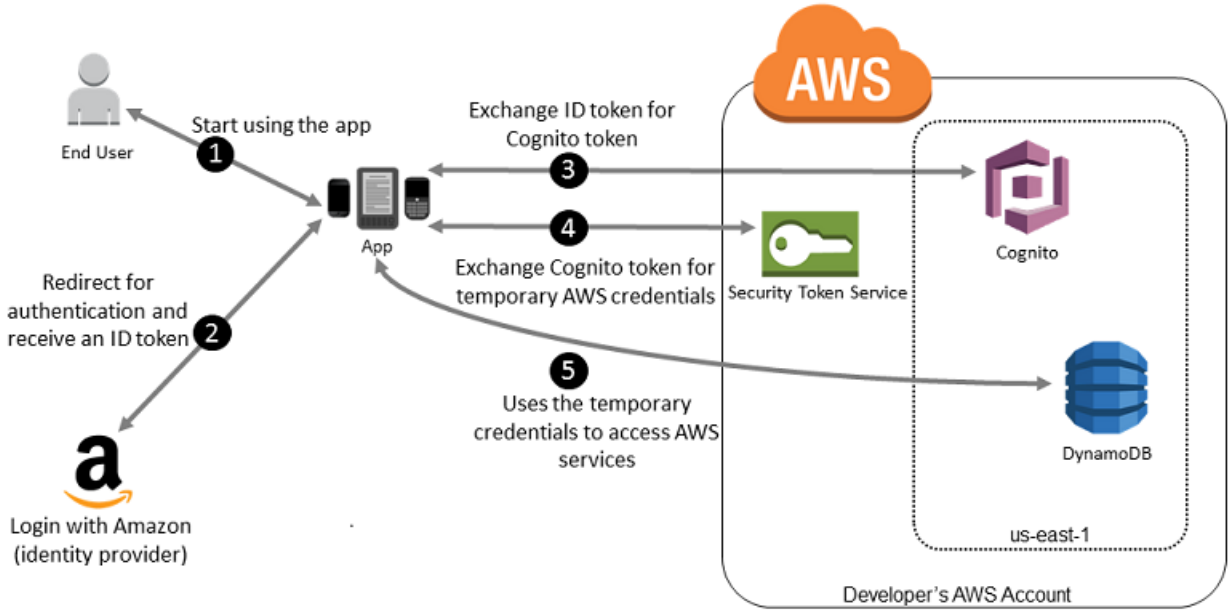
모바일 앱을 위한 Amazon Cognito 사용

웹 자격 증명 페더레이션 사용에서 선호되는 방식은 Amazon Cognito를 사용하는 것입니다. 예를 들어 개발자 Adele이 점수와 프로필이 같은 사용자 데이터가 Amazon S3와 Amazon DynamoDB에 저장되는 모바일 디바이스를 위한 게임을 만들고 있다고 합시다. Adele은 그 디바이스에 이 데이터를 로컬 저장하고 Amazon Cognito를 사용해 여러 디바이스에 걸쳐 데이터를 동기화할 수도 있습니다. Adele은 보안 및 유지 보수 상의 이유로 장기 AWS 보안 자격 증명은 게임과 함께 배포되어서는 안 된다는 것을 알고 있습니다. 또한, 게임 사용자가 아주 많을 수도 있다는 것을 알고 있습니다. 이 모든 이유로 인해 Adele은 각 플레이어에 대해 IAM에서 새로운 사용자 자격 증명을 생성하길 원하지 않습니다. 대신에 사용자가 Login with Amazon, Facebook, Google 또는 OpenID Connect(OIDC) 호환 자격 증명 공급자(IdP)와 같은 널리 알려진 외부 IdP를 통해 이미 설정한 자격 증명을 사용해 로그인할 수 있도록 게임을 구축합니다. Adele의 게임은 이러한 공급자 중 하나의 인증 메커니즘을 이용해 사용자의 자격 증명을 확인할 수 있습니다.

모바일 앱을 활성화해 자신의 AWS 리소스에 액세스하기 위해 Adele은 먼저 자신이 선택한 IdP로 개발자 ID를 등록합니다. Adele은 이들 각 공급자로 애플리케이션을 구성하기도 합니다. Adele은 게임에 대한 Amazon S3 버킷 및 DynamoDB 표가 저장된 AWS 계정에서 Amazon Cognito를 사용해 게임이 필요한 권한을 정확하게 정의하는 IAM 역할을 생성합니다. Adele이 OIDC IdP를 사용하고 있다면, IAM OIDC 자격 증명 공급자 엔터티를 생성하여 자신의 AWS 계정과 IdP 사이에 신뢰를 설정하기도 합니다.

앱의 코드에서 Adele은 자신이 이전에 구성한 IdP에 대한 로그인 인터페이스를 호출합니다. IdP는 사용자가 로그인하도록 허용하는 모든 세부 정보를 처리하고 앱은 공급자에게서 OAuth 액세스 토큰 또는 OIDC ID 토큰을 얻습니다. Adele의 앱은 이 인증 정보를 주고 AWS 액세스 키 ID, 보안 액세스 키 및 세션 토큰으로 구성된 임시 보안 자격 증명 집합을 얻을 수 있습니다. 그러면 앱은 이러한 자격 증명을 사용하여 AWS가 제공하는 웹 서비스에 액세스할 수 있습니다. 앱은 수임하는 역할에 정의된 권한으로 제한됩니다.

다음 그림은 Login with Amazon을 IdP로 사용하는 경우 이것이 어떻게 작동하는지 그 흐름을 단순화해 보여줍니다. 2단계에서 앱은 Facebook, Google 또는 OIDC 호환 IdP를 사용할 수도 있지만, 여기에서는 생략했습니다.



1. 고객은 모바일 디바이스에서 앱을 시작합니다. 앱은 사용자에게 로그인하도록 요청합니다.
2. 앱은 Login with Amazon 리소스를 사용해 사용자의 자격 증명을 수락합니다.
3. 앱은 Cognito API 작업을 사용해 Login with Amazon ID 토큰을 Cognito 토큰과 교환합니다.
4. 앱은 Cognito 토큰을 전달하면서 AWS STS에서 임시 보안 자격 증명을 요청합니다.
5. 임시 보안 자격 증명은 앱에 의해 사용됨으로써 앱이 작동을 요청하는 어떤 AWS 리소스에도 액세스할 수 있습니다. 임시 보안 자격 증명과 연결된 역할과 그에 할당된 정책은 액세스 가능한 대상을 결정합니다.

다음 절차를 통해 앱이 Amazon Cognito를 사용해 사용자를 인증하도록 구성하고 앱에게 AWS 리소스에 대한 액세스 권한을 부여하십시오. 이 시나리오를 완수하기 위한 특정 단계에 대해서는 Amazon Cognito에 대한 문서 단원을 참조하십시오.

1. (선택 사항) Login with Amazon, Facebook, Google 또는 기타 OpenID Connect(OIDC)–호환 IdP를 통해 개발자로 가입하여 그 공급자를 통해 1개 이상의 앱을 구성합니다. Amazon Cognito는 사용자를 위해 인증되지 않은(게스트) 액세스도 지원하기 때문에 이 단계는 옵션입니다.
2. AWS Management 콘솔의 Amazon Cognito로 이동합니다. Amazon Cognito 마법사를 사용해 자격 증명 풀을 생성합니다. 이 풀은 Amazon Cognito가 앱을 위해 최종 사용자 자격 증명을 정돈된 상태로 유지할 목적으로 사용하는 컨테이너입니다. 앱 간에 자격 증명 풀을 공유할 수 있습니다. 자격 증명 풀을 설정할 때 Amazon Cognito는 Amazon Cognito 사용자에 대한 권한을 정의하는 1개 이상의 IAM 역할(인증된 자격 증명에 대해 1개, 그리고 인증되지 않은 "게스트" 자격 증명을 위해 1개)을 생성합니다.
3. iOS용 AWS SDK 또는 Android용 AWS SDK를 다운로드해 앱과 통합하고 Amazon Cognito를 사용하는 데 필요한 파일을 가져옵니다.
4. Amazon Cognito 자격 증명 공급자의 인스턴스를 생성해 자격 증명 풀 ID, AWS 계정 번호 및 자격 증명 풀과 연결한 역할들의 Amazon 리소스 이름(ARN)을 전달합니다. AWS Management 콘솔의 Amazon Cognito 마법사는 샘플 코드를 제공해 시작을 돕습니다.
5. 앱이 AWS 리소스에 액세스할 때 클라이언트 객체에 자격 증명 공급자 인스턴스를 전달합니다. 이렇게 하면 클라이언트에 임시 보안 자격 증명이 전달됩니다. 자격 증명에 대한 권한은 앞서 정의한 역할 또는 역할들에 기반을 두고 있습니다.

자세한 정보는 다음을 참조하십시오.

- Android용 AWS Mobile SDK Developer Guide의 Amazon Cognito 자격 증명
- AWS Mobile SDK for iOS Developer Guide의 Amazon Cognito 자격 증명

모바일 앱을 위한 웹 자격 증명 연동 API 작업 사용

최상의 결과를 얻으려면 거의 모든 웹 자격 증명 연동 시나리오에 대해 Amazon Cognito를 자격 증명 브로커로 사용하십시오. Amazon Cognito는 사용하기 쉽고 익명의(인증되지 않은) 액세스, 디바이스 및 공급자 전반에 걸친 사용자 데이터 동기화와 같은 부가적인 기능을 제공합니다. 그러나 `AssumeRoleWithWebIdentity` API를 수동 호출함으로써 웹 자격 증명 연동을 사용하는 앱을 이미 생성했다면, 그 앱을 계속해서 사용할 수 있고 앱은 여전히 잘 작동될 것입니다.

> **Note**
>
> 웹 자격 증명 연동이 어떤 방식으로 작동하는지에 대한 이해를 돕는 Web Identity Federation Playground를 이용할 수 있습니다. 이 대화형 웹 사이트는 Login with Amazon, Facebook 또는 Google을 통해 인증하고 임시 보안 자격 증명을 얻은 다음, 이러한 자격 증명을 사용하여 AWS에 요청하는 과정을 안내합니다.

Amazon Cognito 없이 웹 자격 증명 연동을 사용하는 과정은 대체로 다음과 같은 개요를 따릅니다.

1. 외부 자격 증명 공급자(IdP)에서 개발자로 로그인하여 앱을 위한 고유 ID를 부여하는 IdP에서 앱을 구성합니다. (서로 다른 공급자는 이 과정에 대해 서로 다른 용어를 사용합니다. 이 개요는 앱을 IdP와 동일시하

는 과정에 대해 구성이라는 용어를 사용합니다). 각 IdP는 IdP 고유의 앱 ID를 제공함으로써, 동일한 앱을 다수의 IdP로 구성하는 경우 앱은 여러 개의 앱 ID를 갖게 됩니다. 각 공급자로 여러 개의 앱을 구성할 수 있습니다.

다음 외부 링크는 흔히 사용되는 자격 증명 공급자(IdP) 중 일부를 사용하는 것에 대한 정보를 제공합니다.

- Login with Amazon 개발자 센터
- Facebook 개발자 사이트의 앱 또는 웹 사이트에 Facebook 로그인 추가하기
- Google 개발자 사이트의 OAuth 2.0을 사용한 로그인(OpenID Connect)

  Note

  Amazon Cognito와 Google이 OIDC 기술에 기반을 두고 있다 해도 이러한 공급자를 사용하기 위해 IAM 자격 증명 공급자 엔터티를 생성할 필요는 없습니다. Amazon Cognito와 Google에 대한 지원은 AWS에 내장되어 있습니다.

2. OIDC와 호환되는 IdP를 사용하는 경우 OIDC용 IAM 자격 증명 공급자 엔터티를 생성합니다.
3. IAM에서 하나 이상의 역할을 생성합니다 (p. 238). 각 역할에 대해 그 역할을 위임할 대상(신뢰 정책)과 앱 사용자들이 가져야 할 권한(권한 정책)을 정의할 수 있습니다. 일반적으로 앱이 지원하는 각 IdP마다 하나의 역할을 생성합니다. 예를 들면 사용자가 Login with Amazon을 통해 로그인할 때 앱이 위임할 수 있는 역할, 사용자가 Facebook을 통해 로그인한 동일 앱에 대한 두 번째 역할 및 사용자가 Google을 통해 로그인하는 앱에 대한 세 번째 역할을 생성할 수 있습니다. 신뢰 관계를 위해서는 IdP(예: Amazon.com)를 `Principal`(신뢰받는 개체)로 지정하고 앱 ID에 할당된 IdP와 일치하는 `Condition`을 포함시키십시오. 서로 다른 공급자에 대한 역할의 예는 이 주제의 후반부에 설명되어 있습니다.
4. 애플리케이션에서 IdP로 사용자를 인증하십시오. 이렇게 하는 방법에 대한 세부 사항은 사용 중인 IdP(Login with Amazon, Facebook 또는 Google)와 앱이 실행되는 플랫폼에 따라 달라집니다. 예를 들어 Android 앱의 인증 방법은 iOS 앱 또는 JavaScript 기반 웹 앱과 다를 수 있습니다.

   일반적으로 사용자가 아직 로그인하지 않은 경우 IdP가 로그인 페이지 표시를 처리합니다. IdP가 사용자를 인증한 후에 IdP는 사용자에 대한 정보가 담긴 인증 토큰을 앱에 반환합니다. 포함된 정보의 내용은 IdP가 노출하는 것과 사용자가 공유하고자 하는 정보가 무엇인지에 달려 있습니다. 앱에서 이 정보를 사용할 수 있습니다.
5. 앱에서 `AssumeRoleWithWebIdentity` 작업을 서명 없이 호출하여 임시 보안 자격 증명을 요청할 수 있습니다. 요청 시 IdP의 인증 토큰을 전달하고 해당 IdP에 대해 생성한 IAM 역할의 Amazon 리소스 이름(ARN)을 지정합니다. AWS는 그 토큰이 신뢰할 수 있고 유효한지 확인하여, 그럴 경우에는 요청 시 이름을 지정하는 역할에 대한 권한을 지닌 앱에 임시 보안 자격 증명을 반환합니다. 그 응답에는 IdP가 사용자에게 연결하는 고유 사용자 ID와 같은, IdP에서 오는 사용자에 대한 메타데이터도 포함되어 있습니다.
6. `AssumeRoleWithWebIdentity` 응답의 임시 보안 자격 증명을 사용하여 앱에서 AWS API 작업에 대한 서명된 요청을 생성합니다. IdP에서 받은 사용자 ID 정보는 앱의 사용자를 구별할 수 있습니다. 예를 들어 사용자 ID를 접두사 또는 접미사로 포함하는 Amazon S3 폴더에 객체를 넣을 수 있습니다. 이렇게 함으로써 폴더를 잠그는 액세스 제어 정책을 생성해 그 ID를 지닌 사용자만 그 폴더에 액세스할 수 있게 됩니다. 자세한 정보는 이 주제의 후반부에서 웹 자격 증명 연동을 사용해 사용자 식별하기 (p. 186) 단원을 참조하십시오.
7. 앱은 AWS에 요청할 필요가 있을 때마다 새 임시 보안 자격 증명을 받지 않아도 되도록 임시 보안 자격 증명을 캐시해야 합니다. 기본적으로 자격 증명은 1시간 동안 유효합니다. 자격 증명이 만료되면(또는 그 전에) `AssumeRoleWithWebIdentity`에 또 한 번 호출을 하여 새로운 임시 보안 자격 증명 집합을 얻으십시오. IdP의 토큰 역시 보통 설정된 시간이 지나면 만료되기 때문에, IdP 및 IdP가 토큰을 어떻게 관리하느냐에 따라 `AssumeRoleWithWebIdentity`에 새로운 호출을 하기 전에 IdP의 토큰을 갱신해야 할 수도 있습니다. iOS를 위한 AWS SDK 또는 Android를 위한 AWS SDK를 사용하는 경우 AmazonSTSCredentialsProvider 작업을 사용해 IAM 임시 자격 증명을 필요에 따라 갱신하는 등 관리할 수 있습니다.

웹 자격 증명 연동을 사용해 사용자 식별하기

IAM에서 액세스 정책을 생성하는 경우 대체로 외부 자격 증명 공급자(IdP)를 사용하여 인증한 사용자의 ID와 구성된 앱에 기반을 두어 권한을 지정할 수 있는 기능이 유용합니다. 예를 들어 웹 자격 증명 연동을 사용하고있는 모바일 앱은 다음과 같은 구조를 사용해 Amazon S3에 정보를 저장하고자 할 것입니다.

```
myBucket/app1/user1
myBucket/app1/user2
myBucket/app1/user3
...
myBucket/app2/user1
myBucket/app2/user2
myBucket/app2/user3
...
```

또한, 공급자별로 이 경로를 구별하는 추가 기능을 원할 수도 있습니다. 이 경우에 그 구조는 다음과 같을 것입니다(공간 절약을 위해 2개의 공급자만 나열했습니다).

```
myBucket/Amazon/app1/user1
myBucket/Amazon/app1/user2
myBucket/Amazon/app1/user3
...
myBucket/Amazon/app2/user1
myBucket/Amazon/app2/user2
myBucket/Amazon/app2/user3

myBucket/Facebook/app1/user1
myBucket/Facebook/app1/user2
myBucket/Facebook/app1/user3
...
myBucket/Facebook/app2/user1
myBucket/Facebook/app2/user2
myBucket/Facebook/app2/user3
...
```

이 구조에서 `app1` 및 `app2`는 서로 다른 게임과 같이 서로 다른 앱을 나타내며, 각 앱 사용자는 구분된 폴더를 갖습니다. `app1` 및 `app2`에 대한 값은 지정하는 친숙한 이름(예: `mynumbersgame`)이거나 앱 구성 시 공급자들이 할당하는 앱 ID일 수도 있습니다. 경로에 공급자 이름을 포함하기로 한다면, 그 값은 `Cognito`, `Amazon`, `Facebook`, `Google`와 같은 친숙한 이름이 될 수도 있습니다.

애플리케이션 이름은 정적 값이므로 일반적으로 AWS Management 콘솔을 통해 `app1`과 `app2`에 대한 폴더를 생성할 수 있습니다. 공급자 이름도 정적 값이므로 경로에 공급자 이름을 포함하는 경우에도 그렇게 할 수 있습니다. 이와 대조적으로 사용자 고유 폴더(*`user1`*, *`user2`*, *`user3`* 등)는 `AssumeRoleWithWebIdentity`에 대한 요청에 의해 반환되는 `SubjectFromWebIdentityToken` 값에서 얻을 수 있는 사용자 ID를 사용해 앱에서 런타임에 생성되어야 합니다.

개별 사용자에게 리소스에 배타적인 액세스 권한을 허용하는 정책을 작성하려면, 앱 이름과 공급자 이름(사용하는 경우)을 비롯해 완전한 폴더 이름과 일치시킬 수 있습니다. 그런 다음 공급자가 반환하는 사용자 ID를 참조하는 다음 공급자별 콘텍스트 키를 포함할 수 있습니다.

- `cognito-identity.amazonaws.com:sub`
- `www.amazon.com:user_id`
- `graph.facebook.com:id`
- `accounts.google.com:sub`

OIDC 공급자의 경우 다음 예시와 같이 하위 콘텍스트 키가 있는 OIDC 공급자의 정규화된 URL을 사용합니다.

- *`server.example.com`*`:sub`

다음 예는 버킷에 대한 접두사가 문자열과 일치하는 경우에만 Amazon S3 버킷에 액세스 권한을 부여하는 권한 정책을 보여줍니다.

`myBucket/Amazon/mynumbersgame/`*`user1`*

이 예는 사용자가 Login with Amazon을 사용해 로그인되어 있고 그 사용자는 `mynumbersgame`이라는 앱을 사용하고 있다고 가정합니다. 사용자의 고유 ID는 `user_id`라는 속성으로 제시됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::myBucket"],
      "Condition": {"StringLike": {"s3:prefix": ["Amazon/mynumbersgame/
${www.amazon.com:user_id}/*"]}}
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::myBucket/amazon/mynumbersgame/${www.amazon.com:user_id}",
        "arn:aws:s3:::myBucket/amazon/mynumbersgame/${www.amazon.com:user_id}/*"
      ]
    }
  ]
}
```

Amazon Cognito, Facebook, Google 또는 기타 OpenID Connect–호환 IdP를 사용해 로그인하는 사용자를 위해 유사한 정책을 생성할 수도 있습니다. 그 정책은 다른 앱 ID뿐만 아니라 다른 공급자 이름을 경로의 일부로 사용할 것입니다.

정책에서 조건 확인을 위해 사용 가능한 웹 자격 증명 연동 키에 대한 자세한 정보는 AWS 웹 자격 증명 연동에서 사용할 수 있는 키 (p. 666) 단원을 참조하십시오.

웹 자격 증명 연동 관련 추가 리소스

다음 리소스는 웹 자격 증명 연동에 대해 자세히 알아보는 데 도움이 됩니다.

- Android용 AWS Mobile SDK Developer Guide의 Amazon Cognito 자격 증명 및 AWS Mobile SDK for iOS Developer Guide의 Amazon Cognito 자격 증명
- Web Identity Federation Playground는 Login with Amazon, Facebook 또는 Google을 통해 인증하고, 임시 보안 자격 증명을 얻은 다음, 이러한 자격 증명을 사용하여 AWS에 요청하는 과정을 안내하는 대화형 웹 사이트입니다.
- AWS .NET Development 블로그의 .NET용 AWS SDK를 사용한 웹 자격 증명 연동 항목은 Facebook에서 웹 자격 증명 연동을 사용하는 방법을 안내하며 `AssumeRoleWithWebIdentity`를 호출하는 방법과 그 API 호출에서 얻은 임시 보안 자격 증명을 사용하여 S3 버킷에 액세스하는 방법을 보여 주는 C# 코드 조각이 포함되어 있습니다.
- iOS용 AWS SDK와 Android용 AWS SDK에는 샘플 앱이 포함되어 있습니다. 이러한 앱에는 자격 증명 공급자를 호출하는 방법과 이러한 공급자의 정보를 사용하여 임시 보안 자격 증명을 가져오고 사용하는 방법을 보여주는 코드가 포함되어 있습니다.
- 모바일 애플리케이션을 사용한 웹 자격 증명 연동 항목에서는 웹 자격 증명 연동에 대해 설명하며 웹 자격 증명 연동을 사용하여 Amazon S3 컨텐츠에 액세스하는 방법의 예를 보여 줍니다.

SAML 2.0 기반 연동에 대하여

AWS는 많은 자격 증명 공급자(IdP)가 사용하는 개방형 표준인 SAML 2.0(Security Assertion Markup Language 2.0)이라는 자격 증명 연동을 지원합니다. 이 기능은 연동 SSO(Single Sign-On)를 활성화하여

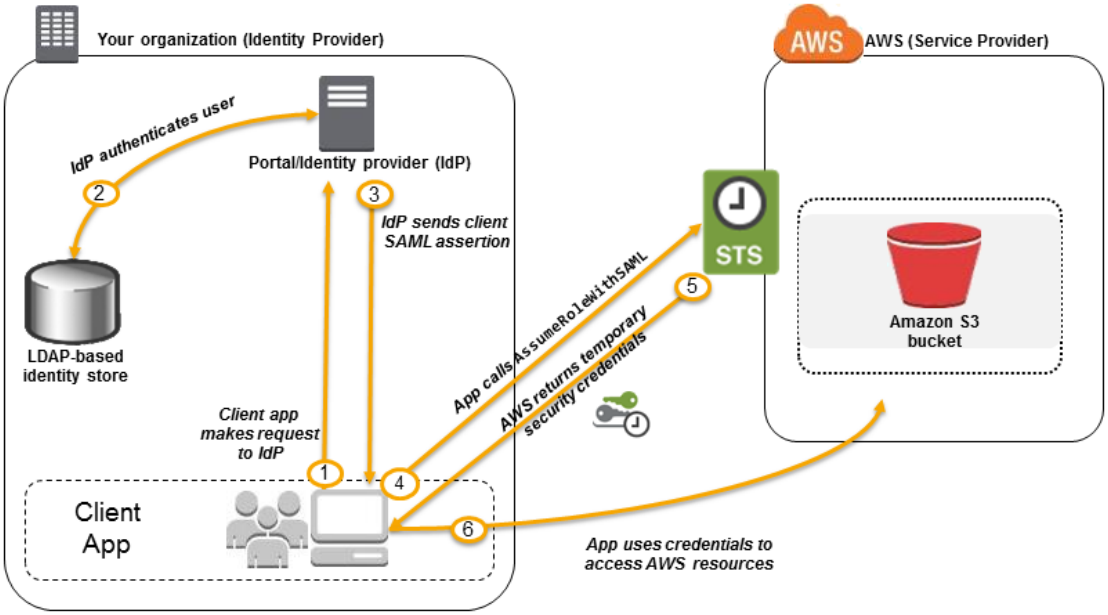
조직의 모든 이에 대해 IAM 사용자를 생성하지 않고도 사용자가 AWS Management 콘솔에 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML을 사용함으로써 AWS로 연동을 구성하는 과정을 단순화할 수 있는데, 이는 사용자 지정 자격 증명 프록시 코드를 작성하는 대신 IdP의 서비스를 사용할 수 있기 때문입니다.

IAM 연동은 다음과 같은 사용 사례를 지원합니다.

- 조직의 사용자 또는 애플리케이션이 AWS API 작업을 호출할 수 있도록 허용하는 연동된 액세스 (p. 189). 조직에서 생성되는 SAML 어설션(인증 응답의 일부)을 사용해 임시 보안 자격 증명을 얻습니다. 이 시나리오는 임시 보안 자격 증명 요청하기 (p. 304) 및 웹 자격 증명 연동에 대하여 (p. 183)에 기술된 것과 같이 IAM이 지원하는 다른 연동 시나리오들과 유사합니다. 그러나 조직의 SAML 2.0–기반 IdP는 인증 수행 및 권한 부여 확인을 위한 런타임에 많은 세부 정보를 처리합니다. 이 주제에서는 이러한 시나리오에 대해 설명합니다.
- 조직에서 AWS Management 콘솔로 이루어지는 웹 기반 SSO(Single Sign-On) (p. 208). SAML 2.0 호환 IdP에서 호스팅하는 조직 내 포털에 사용자가 로그인한 다음 옵션을 선택하여 AWS로 이동하면, 별도의 로그인 정보를 제공하지 않고도 콘솔로 리디렉션됩니다. 타사 SAML IdP를 사용하여 콘솔에 SSO 액세스하거나 사용자 지정 IdP를 만들어 외부 사용자의 콘솔 액세스를 허용할 수 있습니다. 사용자 지정 IdP를 구축하는 방법에 대한 자세한 정보는 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210)를 참조하십시오.

SAML 기반 연동을 이용하여 AWS에 API 액세스

직원들에게 자신의 컴퓨터에서 백업 폴더로 데이터를 복사하는 방법을 제공하려 한다고 가정해 봅시다. 사용자가 컴퓨터에서 실행하는 애플리케이션을 구축합니다. 그 애플리케이션은 백엔드에서 S3 버킷에 있는 객체를 읽고 씁니다. 사용자는 AWS에 직접 액세스할 수 없습니다. 그 대신 다음 프로세스를 사용합니다.



1. 조직 내 사용자가 클라이언트 앱을 사용해 조직의 IdP로부터 인증을 요청합니다.
2. IdP가 조직의 자격 증명 스토어를 이용하여 사용자를 인증합니다.
3. IdP가 사용자에 대한 정보로 SAML 어설션을 만들어 클라이언트 앱으로 보냅니다.
4. 클라이언트 앱이 AWS STS`AssumeRoleWithSAML` API를 호출하면서 SAML 공급자의 ARN, 수임할 역할의 ARN, IdP로부터 받은 SAML 어설션을 전달합니다.
5. 클라이언트 앱에 대한 API 응답에는 임시 보안 자격 증명이 포함되어 있습니다.

6. 클라이언트 앱은 임시 보안 자격 증명을 사용해 Amazon S3 API 작업을 호출합니다.

SAML 2.0 기반 연동에 대한 개요

앞의 시나리오와 다이어그램을 통해 설명한 대로 SAML 2.0 기반 연동을 사용하기 전에, 서로를 신뢰하도록 조직의 IdP와 AWS 계정을 구성해야 합니다. 이 신뢰를 구성하는 일반적인 프로세스는 다음 단계에서 설명합니다. 조직 내에는 Microsoft Active Directory 연동 서비스(AD FS, Windows Server의 일부), Shibboleth 또는 기타 호환 가능한 SAML 2.0 공급자와 같이 SAML 2.0을 지원하는 IdP (p. 201)가 반드시 있어야 합니다.

조직의 IdP와 AWS가 서로 신뢰하도록 구성하는 방법

1. IdP로 AWS를 등록하는 것으로 시작합니다. 조직의 IdP에서 다음 URL에서 얻는 SAML 메타데이터 문서를 사용함으로써 AWS를 서비스 공급자(SP)로 등록합니다.

   ```
   https://signin.aws.amazon.com/static/saml-metadata.xml
   ```
2. 조직의 IdP를 사용해 AWS에서 IdP를 IAM 자격 증명 공급자로 기술하는 동등한 메타데이터 XML 파일을 생성합니다. 그 파일에는 발급자 이름, 생성 일자, 만료 일자 및 AWS가 조직에서 오는 인증 응답의 유효성을 검증하는 데 사용할 수 있는 키가 포함되어 있어야 합니다.
3. IAM 콘솔에서 SAML 자격 증명 공급자 엔터티를 생성합니다. 이 과정의 일부로 Step 2에서 조직의 IdP가 생성한 SAML 메타데이터 문서를 업로드합니다. 자세한 정보는 IAM SAML 자격 증명 공급자 생성 (p. 198)를 참조하십시오.
4. IAM에서 하나 이상의 IAM 역할을 생성합니다. 역할의 신뢰 정책에서 SAML 공급자를 보안 주체로 설정함으로써 조직과 AWS 사이에 신뢰 관계를 설정합니다. 역할의 권한 정책은 조직의 사용자가 AWS에서 하도록 허용된 것을 설정합니다. 자세한 정보는 타사 자격 증명 공급자의 역할 만들기(연동) (p. 238) 단원을 참조하십시오.
5. 조직의 IdP에서 조직 내 사용자 또는 그룹을 IAM 역할로 매핑하는 어설션을 정의합니다. 조직의 다양한 사용자 및 그룹은 서로 다른 IAM 역할에 매핑될 수 있다는 것에 유의하십시오. 매핑 수행을 위한 정확한 절차는 사용하고 있는 IdP에 따라 다릅니다. 사용자를 위한 Amazon S3 폴더의 조기 시나리오 (p. 189)에서는 모든 사용자들이 Amazon S3 권한을 제공하는 동일한 역할에 매핑되는 것이 가능합니다. 자세한 정보는 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오.

   IdP가 AWS 콘솔에 대한 SSO를 지원하는 경우, 콘솔 세션의 최대 지속 기간을 구성할 수 있습니다. 자세한 정보는 SAML 2.0 연동 사용자가 AWS Management 콘솔에 액세스할 수 있게 하기 (p. 208) 단원을 참조하십시오.

   > Note
   >
   > SAML 2.0 연동의 AWS 구현은 IAM 공급자와 AWS 간에 암호화된 SAML 어설션을 지원하지 않습니다. 하지만 고객의 시스템과 AWS 간의 트래픽은 암호화된(TLS) 채널을 통해 전송됩니다.
6. 생성 중인 애플리케이션에서 AWS Security Token Service `AssumeRoleWithSAML` API를 호출해 그것을 Step 3 단계에서 생성한 SAML 공급자의 ARN, Step 4 단계에서 생성한 수임할 역할의 ARN 및 IdP에서 얻는 현재 사용자에 대한 SAML 어설션으로 전달합니다. AWS는 역할 수임 요청이 SAML 공급자에서 참조된 IdP로부터 오는지 확인합니다.

   자세한 정보는 AWS Security Token Service API 참조의 AssumeRoleWithSAML을 참조하십시오.
7. 요청이 성공하면 API는 일련의 임시 보안 자격 증명을 반환하고 애플리케이션은 이를 사용해 AWS에 서명된 요청을 보냅니다. 애플리케이션은 현재 사용자에 대한 정보를 갖고 있어서 이전 시나리오에 기술된 대로 Amazon S3의 사용자별 폴더에 액세스할 수 있습니다.

AWS 리소스에 대한 SAML 연동 액세스를 허용하는 역할에 대한 개요

IAM에서 생성하는 역할 또는 역할들은 조직의 연동 사용자가 AWS에서 하도록 허용되는 것이 무엇인지 정의합니다. 역할에 대한 신뢰 정책을 생성할 때 앞서 생성한 SAML 공급자를 `Principal`로 지정합니다. `Condition`으로 신뢰 정책을 추가로 자세히 살펴봄으로써 특정 SAML 속성과 일치하는 사용자만 그 역할에 액세스하도록 허용할 수 있습니다. 예를 들어 다음 샘플 정책에 설명되어 있듯이 SAML 소속이

staff(https://openidp.feide.no에 의해 어설션되듯이)인 사용자만이 그 역할에 액세스할 수 있도록 지정할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {"Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
ExampleOrgSSOProvider"},
    "Action": "sts:AssumeRoleWithSAML",
    "Condition": {
      "StringEquals": {
        "saml:aud": "https://signin.aws.amazon.com/saml",
        "saml:iss": "https://openidp.feide.no"
      },
      "ForAllValues:StringLike": {"saml:edupersonaffiliation": ["staff"]}
    }
  }]
}
```

정책에서 확인할 수 있는 SAML 키에 대한 자세한 정보는 SAML 기반 AWS STS 연동에 사용할 수 있는 키 (p. 669) 단원을 참조하십시오.

해당 역할의 권한 정책에 대해서는, 역할에 사용하는 방식으로 권한을 지정합니다. 예를 들어 조직의 사용자가 Amazon Elastic Compute Cloud 인스턴스를 관리하도록 허용된다면 AmazonEC2FullAccess 관리형 정책의 작업과 같은 권한 정책의 Amazon EC2 작업을 명시적으로 허용해야 합니다.

SAML 기반 연동에서 사용자를 고유하게 식별하기

IAM에서 액세스 정책을 생성할 때 사용자의 자격 증명에 기반을 두어 권한을 지정할 수 있다는 것은 종종 쓸모가 있습니다. 예를 들어 SAML을 사용해 연동된 사용자들에 대해, 애플리케이션은 다음과 같은 구조를 사용해 Amazon S3에 정보를 저장하고자 할 것입니다.

```
myBucket/app1/user1
myBucket/app1/user2
myBucket/app1/user3
```

버킷과 폴더는 정적 값이므로 Amazon S3 콘솔 또는 AWS CLI를 통해 버킷(myBucket)과 폴더(app1)를 생성할 수 있습니다. 그러나 사용자 고유 폴더(*user1*, *user2*, *user3* 등)는 사용자가 연동 프로세스를 통해 최초로 로그인할 때까지 사용자를 식별하는 값이 알려지지 않기 때문에 코드를 사용해 런타임에 생성되어야 합니다.

사용자 고유의 세부 정보를 리소스 이름의 일부로 참조하는 정책을 작성하려면, 정책 조건에서 사용될 수 있는 SAML 키에서 사용자 자격 증명이 사용 가능해야 합니다. 다음 키는 IAM 정책용 SAML 2.0 기반 연동에 대해 사용 가능합니다. 다음 키가 반환하는 값들을 사용해 Amazon S3 폴더와 같은 리소스에 대한 고유의 사용자 식별자를 생성할 수 있습니다.

- saml:namequalifier. Issuer 반응 값(saml:iss)과 AWS 계정 ID 및 IAM의 SAML 공급자 표시 이름(ARN의 마지막 부분)으로 된 문자열의 연속값에 기반을 둔 해시 값 계정 ID, SAML 공급자 표시 이름의 연속값은 IAM 정책에서 키 saml:doc으로 사용 가능합니다. 계정 ID와 공급자 이름은 "123456789012/provider_name"처럼 '/'로 구분되어야 합니다. 자세한 정보는 saml:doc의 SAML 기반 AWS STS 연동에 사용할 수 있는 키 (p. 669) 키를 참조하십시오.

  NameQualifier와 Subject의 조합은 연동 사용자를 고유한 이름으로 식별하는 데 사용할 수 있습니다. 다음 유사 코드는 이 값이 계산되는 방식을 보여줍니다. 이 유사 코드에서 +는 연결을 나타내고, SHA1는 SHA-1을 사용해 메시지 다이제스트를 생성하는 기능을 나타내며, Base64는 해시 출력의 Base-64 인코딩 버전을 생성하는 기능을 나타냅니다.

  ```
  Base64 ( SHA1 ( "https://example.com/saml" + "123456789012" + "/
  MySAMLIdP" ) )
  ```

SAML 기반 연동에 사용 가능한 정책 키에 대한 자세한 정보는 다음(SAML 기반 AWS STS 연동에 사용할 수 있는 키 (p. 669))을 참조하십시오.

- `saml:sub` (문자열). 이것은 클레임의 주체로서 여기에는 조직 내 사용자 개개인을 식별할 수 있는 고유 값이 포함됩니다(예: `_cbb88bf52c2510eabe00c1642d4643f41430fe25e3`).
- `saml:sub_type` (문자열). 이 키는 `persistent`, `transient`, 또는 SAML 어설션에서 사용되는 `Format` 및 `Subject` 요소의 전체 `NameID` URI일 수 있습니다. `persistent`라는 값은 `saml:sub`의 값이 모든 세션에 걸쳐 사용자에게 동일하다는 것을 나타냅니다. 값이 `transient`인 경우 각 세션마다 사용자의 `saml:sub` 값이 다릅니다. `NameID` 요소의 `Format` 속성에 대한 자세한 정보는 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오.

다음 예는 선행 키를 사용하여 Amazon S3의 사용자 고유 폴더에 대한 권한을 부여하는 권한 정책을 보여줍니다. 그 정책은 `saml:namequalifier` 및 `saml:sub`를 둘 다 포함하는 접두사를 사용해 Amazon S3 객체를 식별하는 것으로 가정합니다. `Condition` 요소에는 `saml:sub_type`이 `persistent`로 설정되어 있는지 확인하는 테스트가 포함되어 있다는 것에 유의하십시오. `transient`로 설정되어 있다면 사용자에 대한 `saml:sub` 값은 각 세션마다 다를 수 있고 값의 조합은 사용자 고유 폴더를 식별하는 데 사용되어서는 안 됩니다.

```
>{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": [
      "arn:aws:s3:::exampleorgBucket/backup/${saml:namequalifier}/${saml:sub}",
      "arn:aws:s3:::exampleorgBucket/backup/${saml:namequalifier}/${saml:sub}/*"
    ],
    "Condition": {"StringEquals": {"saml:sub_type": "persistent"}}
  }
}
```

IdP의 어설션을 정책 키에 매핑하는 것에 대한 자세한 정보는 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오.

IAM 자격 증명 공급자 생성

외부 자격 증명 공급자(IdP) 서비스와의 연동을 구성하려는 경우 IAM 자격 증명 공급자를 생성하여 IdP 및 구성에 대해 AWS에 알려줍니다. 이렇게 하면 AWS 계정과 IdP 사이에 "신뢰"가 설정됩니다. 다음 주제는 각 IdP 유형별로 IAM 자격 증명 공급자를 생성하는 방법에 대해 자세히 설명합니다.

주제

- OpenID Connect(OIDC) 자격 증명 공급자의 생성 (p. 192)
- IAM SAML 자격 증명 공급자 생성 (p. 198)

OpenID Connect(OIDC) 자격 증명 공급자의 생성

IAMOIDC 자격 증명 공급자는 IAM의 엔터티로서 Google이나 Salesforce와 같은 OpenID Connect(OIDC) 표준을 지원하는 자격 증명 공급자(IdP) 서비스를 기술합니다. IAM OIDC 자격 증명 공급자는 OIDC 호환 IdP와 AWS 계정 간에 신뢰를 구축하려 할 때 사용합니다. 예를 들어 AWS 리소스에 액세스하는 데 필요한 모바일 앱이나 웹 애플리케이션을 개발하면서 사용자 지정 로그인 코드를 생성하거나 자신의 사용자 자격 증명을 관리하지 않을 때 유용합니다. 이 시나리오에 대한 자세한 정보는 the section called “웹 자격 증명 연동에 대하여” (p. 183)를 참조하십시오.

AWS Management 콘솔, AWS Command Line Interface, Windows PowerShell용 도구 또는 IAM API를 사용하여 IAM OIDC 자격 증명 공급자를 생성 및 관리할 수 있습니다.

주제

OIDC 공급자의 생성 및 관리(콘솔)

이 지침에 따라 AWS Management 콘솔에서 IAM OIDC 자격 증명 공급자를 생성 및 관리하십시오.

IAM OIDC 자격 증명 공급자를 생성하는 방법(콘솔)

1. IAM OIDC 자격 증명 공급자를 생성하려면 먼저 애플리케이션을 IdP에 등록하여 클라이언트 ID를 받아야 합니다. 클라이언트 ID(사용자라고도 불림)는 앱을 IdP에 등록할 때 발급되는 고유의 앱 식별자입니다. 클라이언트 ID를 얻는 방법에 대한 자세한 정보는 해당 IdP에 대한 설명서를 참조하십시오.
2. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
3. 탐색 창에서 자격 증명 공급자를 선택한 다음 공급자 생성을 선택합니다.
4. 공급자 유형에서 공급자 유형 선택을 선택한 다음 OpenID Connect를 선택합니다.
5. Provider URL(공급자 URL)에서 IdP의 URL을 입력합니다. URL은 다음과 같은 제한을 준수해야 합니다.
   - URL은 대/소문자를 구분합니다.
   - URL은 **`https://`**로 시작해야 합니다.
   - URL은 콜론(:) 문자를 포함할 수 없으므로 포트 번호를 지정할 수 없습니다. 서버가 기본 포트인 443에서 수신 대기해야 함을 의미합니다.
   - IAM OIDC 자격 증명 공급자는 AWS 계정 내에서 고유한 URL을 사용해야 합니다.
6. Audience(대상) 필드에 IdP를 등록하고 Step 1에서 받은 애플리케이션의 클라이언트 ID를 입력하면 AWS에게도 요청됩니다. IdP에 등록한 클라이언트 ID(사용자들이라고도 불림)가 더 있는 경우 나중에 공급자 세부 정보 페이지에서 추가할 수 있습니다. [Next Step]을 선택합니다.
7. Thumbprint(지문)을 사용하여 IdP의 서버 인증서를 확인합니다. 자세한 방법은 OpenID Connect 자격 증명 공급자의 루트 CA 지문 얻기 (p. 195) 단원을 참조하십시오. Create를 선택합니다.
8. 화면 상단에 확인 메시지가 나오면 지금 수행합니다를 클릭하여 역할 탭으로 이동한 후 이 자격 증명 공급자에 사용할 역할을 생성합니다. OIDC 자격 증명 공급자에 사용할 역할 생성에 대한 자세한 정보는 타사 자격 증명 공급자의 역할 만들기(연동) (p. 238) 단원을 참조하십시오. OIDC 자격 증명 공급자가 AWS 계정에 액세스하려면 역할이 필요합니다. 이 단계를 건너뛰고 나중에 역할을 생성하려면 닫기를 선택합니다.

IAM OIDC 자격 증명 공급자에 사용할 지문이나 클라이언트 ID(사용자라고도 함)를 추가 또는 삭제하는 방법(콘솔)

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 자격 증명 공급자를 선택하고 나서 업데이트할 IAM 자격 증명 공급자의 이름을 선택합니다.
3. 지문이나 사용자를 추가하려면 지문 추가 또는 Add an Audience(사용자 추가)를 선택합니다. 지문이나 사용자를 제거하려면 삭제할 항목 옆에 있는 제거를 선택합니다.

   Note

   IAM OIDC 자격 증명 공급자마다 한 개 이상의 지문이 있어야 하며 최대 5개까지 가능합니다. OIDC 자격 증명 공급자마다 한 명 이상의 사용자가 있어야 하며 최대 100명까지 가능합니다.

작업을 마쳤으면 변경 사항 저장을 선택합니다.

IAM OIDC 자격 증명 공급자를 삭제하는 방법(콘솔)

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 자격 증명 공급자를 선택합니다.
3. 삭제할 IAM 자격 증명 공급자 옆의 확인란을 선택합니다.
4. 공급자 삭제를 선택합니다.

IAM OIDC 자격 증명 공급자 생성 및 관리(AWS CLI)

다음 AWS CLI 명령을 사용하여 IAM OIDC 자격 증명 공급자를 생성하고 관리할 수 있습니다.

IAM OIDC 자격 증명 공급자를 생성하는 방법(AWS CLI)

1. (선택 사항) AWS 계정의 전체 IAM OIDC 자격 증명 공급자 목록을 가져오려면 다음 명령을 실행합니다.
   - `aws iam list-open-id-connect-providers`
2. 새 IAM OIDC 자격 증명 공급자를 만들려면 다음 명령을 실행합니다.
   - `aws iam create-open-id-connect-provider`

기존 IAMOIDC 자격 증명 공급자의 서버 인증서 지문 목록을 업데이트하는 방법(AWS CLI)

- IAM OIDC 자격 증명 공급자의 서버 인증서 지문 목록을 업데이트하려면 다음 명령을 실행합니다.
  - `aws iam update-open-id-connect-provider-thumbprint`

기존 IAM OIDC 자격 증명 공급자에서 클라이언트 ID를 추가하거나 제거하는 방법(AWS CLI)

1. (선택 사항) AWS 계정의 전체 IAM OIDC 자격 증명 공급자 목록을 가져오려면 다음 명령을 실행합니다.
   - `aws iam list-open-id-connect-providers`
2. (선택 사항) IAM OIDC 자격 증명 공급자에 대한 자세한 정보를 보려면 다음 명령을 실행합니다.
   - `aws iam get-open-id-connect-provider`
3. 기존 IAM OIDC 자격 증명 공급자에 새로운 클라이언트 ID를 추가하려면 다음 명령을 실행합니다.
   - `aws iam add-client-id-to-open-id-connect-provider`
4. 기존 IAM OIDC 자격 증명 공급자에서 클라이언트를 제거하려면 다음 명령을 실행합니다.
   - `aws iam remove-client-id-from-open-id-connect-provider`

IAM OIDC 자격 증명 공급자를 삭제하는 방법(AWS CLI)

1. (선택 사항) AWS 계정의 전체 IAM OIDC 자격 증명 공급자 목록을 가져오려면 다음 명령을 실행합니다.
   - `aws iam list-open-id-connect-providers`
2. (선택 사항) IAM OIDC 자격 증명 공급자에 대한 자세한 정보를 보려면 다음 명령을 실행합니다.
   - `aws iam get-open-id-connect-provider`
3. IAM OIDC 자격 증명 공급자를 삭제하려면 다음 명령을 실행합니다.

- `aws iam delete-open-id-connect-provider`

OIDC 자격 증명 공급자 만들기 및 관리(AWS API)

다음 IAM API 명령을 사용하여 OIDC 공급자를 만들고 관리할 수 있습니다.

IAM OIDC 자격 증명 공급자를 생성하는 방법(AWS API)

1. (선택 사항) AWS 계정의 전체 IAM OIDC 자격 증명 공급자 목록을 가져오려면 다음 작업을 호출합니다.
   - `ListOpenIDConnectProviders`
2. 새로운 IAM OIDC 자격 증명 공급자를 생성하려면 다음 작업을 호출합니다.
   - `CreateOpenIDConnectProvider`

기존 IAMOIDC 자격 증명 공급자의 서버 인증서 지문 목록을 업데이트하는 방법(AWS API)

- IAM OIDC 자격 증명 공급자의 서버 인증서 지문 목록을 업데이트하려면 다음 작업을 호출합니다.
  - `UpdateOpenIDConnectProviderThumbprint`

기존 IAM OIDC 자격 증명 공급자에서 클라이언트 ID를 추가하거나 제거하는 방법(AWS API)

1. (선택 사항) AWS 계정의 전체 IAM OIDC 자격 증명 공급자 목록을 가져오려면 다음 작업을 호출합니다.
   - `ListOpenIDConnectProviders`
2. (선택 사항) IAM OIDC 자격 증명 공급자에 대한 자세한 정보를 보려면 다음 작업을 호출합니다.
   - `GetOpenIDConnectProvider`
3. 기존 IAM OIDC 자격 증명 공급자에 새로운 클라이언트 ID를 추가하려면 다음 작업을 호출합니다.
   - `AddClientIDToOpenIDConnectProvider`
4. IAM OIDC 자격 증명 공급자에서 클라이언트 ID를 제거하려면 다음 작업을 호출합니다.
   - `RemoveClientIDFromOpenIDConnectProvider`

IAM OIDC 자격 증명 공급자를 삭제하는 방법(AWS API)

1. (선택 사항) AWS 계정의 전체 IAM OIDC 자격 증명 공급자 목록을 가져오려면 다음 작업을 호출합니다.
   - `ListOpenIDConnectProviders`
2. (선택 사항) IAM OIDC 자격 증명 공급자에 대한 자세한 정보를 보려면 다음 작업을 호출합니다.
   - `GetOpenIDConnectProvider`
3. IAM OIDC 자격 증명 공급자를 삭제하려면 다음 작업을 호출합니다.
   - `DeleteOpenIDConnectProvider`

OpenID Connect 자격 증명 공급자의 루트 CA 지문 얻기

IAM에서 OpenID Connect(OIDC) 자격 증명 공급자를 생성 (p. 192)할 때 지문을 제공해야 합니다. IAM에서는 외부 자격 증명 공급자(IdP)가 사용하는 인증서를 서명할 루트 인증 기관(CA)의 지문을 필요로 합니다. 지문은 OIDC 호환 IdP에 대한 인증서 발급에 사용되는 CA에 대한 서명입니다. IAM OIDC 자격 증명 공급자

를 만들 때는 해당 IdP에 의해 인증된 자격 증명에 본인의 AWS 계정에 대한 액세스 권한을 맡깁니다. CA의 인증서 지문을 제공함으로써 등록된 것과 DNS 이름이 동일한 CA에서 발급한 모든 인증서를 신뢰하게 됩니다. 이를 통해 IdP의 서명 인증서를 갱신할 때 각 계정의 신뢰를 업데이트할 필요가 없습니다.

> **Important**
>
> 대부분의 경우 연동 서버는 두 가지 다른 인증서를 사용합니다. 첫 번째는 클라이언트와 연동 엔드포인트 사이의 HTTPS 연결을 설정합니다. 이는 AWS Certificate Manager 등과 같은 퍼블릭 루트 CA에서 안전하게 발급할 수 있습니다. 두 번째는 토큰 서명에 사용됩니다. 프라이빗 CA 사용 시 이를 발급하는 것이 좋습니다.

AWS Command Line Interface, Windows PowerShell용 도구 또는 IAM API (p. 194)를 사용하여 IAM OIDC 자격 증명 공급자를 생성할 수 있습니다. 이러한 방법을 사용하는 경우 수동으로 지문을 얻어서 AWS에 제공해야 합니다. IAM 콘솔 (p. 192)을 사용해 OIDC 자격 증명 공급자를 만들 때 콘솔은 지문을 자동으로 가져오려고 합니다. 또한, 수동으로 OIDC IdP의 지문을 얻어 콘솔에서 올바른 지문을 가져왔는지 확인하는 것이 좋습니다.

웹 브라우저와 OpenSSL 명령줄 도구를 사용하여 OIDC 공급자의 지문을 얻습니다. 자세한 정보는 다음을 참조하십시오.

OIDC IdP의 지문을 얻으려면

1. OIDC IdP의 지문을 얻으려면, 먼저 OpenSSL 명령줄 도구를 얻어야 합니다. 이 도구를 사용하여 OIDC IdP의 인증서 체인을 다운로드하고 인증서 체인에 있는 마지막 인증서의 지문을 생성합니다. OpenSSL을 설치 및 구성해야 하는 경우 OpenSSL 설치 (p. 197) 및 OpenSSL 구성 (p. 198)의 지침을 따르십시오.
2. OIDC IdP의 URL(예: `https://server.example.com`)로 시작한 다음 `/.well-known/openid-configuration`을 추가하여 다음과 같이 OIDC IdP의 구성 문서에 대한 URL을 만듭니다.

   `https://server.example.com/.well-known/openid-configuration`

   웹 브라우저에서 이 URL을 열 때 *`server.example.com`*을 OIDC IdP 서버 이름으로 바꾸어 엽니다.
3. 웹 브라우저에 표시되는 문서에서 `"jwks_uri"`를 찾습니다. 웹 브라우저의 찾기 기능을 사용하여 페이지에서 이 텍스트를 찾을 수 있습니다. `"jwks_uri"`라는 텍스트 바로 뒤에 콜론(:)과 URL이 보일 것입니다. 그 URL의 정규화된 도메인 이름을 복사합니다. `https://` 또는 최상위 도메인 다음에 오는 경로는 포함하지 마십시오.
4. OpenSSL 명령줄 도구를 사용하여 다음 명령을 실행합니다. 이때 *`keys.example.com`*을 Step 3에서 얻은 도메인 이름으로 바꿉니다.

   ```
   openssl s_client -servername keys.example.com -showcerts -connect keys.example.com:443
   ```
5. 명령 창에서 다음 예제와 비슷한 인증서가 보일 때까지 위로 스크롤합니다. 인증서가 2개 이상 있을 경우 명령 출력의 하단에서 표시된 마지막 인증서를 찾습니다. 이는 인증 기관 체인의 루트 CA 인증서가 됩니다.

   ```
   -----BEGIN CERTIFICATE-----
   MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
   VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
   b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
   BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
   MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
   VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
   b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
   YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
   21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
   rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
   Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
   nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
   ```

```
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----
```

인증서를 복사해(`-----BEGIN CERTIFICATE-----` 및 `-----END CERTIFICATE-----` 줄 포함) 텍스트 파일에 붙여 넣습니다. 그 다음에 그 파일을 **`certificate.crt`**라는 이름으로 저장합니다.

6. OpenSSL 명령줄 도구를 사용하여 다음 명령을 실행합니다.

```
openssl x509 -in certificate.crt -fingerprint -noout
```

다음 예제와 비슷한 인증서 지문이 명령 창에 표시됩니다.

```
SHA1 Fingerprint=99:0F:41:93:97:2F:2B:EC:F1:2D:DE:DA:52:37:F9:C9:52:F2:0D:9E
```

이 문자열에서 콜론 문자(:)를 제거하여 다음과 같은 최종 지문을 생성합니다.

```
990F4193972F2BECF12DDEDA5237F9C952F20D9E
```

7. AWS CLI, Windows PowerShell용 도구 또는 IAM API를 사용하여 IAM OIDC 자격 증명 공급자를 만드는 경우 공급자를 만들 때 이 지문을 제공합니다.

   IAM 콘솔에서 IAM OIDC 자격 증명 공급자를 만드는 경우에는 OIDC 공급자를 만들 때 콘솔에서 공급자 정보 확인 페이지에 표시되는 지문과 이 지문을 비교합니다.

   > **Important**
   >
   > 얻은 지문이 콘솔에 표시되는 지문과 일치하지 않을 경우 콘솔에서 OIDC 공급자를 만들어서는 안 됩니다. 대신 잠시 기다렸다가 공급자를 만들기 전에 지문이 일치하는지 확인하며 다시 OIDC 공급자를 만들어 보십시오. 두 번째 시도 후에도 지문이 여전히 일치하지 않을 경우에는 IAM 포럼을 통해 AWS에 문의하십시오.

OpenSSL 설치

아직 OpenSSL을 설치하지 않았다면 이 단원에 나오는 지침을 따르십시오.

Linux 또는 Unix에서 OpenSSL을 설치하려면

1. OpenSSL: Source, Tarballs(https://openssl.org/source/)로 이동합니다.
2. 최신 소스를 다운로드하여 패키지를 생성합니다.

Windows에서 OpenSSL을 설치하려면

1. Windows 버전을 설치할 수 있는 사이트 목록을 보려면 OpenSSL: Binary Distributions(https://wiki.openssl.org/index.php/Binaries)로 이동합니다.
2. 선택한 사이트의 지침을 따라 설치를 시작합니다.
3. Microsoft Visual C++ 2008 재배포 가능 패키지 설치를 묻는 메시지가 표시되고 아직 시스템에 설치되지 않았다면 환경에 적합한 다운로드 링크를 선택합니다. Microsoft Visual C++ 2008 재배포 가능 패키지 설치 마법사의 지시를 따릅니다.

   > **Note**
   >
   > 시스템에 Microsoft Visual C++ 2008 Redistributables가 설치되어 있는지 알 수 없는 경우 OpenSSL을 먼저 설치합니다. Microsoft Visual C++ 2008 Redistributables가 설치되지 않은 경우에는 OpenSSL 설치 관리자에 알림이 표시됩니다. 설치할 OpenSSL 버전에 해당하는 아키텍처(32비트 또는 64비트)를 설치해야 합니다.

4. Microsoft Visual C++ 2008 Redistributables를 설치한 후에는 환경에 맞는 OpenSSL 바이너리를 선택하고 파일을 로컬 위치에 저장합니다. OpenSSL 설치 마법사를 시작합니다.
5. OpenSSL 설치 마법사의 지시에 따릅니다.

OpenSSL 구성

OpenSSL 명령을 사용하려면 OpenSSL이 설치된 위치 정보가 담기도록 운영 체제를 구성해야 합니다.

Linux 또는 Unix에서 OpenSSL을 구성하려면

1. 명령줄에서 `OpenSSL_HOME` 변수를 OpenSSL 설치 위치로 설정합니다.

```
$ export OpenSSL_HOME=path_to_your_OpenSSL_installation
```

2. OpenSSL 설치가 포함되도록 경로를 설정합니다.

```
$ export PATH=$PATH:$OpenSSL_HOME/bin
```

> **Note**
>
> `export` 명령을 사용하여 변경한 환경 변수는 현재 세션에만 유효합니다. 쉘 구성 파일에서 설정하면 환경 변수의 영구 변경이 가능합니다. 자세한 내용은 운영 체제 설명서를 참조하십시오.

Windows에서 OpenSSL을 구성하려면

1. 명령 프롬프트 창을 엽니다.
2. `OpenSSL_HOME` 변수를 OpenSSL 설치 위치로 설정합니다.

```
C:\> set OpenSSL_HOME=path_to_your_OpenSSL_installation
```

3. `OpenSSL_CONF` 변수를 OpenSSL 설치에 있는 구성 파일 위치로 설정합니다.

```
C:\> set OpenSSL_CONF=path_to_your_OpenSSL_installation\bin\openssl.cfg
```

4. OpenSSL 설치가 포함되도록 경로를 설정합니다.

```
C:\> set Path=%Path%;%OpenSSL_HOME%\bin
```

> **Note**
>
> 명령 프롬프트 창에서 변경한 Windows 환경 변수는 현재 명령줄 세션에만 유효합니다. 환경 변수를 시스템 속성으로 설정하면 환경 변수의 영구 변경이 가능합니다. 정확한 절차는 사용 중인 Windows 버전에 따라 달라집니다. 예를 들어, Windows 7에서 제어판, 시스템 및 보안, 시스템을 엽니다. 그런 다음 고급 시스템 설정, 고급 탭, 환경 변수를 선택합니다. 자세한 내용은 Windows 설명서를 참조하십시오.

IAM SAML 자격 증명 공급자 생성

IAM SAML 2.0 자격 증명 공급자는 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 지원하는 외부 자격 증명 공급자(IdP) 서비스를 기술하는 IAM의 엔터티입니다. 조직의 사용자가 AWS 리소스에 액세스할 수 있도록 Shibboleth 또는 Active Directory 연동 서비스와 같은 SAML 호환 IdP와 AWS 간에 신뢰를 구축하고자 할 때 IAM 자격 증명 공급자를 사용합니다. IAM SAML 자격 증명 공급자는 IAM 신뢰 정책에서 보안 주체로 사용됩니다.

이 시나리오에 대한 자세한 정보는 SAML 2.0 기반 연동에 대하여 (p. 188)를 참조하십시오.

AWS Management 콘솔에서 또는 AWS CLI, Windows PowerShell용 도구 또는 AWS API 호출을 사용해 IAM 자격 증명 공급자를 생성하고 관리할 수 있습니다.

SAML 공급자를 생성한 후에는 1개 이상의 IAM 역할을 생성해야 합니다. 역할은 AWS의 자격 증명으로서 자신만의 고유한 자격 증명이 없지만(사용자가 그러하듯이), 이 콘텍스트에서는 조직의 IdP에 의해 인증된 연동 사용자에게 동적으로 할당됩니다. 그 역할은 조직의 IdP가 AWS에 액세스하기 위해 임시 보안 자격 증명을 요청할 수 있도록 허용합니다. 역할에 할당된 정책은 연동 사용자가 AWS에서 하도록 허용된 것이 무엇인지 결정합니다. SAML 연동을 위한 역할을 생성하려면 타사 자격 증명 공급자의 역할 만들기(연동) (p. 238) 단원을 참조하십시오.

마지막으로 역할을 만든 후에는 AWS에 대한 정보와 연동 사용자가 사용하도록 하고 싶은 역할(들)로 IdP를 구성하여 SAML 신뢰를 완료합니다. 이를 가리켜 IdP와 AWS 간 신뢰 당사자 신뢰 구성이라고 합니다. 신뢰 당사자 신뢰를 구성하려면 신뢰 당사자 신뢰로 SAML 2.0 IdP를 구성하고 클레임 추가하기 (p. 201) 단원을 참조하십시오.

주제

IAM 자격 증명 공급자 생성 및 관리(콘솔)

AWS Management 콘솔 콘솔을 사용하여 IAM SAML 자격 증명 공급자를 만들고 삭제할 수 있습니다.

IAM 자격 증명 공급자를 생성하는 방법(콘솔)

1. IAM 자격 증명 공급자를 생성하기 전에 IdP에게서 얻는 SAML 메타데이터 문서가 필요합니다. 이 문서에는 발급자 이름, 만료 정보 및 IdP에서 받은 SAML 인증 응답(어설션)의 유효성을 검증하는 데 사용할 수 있는 키가 포함되어 있습니다. 메타데이터 문서를 생성하려면 조직이 IdP로 사용하는 자격 증명 관리 소프트웨어를 사용하십시오. 필요한 SAML 메타데이터 문서를 생성하는 방법을 비롯해, 사용 가능한 다수의 IdP를 구성하여 AWS에서 작동되도록 하는 방법에 대한 지침은 타사 SAML 솔루션 공급자를 AWS와 통합 (p. 201) 단원을 참조하십시오.

   Important

   메타데이터 파일은 바이트 순서 표시(BOM)가 없는 UTF-8 형식으로 인코딩되어야 합니다. 또한 SAML 메타데이터 문서의 일부로 포함된 x.509 인증서는 1,024비트 이상의 키를 사용해야 합니다. 키 크기가 이보다 작으면 "메타데이터를 구문 분석할 수 없음" 오류로 인해 IdP 생성에 실패합니다. BOM을 제거하려면 Notepad++와 같은 텍스트 편집 도구를 사용해 파일을 UTF-8로 인코딩합니다.
2. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
3. 탐색 창에서 자격 증명 공급자와 공급자 생성을 차례로 클릭합니다.
4. Provider Type(공급자 유형)에서 공급자 유형 선택(Choose a provider type)을 클릭한 다음 SAML을 클릭합니다.
5. 자격 증명 공급자의 이름을 입력합니다.
6. 메타데이터 문서에서 파일 선택을 클릭하고 Step 1에서 다운로드한 SAML 메터데이터 문서를 지정한 다음, 열기를 클릭합니다. [Next Step]을 클릭합니다.
7. 자신이 제공한 정보를 확인하고 생성을 클릭합니다.

SAML 공급자를 삭제하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 자격 증명 공급자를 클릭합니다.
3. 삭제할 자격 증명 공급자 옆의 확인란을 선택합니다.
4. Delete Providers(공급자 삭제)를 클릭합니다.

IAM SAML 자격 증명 공급자 생성 및 관리(AWS CLI)

AWS CLI를 사용하여 SAML 공급자를 만들고 삭제할 수 있습니다.

IAM 자격 증명 공급자를 생성하고 메타데이터 문서를 업로드하는 방법(AWS CLI)

- 다음 명령을 실행합니다. `aws iam create-saml-provider`

IAM 자격 증명 공급자의 새 메타데이터 문서를 업로드하는 방법(AWS CLI)

- 다음 명령을 실행합니다. `aws iam update-saml-provider`

IAM SAML 자격 증명 공급자를 삭제하는 방법(AWS CLI)

1. (선택 사항) ARN, 생성 날짜, 만료 등 모든 공급자에 대한 정보를 나열하려면 다음 명령을 실행합니다.
   - `aws iam list-saml-providers`
2. (선택 사항)ARN, 생성 날짜, 만료 등 특정 공급자에 대한 정보를 얻으려면 다음 명령을 실행합니다.
   - `aws iam get-saml-provider`
3. IAM 자격 증명 공급자를 삭제하려면 다음 명령을 실행합니다.
   - `aws iam delete-saml-provider`

IAM SAML 자격 증명 공급자 만들기 및 관리(AWS API)

AWS API를 사용하여 SAML 공급자를 만들고 삭제할 수 있습니다.

IAM 자격 증명 공급자를 생성하고 메타데이터 문서를 업로드하려면(AWS API)

- 다음 연산을 호출합니다. `CreateSAMLProvider`

IAM 자격 증명 공급자의 새 메타데이터 문서를 업로드하는 방법(AWS API)

- 다음 연산을 호출합니다. `UpdateSAMLProvider`

IAM 자격 증명 공급자를 삭제하는 방법(AWS API)

1. (선택 사항)ARN, 생성 날짜, 만료 등 모든 IdP에 대한 정보를 나열하려면 다음 연산을 호출합니다.
   - `ListSAMLProviders`
2. (선택 사항)ARN, 생성 날짜, 만료 등 특정 공급자에 대한 정보를 얻으려면 다음 연산을 호출합니다.
   - `GetSAMLProvider`
3. IdP를 삭제하려면 다음 연산을 호출합니다.

- `DeleteSAMLProvider`

신뢰 당사자 신뢰로 SAML 2.0 IdP를 구성하고 클레임 추가하기

SAML 액세스를 위한 IAM 자격 증명 공급자 및 역할을 생성한다는 것은 외부 자격 증명 공급자(IdP)와 관련 사용자에게 허용된 작업을 AWS에 알려주는 것입니다. 그 다음 단계는 IdP에게 서비스 공급자인 AWS에 대해 알려주는 것입니다. 이를 가리켜 IdP와 AWS 간 신뢰 당사자 신뢰 추가라고 합니다. 신뢰 당사자 신뢰를 추가하기 위한 정확한 프로세스는 사용 중인 IdP에 따라 달라집니다. 자세한 정보는 자격 증명 관리 소프트웨어의 설명서를 참조하십시오.

오늘날 IdP는 신뢰 당사자 정보와 인증서가 저장된 XML 문서를 IdP가 읽을 수 있도록 URL 지정을 허용하는 곳이 많습니다. AWS의 경우 `https://signin.aws.amazon.com/static/saml-metadata.xml`을 사용할 수 있습니다.

URL을 직접 지정할 수 없는 경우 위 URL에서 XML 문서를 다운로드하여 IdP 소프트웨어로 가져오면 됩니다.

또한, AWS를 신뢰 당사자로 지정하는 IdP에서는 적절한 클레임 규칙을 생성해야 합니다. IdP는 AWS 엔드포인트로 SAML 반응을 전송할 때 1개 이상의 클레임을 포함하는 SAML 어설션을 포함합니다. 클레임은 사용자 및 사용자 소속 그룹에 대한 정보입니다. 클레임 규칙은 그 정보를 SAML 속성에 매핑합니다. 이는 IAM 정책에서 AWS가 연동 사용자의 권한을 검사하는 데 필요한 속성이 IdP의 SAML 인증 응답에 저장되어 있는지 확인하도록 해줍니다. 자세한 정보는 다음 주제 단원을 참조하십시오.

- AWS 리소스에 대한 SAML 연동 액세스를 허용하는 역할에 대한 개요 (p. 190). 이 주제에서는 IAM 정책의 SAML별 키 사용을 비롯해 이 키를 사용하여 SAML 연동 사용자의 권한을 제한하는 방법에 대해 살펴봅니다.
- 인증 응답을 위한 SAML 어설션 구성 (p. 203)를 선택하십시오. 이 주제에서는 사용자에 대한 정보가 포함된 SAML 클레임을 구성하는 방법에 대해 살펴봅니다. 그 클레임은 SAML 어설션에 번들링되어 있으며 AWS로 전동되는 SAML 응답에 포함되어 있습니다. AWS 정책에 필요한 그 정보가 AWS가 인식하고 사용할 수 있는 형식으로 SAML 어설션에 반드시 포함되도록 해야 합니다.
- 타사 SAML 솔루션 공급자를 AWS와 통합 (p. 201). 이 주제에서는 자격 증명 솔루션과 AWS의 통합 방법에 대한 타사의 설명서 링크를 제공합니다.

타사 SAML 솔루션 공급자를 AWS와 통합

다음 링크는 AWS 연동을 처리할 타사 SAML 2.0 자격 증명 공급자(IdP) 솔루션을 구성하는 데 도움이 됩니다.

> **Note**
>
> AWS Support 엔지니어는 타사 소프트웨어를 사용하는 몇 가지 통합 작업과 함께 비즈니스 및 엔터프라이즈 지원 계획이 있는 고객을 지원할 수 있습니다. 지원되는 플랫폼 및 애플리케이션의 최신 목록은 AWS Support FAQ에서 지원되는 타사 소프트웨어는 무엇입니까?를 참조하십시오.

솔루션	추가 정보
Auth0	AWS Integration in Auth0 – Auth0 설명서 웹 사이트의 이 페이지에서는 AWS Management 콘솔에서 SSO(Single Sign-On)를 설정하는 방법을 설명하고 JavaScript 예제를 소개합니다. 세션 태그 (p. 294)를 전달하도록 Auth0을 구성할 수 있습니다. 자세한 내용은 Auth0, IAM 세션 태그용 AWS와의 파트너십 발표단원을 참조하십시오.
Bitium	Configuring SAML for Amazon Web Services(AWS) – Bitium 지원 사이트의 이 문서는 Bitium을 사용하여 AWS를 SAML SSO로 설정하는 방법을 설명합니다.

솔루션	추가 정보
Centrify	Configure Centrify and Use SAML for SSO to AWS – Centrify 웹 사이트의 이 페이지는 Centrify를 구성해 SSO를 위한 SAML을 AWS에 사용하는 방법에 대해 설명합니다.
Clearlogin	Amazon Web Services Setup – Clearlogin 도움말 센터의 이 문서에서는 Clearlogin과 AWS 간에 SSO 기능을 설정하는 방법을 설명합니다.
ForgeRock	ForgeRock Identity Platform이 AWS와 통합됩니다. 세션 태그 (p. 294)를 전달하도록 ForgeRock을 구성할 수 있습니다. 자세한 내용은 Amazon Web Services의 속성 기반 액세스 제어를 참조하십시오.
Google G Suite	Amazon Web Services cloud application – Google G Suite Administrator Help 사이트의 이 문서에서는 G Suite를 SAML 2.0 IdP로 구성하고 AWS를 서비스 공급자로 구성하는 방법을 설명합니다.
IBM	세션 태그 (p. 294)를 전달하도록 IBM을 구성할 수 있습니다. 자세한 내용은 AWS 세션 태그를 지원하는 최초 제품 중 하나인 IBM Cloud Identity IDaaS를 참조하십시오.
Identacor	Configuring SSO (SAML) for AWS – Identacor 웹 사이트의 이 문서에서는 AWS용 SSO를 설정하고 활성화하는 방법을 설명합니다.
Matrix42	MyWorkspace 시작 안내서 - 이 안내서에서는 AWS Identity 서비스를 Matrix42 MyWorkspace와 통합하는 방법에 대해 설명합니다.
Microsoft AD FS(Active Directory Federation Services)	Enabling Federation to AWS Using Windows Active Directory, AD FS, and SAML 2.0 – AWS 보안 블로그의 이 게시물은 EC2 인스턴스에서 AD FS를 설정하고 AWS로 SAML 연동을 활성화하는 방법을 보여줍니다. 세션 태그 (p. 294)를 전달하도록 AD FS를 구성할 수 있습니다. 자세한 내용은 AD FS에서 속성 기반 액세스 제어를 사용하여 IAM 권한 관리 간소화를 참조하십시오. PowerShell Automation to Give AWS Console Access – Sivaprasad Padisetty의 블로그에 실린 이 게시물은 Windows PowerShell을 사용하여 Active Directory 및 AD FS를 설정하는 프로세스를 자동화하는 방법을 설명합니다. 또한 AWS와 SAML 연동 활성화에 대해서도 설명합니다.
miniOrange	SSO for AWS – miniOrange 웹 사이트의 이 페이지에서는 AWS에 대한 대기업 보안 액세스 및 AWS 애플리케이션에 대한 완전한 액세스 제어를 설정하는 방법을 설명합니다.
MIRACL	AWS 내에서 MIRACL Trust SSO를 ID 공급자로 설정 – MIRACL 웹 사이트의 이 페이지에서는 MIRACL Trust SSO SAML을 사용하여 SSO 인증을 위한 AWS 서비스 공급자를 구성하는 방법에 대해 설명합니다.

솔루션	추가 정보
Okta	Okta를 이용한 Amazon Web Services 명령줄 인터페이스 통합 – Okta 지원 사이트의 이 페이지에서는 Okta를 AWS와 함께 사용하도록 구성하는 방법을 알아볼 수 있습니다. 세션 태그 (p. 294)를 전달하도록 Okta를 구성할 수 있습니다. 자세한 내용은 세션 태그를 통해 액세스를 간소화하는 Okta 및 AWS 파트너를 참조하십시오.
OneLogin	OneLogin Knowledgebase에서 **`SAML AWS`**라는 검색어를 입력하여 단일 역할 및 다중 역할 시나리오를 위해 OneLogin과 AWS 사이에 AWS SSO 기능을 설정하는 방법이 설명된 일련의 문서를 찾으십시오. 세션 태그 (p. 294)를 전달하도록 OneLogin을 구성할 수 있습니다. 자세한 내용은 OneLogin 및 세션 태그: AWS 리소스에 대한 속성 기반 액세스 제어를 참조하십시오.
Ping Identity	PingFederate AWS Connector – Single Sign-On(SSO) 및 프로비저닝 연결을 쉽게 설정할 수 있는 빠른 연결 템플릿인 PingFederate AWS Connector에 대한 세부 정보를 봅니다. 설명서를 읽고 AWS와의 통합을 위한 최신 PingFederate AWS Connector를 다운로드합니다. 세션 태그 (p. 294)를 전달하도록 Ping ID를 구성할 수 있습니다. 자세한 내용은 AWS에서 속성 기반 액세스 제어를 위한 Ping Identity 지원 발표를 참조하십시오 .
RadiantLogic	Radiant Logic Technology Partners – Radiant Logic의 RadiantOne 연동 자격 증명 서비스를 AWS와 통합하여 SAML 기반의 SSO를 위한 자격 증명 허브를 구축할 수 있습니다.
RSA	RSA Link는 온라인 커뮤니티를 통해 정보를 공유하고 토론할 수 있습니다. 세션 태그 (p. 294)를 전달하도록 RSA를 구성할 수 있습니다. 자세한 내용은 RSA SecurID 및 세션 태그를 사용하여 AWS에서 ID 액세스 및 보증 의사 결정 간소화를 참조하십시오.
Salesforce.com	How to configure SSO from Salesforce to AWS – Salesforce.com 개발자 사이트에 실린 이 사용 방법 설명서에서는 Salesforce에 IdP(자격 증명 공급자)를 설정하고 AWS를 서비스 공급자로 구성하는 방법을 설명합니다.
SecureAuth	AWS - SecureAuth SAML SSO – SecureAuth 웹 사이트의 이 문서는 SecureAuth 어플라이언스를 위해 SAML과 AWS의 통합을 설정하는 방법을 설명합니다.
Shibboleth	How to Use Shibboleth for SSO to the AWS Management 콘솔 – AWS 보안 블로그의 이 항목에서는 Shibboleth를 설정하고 이를 AWS에 대한 자격 증명 공급자로 구성하는 방법을 단계별로 안내합니다. 세션 태그 (p. 294)를 전달하도록 Shibboleth를 구성할 수 있습니다.

자세한 정보는 AWS 웹 사이트의 IAM Partners 페이지 단원을 참조하십시오.

인증 응답을 위한 SAML 어설션 구성

조직에서 한 사용자의 자격 증명이 확인된 후에 외부 자격 증명 공급자(IdP)는 인증 응답을 `https://signin.aws.amazon.com/saml`의 AWS SAML 엔드포인트로 보냅니다. 이 응답은 SAML 2.0을 위한 HTTP POST 바인딩 표준을 준수하고 다음 요소 또는 클레임이 저장된 SAML 토큰을 포함하는 POST 요청입니다. SAML 호환 IdP에서 이 클레임들을 구성합니다. 이 클레임들을 입력하는 방법에 대한 지침에 대해서는 귀하의 IdP를 위한 문서를 참고하십시오.

IdP가 AWS에 클레임이 포함된 리소스를 전송하는 경우 수신 클레임 중 다수가 AWS 콘텍스트 키에 매핑됩니다. 이러한 콘텍스트 키는 `Condition` 요소를 사용하여 IAM 정책에서 확인할 수 있습니다. 사용 가능한 매핑 목록은 SAML 속성을 AWS 신뢰 정책 콘텍스트 키에 매핑 (p. 206) 섹션에 나와 있습니다.

`Subject` 및 `NameID`

다음 발췌문은 한 가지 예를 보여줍니다. 자신의 값을 표시된 것으로 대치합니다. `SubjectConfirmation` 속성과 `SubjectConfirmationData` 속성을 둘 다 포함하는 `NotOnOrAfter` 요소와 함께 정확하게 `Recipient` 요소가 하나 있어야 합니다. 이러한 속성에는 다음 예제에서처럼 AWS 엔드포인트(`https://signin.aws.amazon.com/saml`)와 일치해야 하는 값이 포함되어 있습니다. Single Sign-On 상호 작용에 지원되는 이름 식별자 형식에 대한 자세한 정보는 Oracle Sun OpenSSO Enterprise Administration Reference 단원을 참조하십시오.

```
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">_cbb88bf52c2510eabe00c1642d4643f41430fe25e3</NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData NotOnOrAfter="2013-11-05T02:06:42.876Z" Recipient="https://
signin.&home-domain;/saml"/>
  </SubjectConfirmation>
</Subject>
```

`AudienceRestriction` 및 `Audience`

보안상의 이유로 AWS는 IdP가 AWS로 보낸다는 SAML 어설션에서 대상으로 포함되어야 합니다. `Audience` 요소의 값에 대해 `https://signin.aws.amazon.com/saml` 또는 `urn:amazon:webservices`를 지정합니다. SAML 어설션의 다음 샘플 XML 조각은 이 키가 어떻게 IdP에 의해 지정되는지 보여줍니다. 사용 사례에 적용되는 샘플을 포함합니다.

```
<Conditions>
  <AudienceRestriction>
    <Audience>https://signin.&home-domain;/saml</Audience>
  </AudienceRestriction>
</Conditions>
```

```
<Conditions>
  <AudienceRestriction>
    <Audience>urn:amazon:webservices</Audience>
  </AudienceRestriction>
</Conditions>
```

Important

IdP의 SAML 어설션에 있는 SAML `AudienceRestriction` 값은 IAM 정책에서 테스트할 수 있는 `saml:aud` 콘텍스트 키에 매핑되지 않습니다. 그 대신에 `saml:aud` 콘텍스트 키는 SAML 수신자 속성에서 온 것으로, 그 이유는 이 속성이 `accounts.google.com:aud`와 같은 OIDC 대상 필드와 동일한 SAML이기 때문입니다.

SAML Role `Attribute`

`Name` 속성이 `https://aws.amazon.com/SAML/Attributes/Role`로 설정된 `Attribute` 요소를 사용할 수 있습니다. 이 요소는 IdP에 의해 사용자가 매핑되는 IAM 자격 증명 공급자 및 역할을 나열하는 `AttributeValue` 요소를 한 개 이상 포함합니다. IAM 역할과 IAM 자격 증명 공급자는 AssumeRoleWithSAML로 전달되는 `RoleArn` 및 `PrincipalArn` 파라미터와 동일한 형식의 쉼표로 구분된 ARN 페어로 지정됩니다. 이 요소는 하나 이상의 역할 공급자 페어(`AttributeValue` 요소)를 포함해야 하며 여러 페어를 포함할 수 있습니다. 요소가 다수의 페어를 포함하는 경우 사용자가 WebSSO를 사용하여 AWS Management 콘솔에 로그인할 때 어떤 역할을 맡을지 선택하라는 메시지가 표시됩니다.

Important

Name 태그의 Attribute 속성 값은 대/소문자를 구분합니다. 정확하게 https://aws.amazon.com/SAML/Attributes/Role로 설정해야 합니다.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/Role">
  <AttributeValue>arn:aws:iam::account-number:role/role-name1,arn:aws:iam::account-number:saml-provider/provider-name</AttributeValue>
  <AttributeValue>arn:aws:iam::account-number:role/role-name2,arn:aws:iam::account-number:saml-provider/provider-name</AttributeValue>
  <AttributeValue>arn:aws:iam::account-number:role/role-name3,arn:aws:iam::account-number:saml-provider/provider-name</AttributeValue>
</Attribute>
```

SAML RoleSessionName Attribute

Name 속성이 https://aws.amazon.com/SAML/Attributes/RoleSessionName으로 설정된 Attribute 요소를 사용할 수 있습니다. 이 요소에는 SSO를 위해 발급된 AWS 임시 자격 증명에 식별자를 제공하는 AttributeValue 요소가 하나 포함되어 있습니다. 이 요소는 AWS Management 콘솔 콘솔에서 사용자 정보를 표시하는 데 사용됩니다. AttributeValue 요소 값은 길이가 2~64자여야 하며 영숫자, 밑줄 및 다음 문자만 포함할 수 있습니다. +(더하기 기호), =(등호), ,(쉼표), .(마침표), @(at 기호), -(하이픈). 공백은 포함할 수 없습니다. 값은 일반적으로 사용자 ID(johndoe) 또는 이메일 주소(johndoe@example.com)입니다. 사용자의 표시 이름(John Doe)과 같이 값이 공백을 포함하면 안 됩니다.

Important

Name 태그의 Attribute 속성 값은 대/소문자를 구분합니다. 정확하게 https://aws.amazon.com/SAML/Attributes/RoleSessionName로 설정해야 합니다.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/RoleSessionName">
  <AttributeValue>user-id-name</AttributeValue>
</Attribute>
```

SAML SessionDuration Attribute

(선택 사항) Name 속성이 https://aws.amazon.com/SAML/Attributes/SessionDuration"로 설정된 Attribute 요소를 사용할 수 있습니다. 이 요소에는 사용자가 AWS Management 콘솔에 액세스할 수 있는 기간을 지정하는 AttributeValue 요소가 한 개 포함되어 있습니다. 이 시간이 지나면 새로운 임시 자격 증명을 요청해야 합니다. 이 값은 세션에 대한 기간(초)을 나타내는 정수입니다. 이 값은 900초(15분)~43200초(12시간)일 수 있습니다. 이 속성이 없으면 자격 증명은 한 시간 동안 지속됩니다(DurationSeconds API의 AssumeRoleWithSAML 파라미터 기본값).

이 속성을 사용하려면 https://signin.aws.amazon.com/saml에서 콘솔 로그인 웹 엔드포인트를 통해 AWS Management 콘솔에 대한 SSO(Single Sign-On) 액세스를 제공하도록 SAML 공급자를 구성해야 합니다. 이 속성은 AWS Management 콘솔에 대해서만 세션을 연장할 수 있습니다. 다른 자격 증명의 수명을 늘릴 수는 없습니다. 그러나 AssumeRoleWithSAML API 호출에 존재하는 경우 세션 기간을 단축하는 데 사용할 수 있습니다. 호출에 의해 반환되는 자격 증명의 기본 수명은 60분입니다.

이와 함께 SessionNotOnOrAfter 속성도 정의되어 있다면 SessionDuration 또는 SessionNotOnOrAfter 속성 중 더 작은 값으로 콘솔 세션의 최대 지속 시간을 정합니다.

지속 기간을 더 늘려 콘솔 세션을 활성화하면 자격 증명이 손상될 위험이 높아집니다. 이러한 위험을 줄이려면 IAM 콘솔의 Role Summary(역할 요약) 페이지에서 Revoke Sessions(세션 취소)를 선택하여 원하는 역할의 활성 콘솔 세션을 즉시 비활성화하면 됩니다. 자세한 정보는 IAM 역할의 임시 보안 자격 증명 취소 (p. 273) 단원을 참조하십시오.

Important

Name 태그의 Attribute 속성 값은 대/소문자를 구분합니다. 정확하게 https://aws.amazon.com/SAML/Attributes/SessionDuration로 설정해야 합니다.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/SessionDuration">
  <AttributeValue>1800</AttributeValue>
</Attribute>
```

SAML PrincipalTag Attribute

(선택 사항) Name 속성이 https://aws.amazon.com/SAML/Attributes/PrincipalTag:*{TagKey}*로 설정된 Attribute 요소를 사용할 수 있습니다. 이 요소를 사용하면 속성을 SAML 어설션에 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 AttributeValue 요소를 포함합니다. 예를 들어, 태그 키-값 페어 Project = Marketing 및 CostCenter = 12345를 전달하려면 다음 속성을 사용합니다. 각 태그에 대해 별도의 Attribute 요소를 포함합니다.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:Project">
  <AttributeValue>Marketing</AttributeValue>
</Attribute>
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:CostCenter">
  <AttributeValue>12345</AttributeValue>
</Attribute>
```

위의 태그를 전이적으로 설정하려면 Name 속성이 https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys로 설정된 다른 Attribute 요소를 포함합니다. 세션 태그를 전이적으로 설정하는 선택적 다중 값 속성입니다. 전이적 태그는 SAML 세션을 사용하여 AWS에서 다른 역할을 맡을 때 유지됩니다. 이를 역할 체인 (p. 176)이라고 합니다. 예를 들어, Principal 및 CostCenter 태그를 전이적으로 설정하려면 다음 속성을 사용하여 키를 지정합니다.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>Project</AttributeValue>
  <AttributeValue>CostCenter</AttributeValue>
</Attribute>
```

SAML 속성을 AWS 신뢰 정책 콘텍스트 키에 매핑

이 섹션의 표들은 흔히 사용되는 SAML 속성들을 나열하고, 그 속성들이 AWS에서 신뢰 정책 조건 콘텍스트 키에 어떻게 매핑되는지 보여줍니다. 이러한 키를 사용하여 역할에 대한 액세스를 제어할 수 있습니다. 이렇게 하려면 키를 SAML 액세스 요청과 함께 제공되는 어설션에 포함된 값과 비교합니다.

> **Important**
>
> 이런 키는 IAM 신뢰 정책(역할을 수임할 수 있는 사용자를 결정하는 정책)에서만 사용할 수 있고, 권한 정책에는 적용할 수 없습니다.

eduPerson 및 eduOrg 속성 표에서 값은 문자열 또는 문자열 목록의 형태로 입력됩니다. 문자열 값의 경우, StringEquals 또는 StringLike 조건을 이용해 IAM 신뢰 정책에서 이러한 값을 테스트할 수 있습니다. 문자열 목록이 포함된 값의 경우에는 ForAnyValue 및 ForAllValues 정책 설정 연산자 (p. 608)를 사용해 신뢰 정책에서 값을 테스트합니다.

> **Note**
>
> AWS 콘텍스트 키당 하나의 클레임만을 포함해야 합니다. 하나 이상의 클레임을 포함하는 경우, 하나의 클레임만 매핑됩니다.

eduPerson 및 eduOrg 속성

eduPerson 또는 eduOrg 속성(**`Name`** 키)	이 AWS 컨텍스트 키(**`FriendlyName`** 키)에 대한 매핑	Type
`urn:oid:1.3.6.1.4.1.5923.1.1.1.1`	`eduPersonAffiliation`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.1.1.2`	`eduPersonNickname`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.1.1.3`	`eduPersonOrgDN`	문자열
`urn:oid:1.3.6.1.4.1.5923.1.1.1.4`	`eduPersonOrgUnitDN`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.1.1.5`	`eduPersonPrimaryAffiliation`	문자열
`urn:oid:1.3.6.1.4.1.5923.1.1.1.6`	`eduPersonPrincipalName`	문자열
`urn:oid:1.3.6.1.4.1.5923.1.1.1.7`	`eduPersonEntitlement`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.1.1.8`	`eduPersonPrimaryOrgUnitDN`	문자열
`urn:oid:1.3.6.1.4.1.5923.1.1.1.9`	`eduPersonScopedAffiliation`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.1.1.10`	`eduPersonTargetedID`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.1.1.11`	`eduPersonAssurance`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.2.1.2`	`eduOrgHomePageURI`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.2.1.3`	`eduOrgIdentityAuthNPolicyURI`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.2.1.4`	`eduOrgLegalName`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.2.1.5`	`eduOrgSuperiorURI`	문자열 목록
`urn:oid:1.3.6.1.4.1.5923.1.2.1.6`	`eduOrgWhitePagesURI`	문자열 목록
`urn:oid:2.5.4.3`	`cn`	문자열 목록

Active Directory 속성

AD 속성	이 AWS 컨텍스트 키에 대한 매핑	Type
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`	`name`	문자열
`http://schemas.xmlsoap.org/claims/CommonName`	`commonName`	문자열
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`	`givenName`	문자열
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`	`surname`	문자열
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`	`mail`	문자열

AD 속성	이 AWS 컨텍스트 키에 대한 매핑	Type
`http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid`	`uid`	문자열

X.500 속성

X.500 속성	이 AWS 컨텍스트 키에 대한 매핑	Type
`2.5.4.3`	`commonName`	문자열
`2.5.4.4`	`surname`	문자열
`2.4.5.42`	`givenName`	문자열
`2.5.4.45`	`x500UniqueIdentifier`	문자열
`0.9.2342.19200300100.1.1`	`uid`	문자열
`0.9.2342.19200300100.1.3`	`mail`	문자열
`0.9.2342.19200300.100.1.45`	`organizationStatus`	문자열

SAML 2.0 연동 사용자가 AWS Management 콘솔에 액세스할 수 있게 하기

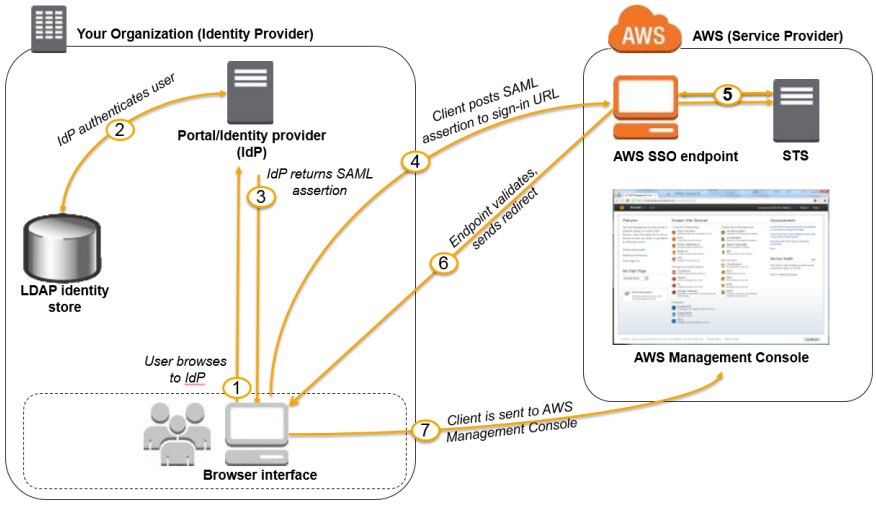
역할을 사용해 SAML 2.0 호환 자격 증명 공급자(IdP) 및 AWS를 구성하여 연동 사용자가 AWS Management 콘솔에 액세스하도록 허용할 수 있습니다. 역할은 콘솔에서 작업을 수행할 수 있는 권한을 사용자에게 부여합니다. SAML 연동 사용자가 다른 방법으로 AWS에 액세스할 수 있게 하려면 다음 주제 중 하나를 참조하십시오.

- AWS CLI: IAM 역할로 전환하기(AWS CLI) (p. 258)
- Windows PowerShell용 도구: IAM 역할로 전환하기(Windows PowerShell용 도구) (p. 262)
- AWS API: IAM 역할(AWS API)로 전환하기 (p. 263)

개요

다음 다이어그램은 SAML 지원 Single Sign-On의 흐름을 보여줍니다.

> **Note**
>
> 이와 같은 SAML의 특수한 사용이 SAML 2.0 기반 연동에 대하여 (p. 188)에 설명된 더 일반적인 사용과 차이가 나는 이유는, 이 워크플로우가 사용자를 대신해 AWS Management 콘솔을 열기 때문입니다. 이를 위해서는 `AssumeRoleWithSAML` API를 직접 호출하는 대신 AWS SSO 엔드포인트를 사용해야 합니다. 엔드포인트는 사용자를 위해 API를 호출하고 사용자의 브라우저를 AWS Management 콘솔로 자동 리디렉션하는 URL을 반환합니다.



다이어그램은 다음 단계들을 보여줍니다.

1. 사용자는 검색을 통해 조직의 포털에 이르러 옵션을 선택해 AWS Management 콘솔로 갑니다. 조직에서 포털은 일반적으로, 조직과 AWS 간의 신뢰 교환을 다루는 IdP의 기능을 담당합니다. 예를 들어 Active Directory Federation Services에서 포털 URL은 `https://ADFSServiceName/adfs/ls/IdpInitiatedSignOn.aspx`입니다.
2. 포털은 사용자의 조직 내 자격 증명을 확인합니다.
3. 포털은 사용자를 식별하고 사용자에 대한 속성을 포함하는 어설션이 포함된 SAML 인증 응답을 생성합니다. 콘솔 세션의 유효 기간을 지정하는 `SessionDuration`이라는 SAML 어설션 속성을 포함하여 IdP를 구성할 수도 있습니다. 속성을 세션 태그 (p. 294)로 전달하도록 IdP를 구성할 수도 있습니다. 포털은 이 응답을 클라이언트 브라우저로 전송합니다.
4. 클라이언트 브라우저는 AWS Single Sign-On 엔드포인트로 리디렉션되고 SAML 어설션을 게시합니다.
5. 엔드포인트는 사용자 대신 임시 보안 자격 증명을 요청하고 그 자격 증명을 사용하는 콘솔 로그인 URL을 생성합니다.
6. AWS는 리디렉션으로 클라이언트에게 로그인 URL을 반송합니다.
7. 클라이언트 브라우저는 AWS Management 콘솔로 리디렉션됩니다. SAML 인증 응답이 여러 개의 IAM 역할에 매핑되는 속성을 포함하는 경우 사용자는 콘솔에 액세스하는 데 사용할 역할을 선택하라는 메시지를 먼저 받습니다.

사용자의 시점에서는 그 과정을 투명하게 들여다볼 수 있습니다. 사용자는 조직의 내부 포털에서 시작하여 AWS 자격 증명을 제공할 필요 없이 AWS Management 콘솔에서 마칩니다.

세부 단계들에 대한 링크를 따라 이 행동을 구성하는 방법을 개관하시려면 다음 섹션들을 참조하십시오.

AWS에 대한 SAML 공급자로 네트워크 구성하기

귀하의 조직 네트워크의 내부에서 자격 증명 스토어(Windows Active Directory 등)를 구성해 Windows Active Directory Federation Services, Shibboleth와 같은 SAML 기반 IdP로 작업합니다. IdP를 사용하여 귀하의 조직을 IdP로 기술하고 인증 키를 포함하는 메타데이터 문서를 생성합니다. 또한 조직의 포털을 구성해, AWS Management 콘솔에 대한 사용자 요청을 SAML 어설션을 이용한 인증을 위해 AWS SAML 엔드포인트로 라우팅합니다. metadata.xml 파일을 생성하기 위해 IdP를 어떻게 구성하는가는 IdP에 따라 다릅니다. 지침을 보시려면 IdP의 문서를 참고하시거나 지원되는 SAML 공급자들 중 다수의 웹 문서 링크가 있는 타사 SAML 솔루션 공급자를 AWS와 통합 (p. 201)를 참조하십시오.

IAM에서 SAML 공급자 생성하기

그 다음에는 AWS Management 콘솔에 로그인하여 IAM 콘솔로 이동합니다. 그곳에서 새로운 SAML 공급자를 생성합니다. 그 공급자는 조직의 Idp에 대한 정보를 담고 있는 IAM의 엔터티입니다. 이 과정의 일부로 이

전 섹션에서 조직의 IdP 소프트웨어가 생성한 메타데이터 문서를 업로드합니다. 자세한 정보는 IAM SAML 자격 증명 공급자 생성 (p. 198) 단원을 참조하십시오.

연동된 사용자들을 위해 AWS에서 권한 구성하기

그 다음 단계는 조직의 IdP와 IAM 간에 신뢰 관계를 수립하는 IAM 역할을 생성하는 것입니다. 이 역할은 연동을 위해 IdP를 보안 주체(신뢰할 수 있는 엔터티)로 식별해야 합니다. 그 역할은 조직의 IdP에 의해 인증된 사용자들이 AWS에서 할 수 있도록 허용되는 것이 무엇인지 정의하기도 합니다. IAM 콘솔을 사용하여 이 역할을 생성할 수 있습니다. 역할을 맡을 수 있는 사용자를 나타내는 신뢰 정책을 생성할 때 이전에 IAM에서 생성한 SAML 공급자를 지정합니다. 또한 역할을 맡을 수 있도록 사용자가 일치해야 하는 SAML 속성을 하나 이상 지정합니다. 예를 들어 SAML `eduPersonOrgDN` 값이 `ExampleOrg`인 사용자에게만 로그인을 허용하도록 구성할 수 있습니다. 그 역할 마법사는 조건을 자동으로 추가해 `saml:aud` 속성을 테스트함으로써 그 역할이 AWS Management 콘솔에 로그인하는 것을 위해서만 위임되는 것인지 확인합니다. 그 역할을 위한 신뢰 정책은 다음과 같을 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {"Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
ExampleOrgSSOProvider"},
    "Action": "sts:AssumeRoleWithSAML",
    "Condition": {"StringEquals": {
      "saml:edupersonorgdn": "ExampleOrg",
      "saml:aud": "https://signin.aws.amazon.com/saml"
    }}
  }]
}
```

역할의 권한 정책 (p. 349)에 대해 어떤 역할, 사용자, 또는 그룹에 사용하는 방식으로 권한을 지정합니다. 예를 들어, 조직의 사용자가 Amazon EC2 인스턴스를 관리하도록 허용될 경우 권한 정책에서 명시적으로 Amazon EC2 작업을 허용합니다. 이것은 Amazon EC2 전체 액세스 관리형 정책과 같은 관리형 정책 (p. 450)을 배정함으로써 할 수 있습니다.

SAML IdP를 위한 역할 생성에 관한 자세한 정보는 SAML 2.0 연동을 위한 역할 생성(콘솔) (p. 244)을 참조하십시오.

구성 완료 및 SAML 어설션 생성

역할을 생성한 후에는 https://signin.aws.amazon.com/static/saml-metadata.xml에 있는 `saml-metadata.xml` 파일을 설치하여 SAML IdP에게 서비스 공급자가 AWS라고 알려주십시오. 그 파일의 설치 방법은 IdP에 따라 다릅니다. 어떤 IdP는 URL을 입력할 수 있는 옵션을 제공하고, 그 결과 IdP가 그 파일을 획득하고 설치해 줍니다. 다른 IdP들의 경우에는 URL에서 파일을 내려받은 다음 로컬 파일로 제공해야 합니다. 세부 정보를 보시려면 IdP의 문서를 참고하시거나 지원되는 SAML 공급자들 중 다수의 웹 문서 링크가 있는 타사 SAML 솔루션 공급자를 AWS와 통합 (p. 201)를 참조하십시오.

또한, IdP가 인증 응답의 일부로 AWS에 SAML 속성으로 전달하기 원하는 정보를 구성합니다. 이 정보의 대부분은 정책에서 평가할 수 있는 조건 컨텍스트 키로 AWS에 나타납니다. 이러한 조건 키를 사용하면 올바른 컨텍스트의 승인된 사용자에게만 AWS 리소스에 액세스할 수 있는 권한이 부여됩니다. 콘솔을 사용할 수 있는 시간을 제한하는 시간 창을 지정할 수 있습니다. 또한 사용자가 콘솔에 액세스할 수 있는 최대 시간(최대 12시간)을 지정할 수 있습니다. 사용자는 이 시간 이후에 자신의 자격 증명을 새로 고쳐야 합니다. 자세한 정보는 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오.

사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기

코드를 작성하고 실행해 조직 네트워크에 로그인하는 사용자가 AWS Management 콘솔에 안전하게 액세스할 수 있게 하는 URL을 생성할 수 있습니다. 그 URL에는 AWS에서 얻고 AWS에 사용자를 인증하는 로그인 토큰이 포함되어 있습니다.

Note

조직에서 SAML과 호환이 되는 자격 증명 공급자(IdP)를 사용한다면, 코드를 작성하지 않고도 콘솔에 대한 액세스를 설정할 수 있습니다. 이는 Microsoft의 Active Directory Federation Services 또는 오픈 소스 Shibboleth와 같은 공급자와 함께 작동합니다. 자세한 정보는 SAML 2.0 연동 사용자가 AWS Management 콘솔에 액세스할 수 있게 하기 (p. 208) 단원을 참조하십시오.

조직의 사용자가 AWS Management 콘솔에 액세스할 수 있도록 하려는 경우 다음 단계를 수행하여 사용자 지정 자격 증명 브로커를 생성할 수 있습니다.

1. 사용자가 로컬 자격 증명 시스템에 의해 인증되는지 확인합니다.
2. AWS Security Token Service(AWS STS) AssumeRole(권장) 또는 GetFederationToken API 작업을 호출하여 사용자를 위한 임시 보안 자격 증명을 얻을 수 있습니다. 역할을 수임하는 데 사용할 수 있는 여러 방법을 알아보려면 IAM 역할 사용 (p. 250) 단원을 참조하십시오. 보안 자격 증명을 획득할 때 선택적 세션 태그를 전달하는 방법은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.
   - 역할에 대한 임시 보안 자격 증명을 얻기 위해 `AssumeRole*` API 작업 중 하나를 사용한 경우 이 호출에는 `DurationSeconds` 파라미터를 포함할 수 있습니다. 이 파라미터는 역할 세션 기간을 900초(15초)에서 해당 역할에 대한 최대 세션 기간 설정까지 지정합니다. 역할에 대한 최댓값을 확인 또는 변경하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오. 또한 `AssumeRole*` API 작업을 사용하는 경우 장기 자격 증명을 사용하여 IAM 사용자로 호출해야 합니다. 그렇지 않으면 3단계의 연동 엔드포인트 호출에 실패합니다.
   - 보안 자격 증명을 얻기 위해 `GetFederationToken` API 작업을 사용한 경우 이 호출에는 `DurationSeconds` 파라미터를 포함할 수 있습니다. 이 파라미터는 역할 세션에 대한 기간을 지정합니다. 이 값은 900초(15분)~129,600초(36시간)일 수 있습니다. IAM 사용자에 대한 장기 AWS 보안 자격 증명을 사용하는 경우에만 이 API를 호출할 수 있습니다. AWS 계정 루트 사용자 자격 증명을 사용하여 호출할 수도 있지만 권장되는 방법은 아닙니다. 루트 사용자로 호출한 경우 기본 세션은 한 시간 동안 지속됩니다. 또는 900초(15분)에서 최대 3,600초(1시간)로 세션을 지정할 수 있습니다.
3. AWS 연동 엔드포인트를 호출하고 임시 보안 자격 증명을 제공하여 로그인 토큰을 요청하십시오.
4. 토큰을 포함하는 콘솔에 대한 URL을 생성합니다:
   - URL에 `AssumeRole*` API 작업 중 하나를 사용하는 경우 `SessionDuration` HTTP 파라미터를 포함할 수 있습니다. 이 파라미터는 콘솔 세션 시간을 900초(15분)~43200초(12시간)로 지정합니다.
   - URL에 `GetFederationToken` API 작업을 사용하는 경우 `DurationSeconds` 파라미터를 포함할 수 있습니다. 이 파라미터는 연동된 콘솔 세션에 대한 기간을 지정합니다. 이 값은 900초(15분)~129,600초(36시간)일 수 있습니다.

     Note

     `SessionDuration`을 사용하여 임시 자격 증명을 얻을 경우에는 `GetFederationToken` HTTP 파라미터를 사용하지 마십시오. 이 파라미터를 사용하면 작업이 실패합니다.
5. 사용자에게 URL을 부여하거나 사용자 대신 URL을 호출합니다.

연동 엔드포인트가 제공하는 URL은 생성된 후 15분 동안 유효합니다. 이 시간은 URL과 연결된 임시 보안 자격 증명 세션의 기간(초)과 다릅니다. 이러한 자격 증명은 생성된 시각을 시작으로 생성 시 지정한 기간 동안 유효합니다.

Important

URL은 연결된 임시 보안 자격 증명에서 권한을 허용한 경우 AWS Management 콘솔을 통해 AWS 리소스에 대한 액세스 권한을 부여한다는 것에 유의하십시오. 이러한 이유 때문에 URL은 비밀로 취급해야 합니다. 예를 들어 SSL 연결을 통해 302 HTTP 응답 상태 코드를 사용함으로써 안전한 리디렉션을 통해 URL을 반환하는 것이 좋습니다. 302 HTTP 응답 상태 코드에 대한 자세한 정보는 RFC 2616, 단원 10.3.3을 참조하십시오.

Single Sign-On 솔루션을 실행하는 방법을 보여주는 샘플 애플리케이션을 보려면 AWS 샘플 코드 및 라이브러리의 AWS Management 콘솔 연동 프록시 샘플 사용 사례를 참조하십시오.

이 작업을 완료하려면 AWS Identity and Access Management를 위한 HTTPS 쿼리 API(IAM) 및 AWS Security Token Service(AWS STS)를 참조하십시오. 아니면 적절한 AWS SDK와 함께 Java, Ruby 또는 C# 과 같은 프로그래밍 언어를 사용할 수도 있습니다. 다음 단원에서는 이들 각 메서드에 대해 설명합니다.

주제

IAM 쿼리 API 작업을 사용한 예제 코드

연동 사용자에게 AWS Management 콘솔에 대한 직접 액세스를 부여하는 URL을 생성할 수 있습니다. 이 작업은 IAM 및 AWS STS HTTPS Query API를 사용합니다. 쿼리 요청에 대한 자세한 정보는 쿼리 요청 실행 단원을 참조하십시오.

> **Note**
>
> 다음 절차에는 텍스트 문자열에 대한 예시가 있습니다. 가독성을 증진하기 위해 일부 긴 예시에는 줄 바꿈이 추가되었습니다. 자신만이 쓸 용도로 이러한 문자열을 생성할 때는 줄 바꿈을 모두 빼야 합니다.

AWS Management 콘솔에서 연동 사용자에게 리소스 액세스 권한을 부여하려면

1. 자격 증명 및 인증 시스템에서 사용자를 인증합니다.
2. 사용자에 대한 임시 보안 자격 증명을 얻습니다. 임시 자격 증명은 액세스 키 ID, 보안 액세스 키 및 보안 토큰으로 구성됩니다. 임시 자격 증명 생성에 대한 자세한 정보는 다음(임시 보안 자격 증명 (p. 302)) 을 참조하십시오.

   임시 자격 증명을 얻으려면 AWS STS AssumeRole API(권장) 또는 GetFederationToken API를 호출하면 됩니다. 이러한 API 작업 간의 차이에 대한 자세한 정보는 AWS 보안 블로그에서 AWS 계정에 대한 액세스 권한을 안전하게 위임하기 위한 API 옵션 이해하기를 참조하십시오.

   > **Important**
   >
   > GetFederationToken API를 사용하여 임시 보안 자격 증명을 생성한 경우 해당 역할을 수임한 사용자에게 자격 증명을 부여하는 권한을 지정해야 합니다. `AssumeRole*`로 시작하는 API 작업 중 어느 것에 대해서도 IAM 역할을 사용해 권한을 할당할 수 있습니다. 다른 API 작업의 경우 그 메커니즘이 API에 따라 달라집니다. 자세한 정보는 사용자 임시 보안 자격 증명에 대한 권한 제어 (p. 316) 단원을 참조하십시오. 또한 `AssumeRole*` API 작업을 사용하는 경우 장기 자격 증명을 사용하여 IAM 사용자로 호출해야 합니다. 그렇지 않으면 3단계의 연동 엔드포인트 호출에 실패합니다.
3. 임시 보안 자격 증명을 획득한 후에는 자격 증명을 JSON 세션 문자열로 구성해 로그인 토큰과 교환합니다. 다음 예에서는 자격 증명을 인코딩하는 방법을 보여줍니다. 자리 표시자 텍스트를 이전 단계에서 받는 자격 증명의 적절한 값들로 교체합니다.

   ```
   {"sessionId":"*** temporary access key ID ***",
   "sessionKey":"*** temporary secret access key ***",
   "sessionToken":"*** security token ***"}
   ```
4. URL encode 이전 단계의 세션 문자열. 인코딩하고 있는 정보가 지닌 중요성으로 인해 이러한 인코딩에는 웹 서비스를 사용하지 않는 것이 좋습니다. 대신 개발 도구 키트에 로컬로 설치된 함수 또는 기능을 사용하여 이 정보를 안전하게 인코딩합니다. Python의 `urllib.quote_plus` 함수, Java의 `URLEncoder.encode` 함수 또는 Ruby의 `CGI.escape` 함수를 사용할 수 있습니다. 이 주제 후반의 예제를 참조하십시오.
5. 다음 주소에서 AWS 연동 엔드포인트로 요청을 전송하십시오.

```
https://signin.aws.amazon.com/federation
```

요청에는 `Action` 및 `Session` 파라미터가 포함되어야 하며, `AssumeRole*` API 사용했다면 다음 예제의 `SessionDuration` HTTP 파라미터를 선택적으로 포함시킬 수 있습니다.

```
Action = getSigninToken
SessionDuration = time in seconds
Session = *** the URL encoded JSON string created in steps 3 & 4 ***
```

`SessionDuration` HTTP 파라미터는 연동된 콘솔 세션에 대한 기간을 지정합니다. 이 기간은 `DurationSeconds` 파라미터를 사용하여 지정하는 임시 자격 증명의 기간과는 다릅니다. `SessionDuration`의 최댓값은 43200(12시간)까지 지정할 수 있습니다. `SessionDuration` 파라미터가 없을 때는 2단계에서 AWS STS에서 검색한 자격 증명의 지속 시간을 세션의 기본값으로 사용합니다(기본 1시간). `DurationSeconds` 파라미터를 사용하여 기간을 지정하는 방법에 대한 자세한 정보는 `AssumeRole` API 관련 문서를 참조하십시오. 연동 엔드포인트의 `getSigninToken` 작업을 이용하면 한 시간보다 긴 콘솔 세션을 만들 수 있습니다.

> **Note**
>
> `SessionDuration`을 사용하여 임시 자격 증명을 얻을 경우에는 `GetFederationToken` HTTP 파라미터를 사용하지 마십시오. 이 파라미터를 사용하면 작업이 실패합니다.

기간이 연장된 콘솔 세션을 활성화하면 자격 증명이 노출될 위험이 높아집니다. 이러한 위험을 줄이려면 IAM 콘솔 페이지의 Role Summary(역할 요약)에서 Revoke Sessions(세션 취소)를 선택하여 원하는 역할의 활성 콘솔 세션을 즉시 비활성화하면 됩니다. 자세한 정보는 IAM 역할의 임시 보안 자격 증명 취소 (p. 273)를 참조하십시오.

다음은 요청에 대한 예시입니다. 가독성을 위해 줄바꿈이 되어 있지만 한 줄로 된 문자열로 제출해야 합니다.

```
https://signin.aws.amazon.com/federation
?Action=getSigninToken
&SessionDuration=1800
&Session=%7B%22sessionId%22%3A+%22ASIAJUMHIZPTOKTBMK5A%22%2C+%22sessionKey%22
%3A+%22LSD7LWI%2FL%2FN%2BgYpan5QFz0XUpc8s7HYjRsgcsrsm%22%2C+%22sessionToken%2
2%3A+%22FQoDYXdzEBQaDLbj3VWv2u50NN%2F3yyLSASwYtWhPnGPMNmzZFfZsL0Qd3vtYHw5A5dW
AjOsrkdPkghomIe3mJip5%2F0djDBbo7SmO%2FENDEiCdpsQKodTpleKA8xQq0CwFg6a69xdEBQT8
FipATnLbKoyS4b%2FebhnsTUjZZQWp0wXXqFF7gSm%2FMe2tXe0jzsdP0O12obez9lijPSdF1k2b5
PfGhiuyAR9aD5%2BubM0pY86fKex1qsytjvyTbZ9nXe6DvxVDcnCOhOGETJ7XFkSFdH0v%2FYR25C
UAhJ3nXIkIbG7Ucv9cOEpCf%2Fg23ijRgILIBQ%3D%3D%22%7D
```

연동 엔드포인트의 응답은 `SigninToken` 값이 있는 JSON 문서입니다. 다음의 예와 유사합니다.

```
{"SigninToken":"*** the SigninToken string ***"}
```

6. 마지막으로 연동 사용자가 AWS Management 콘솔에 액세스하는 데 사용할 수 있는 URL을 생성하십시오. 그 URL은 다음 파라미터와 함께 Step 5 (p. 212)에서 사용한 것과 동일한 연동 URL 엔드포인트입니다.

```
?Action = login
&Issuer = *** the form-urlencoded URL for your internal sign-in page ***
&Destination = *** the form-urlencoded URL to the desired AWS console page ***
&SigninToken = *** the value of SigninToken received in the previous step ***
```

다음 예는 최종 URL이 결국 어떤 모양을 갖추게 되는지 보여줍니다. 이 URL은 생성된 시각으로부터 15분 동안 유효합니다. URL에 내장된 콘솔 세션과 임시 보안 자격 증명은 이를 처음 요청할 때 `SessionDuration` HTTP 파라미터에 지정한 지속 기간만큼 유효합니다.

```
https://signin.aws.amazon.com/federation
?Action=login
&Issuer=https%3A%2F%2Fexample.com
&Destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs
&SigninToken=VCQgs5qZZt3Q6fn8Tr5EXAMPLEmLnwB7JjUc-SHwnUUWabcRdnWsi4DBn-dvC
CZ85wrD0nmldUcZEXAMPLE-vXYH4Q__mleuF_W2BE5HYexbe9y4Of-kje53SsjNNecATfjIzpW1
WibbnH6YcYRiBoffZBGExbEXAMPLE5aiKX4THWjQKC6gg6alHu6JFrnOJoK3dtP6I9a6hi6yPgm
iOkPZMmNGmhsvVxetKzr8mx3pxhHbMEXAMPLETv1pij0rok3IyCR2YVcIjqwfWv32HU2Xlj471u
3fU6uOfUComeKiqTGX974xzJOZbdmX_t_lLrhEXAMPLEDDIisSnyHGw2xaZZqudm4mo2uTDk9Pv
9l5K0ZCqIgEXAMPLEcA6tgLPykEWGUyH6BdSC6166n4M4JkXIQgac7_7821YqixsNxZ6rsrpzwf
nQoS14O7R0eJCCJ684EXAMPLEZRdBNnuLbUYpz2Iw3vIN0tQgOujwnwydPscM9F7foaEK3jwMkg
Apeb1-6L_OB12MZhuFxx55555EXAMPLEhyETEd4ZulKPdXHkgl6T9ZkIlHz2Uy1RUTUhhUxNtSQ
nWc5xkbBoEcXqpoSIeK7yhje9Vzhd61AEXAMPLElbWeouACEMG6-Vd3dAgFYd6i5FYoyFrZLWvm
0LSG7RyYKeYN5VIzUk3YWQpyjP0RiT5KUrsUi-NEXAMPLExMOMdoODBEgKQsk-iu2ozh6r8bxwC
RNhujg
```

Python을 사용한 예제 코드

다음 예는 Python을 사용해 연동 사용자에게 AWS Management 콘솔에 대한 직접 액세스 권한을 부여하는 URL을 프로그래밍 방식으로 생성하는 방법을 보여줍니다. 이 예제에서는 Python용 AWS SDK(Boto3)을 사용합니다.

코드는 AssumeRole API를 사용해 임시 보안 자격 증명을 획득합니다.

```
import urllib, json, sys
import requests # 'pip install requests'
import boto3 # AWS SDK for Python (Boto3) 'pip install boto3'

# Step 1: Authenticate user in your own identity system.

# Step 2: Using the access keys for an IAM user in your AWS account,
# call "AssumeRole" to get temporary access keys for the federated user

# Note: Calls to AWS STS AssumeRole must be signed using the access key ID
# and secret access key of an IAM user or using existing temporary credentials.
# The credentials can be in EC2 instance metadata, in environment variables,
# or in a configuration file, and will be discovered automatically by the
# client('sts') function. For more information, see the Python SDK docs:
# http://boto3.readthedocs.io/en/latest/reference/services/sts.html
# http://boto3.readthedocs.io/en/latest/reference/services/sts.html#STS.Client.assume_role
sts_connection = boto3.client('sts')

assumed_role_object = sts_connection.assume_role(
    RoleArn="arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/ROLE-NAME",
    RoleSessionName="AssumeRoleSession",
)

# Step 3: Format resulting temporary credentials into JSON
url_credentials = {}
url_credentials['sessionId'] = assumed_role_object.get('Credentials').get('AccessKeyId')
url_credentials['sessionKey'] =
 assumed_role_object.get('Credentials').get('SecretAccessKey')
url_credentials['sessionToken'] =
 assumed_role_object.get('Credentials').get('SessionToken')
json_string_with_temp_credentials = json.dumps(url_credentials)

# Step 4. Make request to AWS federation endpoint to get sign-in token. Construct the
 parameter string with
# the sign-in action request, a 12-hour session duration, and the JSON document with
 temporary credentials
# as parameters.
```

```
request_parameters = "?Action=getSigninToken"
request_parameters += "&SessionDuration=43200"
if sys.version_info[0] < 3:
    def quote_plus_function(s):
        return urllib.quote_plus(s)
else:
    def quote_plus_function(s):
        return urllib.parse.quote_plus(s)
request_parameters += "&Session=" + quote_plus_function(json_string_with_temp_credentials)
request_url = "https://signin.aws.amazon.com/federation" + request_parameters
r = requests.get(request_url)
# Returns a JSON document with a single element named SigninToken.
signin_token = json.loads(r.text)

# Step 5: Create URL where users can use the sign-in token to sign in to
# the console. This URL must be used within 15 minutes after the
# sign-in token was issued.
request_parameters = "?Action=login"
request_parameters += "&Issuer=Example.org"
request_parameters += "&Destination=" + quote_plus_function("https://
console.aws.amazon.com/")
request_parameters += "&SigninToken=" + signin_token["SigninToken"]
request_url = "https://signin.aws.amazon.com/federation" + request_parameters

# Send final URL to stdout
print (request_url)
```

Java를 사용한 예제 코드

다음 예는 Java를 사용해 연동 사용자에게 AWS Management 콘솔에 대한 직접 액세스 권한을 부여하는 URL을 프로그래밍 방식으로 생성하는 방법을 보여줍니다. 다음 코드 조각은 Java용 AWS SDK를 사용합니다.

```
import java.net.URLEncoder;
import java.net.URL;
import java.net.URLConnection;
import java.io.BufferedReader;
import java.io.InputStreamReader;
// Available at http://www.json.org/java/index.html
import org.json.JSONObject;
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.services.securitytoken.AWSSecurityTokenServiceClient;
import com.amazonaws.services.securitytoken.model.Credentials;
import com.amazonaws.services.securitytoken.model.GetFederationTokenRequest;
import com.amazonaws.services.securitytoken.model.GetFederationTokenResult;


/* Calls to AWS STS API operations must be signed using the access key ID
   and secret access key of an IAM user or using existing temporary
   credentials. The credentials should not be embedded in code. For
   this example, the code looks for the credentials in a
   standard configuration file.
*/
AWSCredentials credentials =
  new PropertiesCredentials(
         AwsConsoleApp.class.getResourceAsStream("AwsCredentials.properties"));

AWSSecurityTokenServiceClient stsClient =
  new AWSSecurityTokenServiceClient(credentials);

GetFederationTokenRequest getFederationTokenRequest =
  new GetFederationTokenRequest();
getFederationTokenRequest.setDurationSeconds(1800);
```

```
getFederationTokenRequest.setName("UserName");

// A sample policy for accessing Amazon Simple Notification Service (Amazon SNS) in the
 console.

String policy = "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Action\":\"sns:*\"," +
  "\"Effect\":\"Allow\",\"Resource\":\"*\"}]}";

getFederationTokenRequest.setPolicy(policy);

GetFederationTokenResult federationTokenResult =
  stsClient.getFederationToken(getFederationTokenRequest);

Credentials federatedCredentials = federationTokenResult.getCredentials();

// The issuer parameter specifies your internal sign-in
// page, for example https://mysignin.internal.mycompany.com/.
// The console parameter specifies the URL to the destination console of the
// AWS Management Console. This example goes to Amazon SNS.
// The signin parameter is the URL to send the request to.

String issuerURL = "https://mysignin.internal.mycompany.com/";
String consoleURL = "https://console.aws.amazon.com/sns";
String signInURL = "https://signin.aws.amazon.com/federation";

// Create the sign-in token using temporary credentials,
// including the access key ID,  secret access key, and security token.
String sessionJson = String.format(
  "{\"%1$s\":\"%2$s\",\"%3$s\":\"%4$s\",\"%5$s\":\"%6$s\"}",
  "sessionId", federatedCredentials.getAccessKeyId(),
  "sessionKey", federatedCredentials.getSecretAccessKey(),
  "sessionToken", federatedCredentials.getSessionToken());

// Construct the sign-in request with the request sign-in token action, a
// 12-hour console session duration, and the JSON document with temporary
// credentials as parameters.

String getSigninTokenURL = signInURL +
                           "?Action=getSigninToken" +
                           "&DurationSeconds=43200" +
                           "&SessionType=json&Session=" +
                           URLEncoder.encode(sessionJson,"UTF-8");

URL url = new URL(getSigninTokenURL);

// Send the request to the AWS federation endpoint to get the sign-in token
URLConnection conn = url.openConnection ();

BufferedReader bufferReader = new BufferedReader(new
  InputStreamReader(conn.getInputStream()));
String returnContent = bufferReader.readLine();

String signinToken = new JSONObject(returnContent).getString("SigninToken");

String signinTokenParameter = "&SigninToken=" + URLEncoder.encode(signinToken,"UTF-8");

// The issuer parameter is optional, but recommended. Use it to direct users
// to your sign-in page when their session expires.

String issuerParameter = "&Issuer=" + URLEncoder.encode(issuerURL, "UTF-8");

// Finally, present the completed URL for the AWS console session to the user

String destinationParameter = "&Destination=" + URLEncoder.encode(consoleURL,"UTF-8");
String loginURL = signInURL + "?Action=login" +
```

```
                    signinTokenParameter + issuerParameter + destinationParameter;
```

URL을 생성하는 방법을 보여주는 예(Ruby)

다음 예는 Ruby를 사용해 연동 사용자에게 AWS Management 콘솔에 대한 직접 액세스 권한을 부여하는 URL을 프로그래밍 방식으로 생성하는 방법을 보여줍니다. 이 코드 조각은 Ruby용 AWS SDK를 사용합니다.

```
require 'rubygems'
require 'json'
require 'open-uri'
require 'cgi'
require 'aws-sdk'

# Create a new STS instance
#
# Note: Calls to AWS STS API operations must be signed using an access key ID
# and secret access key. The credentials can be in EC2 instance metadata
# or in environment variables and will be automatically discovered by
# the default credentials provider in the AWS Ruby SDK.
sts = Aws::STS::Client.new()

# The following call creates a temporary session that returns
# temporary security credentials and a session token.
# The policy grants permissions to work
# in the AWS SNS console.

session = sts.get_federation_token({
  duration_seconds: 1800,
  name: "UserName",
  policy: "{\"Version\":\"2012-10-17\",\"Statement\":{\"Effect\":\"Allow\",\"Action\":
\"sns:*\",\"Resource\":\"*\"}}",
})

# The issuer value is the URL where users are directed (such as
# to your internal sign-in page) when their session expires.
#
# The console value specifies the URL to the destination console.
# This example goes to the Amazon SNS console.
#
# The sign-in value is the URL of the AWS STS federation endpoint.
issuer_url = "https://mysignin.internal.mycompany.com/"
console_url = "https://console.aws.amazon.com/sns"
signin_url = "https://signin.aws.amazon.com/federation"

# Create a block of JSON that contains the temporary credentials
# (including the access key ID, secret access key, and session token).
session_json = {
  :sessionId => session.credentials[:access_key_id],
  :sessionKey => session.credentials[:secret_access_key],
  :sessionToken => session.credentials[:session_token]
}.to_json

# Call the federation endpoint, passing the parameters
# created earlier and the session information as a JSON block.
# The request returns a sign-in token that's valid for 15 minutes.
# Signing in to the console with the token creates a session
# that is valid for 12 hours.
get_signin_token_url = signin_url +
                       "?Action=getSigninToken" +
                       "&SessionType=json&Session=" +
                       CGI.escape(session_json)

returned_content = URI.parse(get_signin_token_url).read
```

```
# Extract the sign-in token from the information returned
# by the federation endpoint.
signin_token = JSON.parse(returned_content)['SigninToken']
signin_token_param = "&SigninToken=" + CGI.escape(signin_token)

# Create the URL to give to the user, which includes the
# sign-in token and the URL of the console to open.
# The "issuer" parameter is optional but recommended.
issuer_param = "&Issuer=" + CGI.escape(issuer_url)
destination_param = "&Destination=" + CGI.escape(console_url)
login_url = signin_url + "?Action=login" + signin_token_param +
  issuer_param + destination_param
```

서비스 연결 역할 사용

서비스 연결 역할은 AWS 서비스에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 해당 서비스에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다. 또한 연결된 서비스는 서비스 연결 역할을 만들고 수정하며 삭제하는 방법을 정의합니다. 서비스는 역할을 자동으로 만들거나 삭제할 수 있습니다. 서비스의 프로세스나 마법사를 사용하여 사용자가 역할을 만들거나 수정하거나 삭제하도록 허용할 수도 있습니다. 또는 사용자가 IAM을 사용하여 역할을 만들거나 삭제하도록 요구할 수도 있습니다. 서비스 연결 역할은 그 방법에 상관없이 사용자 대신 작업을 완료하는 데 필요한 권한을 수동으로 추가할 필요가 없기 때문에 설정이 쉬워집니다.

연결된 서비스에서 서비스 연결 역할 권한을 정의하므로 정의되지 않은 경우에만 해당 역할로 서비스를 수행할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 개체에 연결할 수 없습니다.

먼저 역할의 관련 리소스를 삭제해야만 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 리소스가 보호됩니다.

> Tip
>
> 서비스 연결 역할의 사용을 지원하는 서비스에 대한 자세한 정보는 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [Yes] 링크를 선택합니다.

서비스 연결 역할 권한

사용자 또는 역할이 서비스 연결 역할을 작성하거나 편집할 수 있도록 IAM 개체(사용자, 그룹, 역할 등)의 권한을 구성해야 합니다.

> Note
>
> 서비스 링크된 역할에 대한 ARN은 정책에서 *SERVICE-NAME*.amazonaws.com으로 나타내지는 서비스 보안 주체를 포함합니다. 각 경우마다 다르고 AWS 서비스에 따라 형식이 다양하기 때문에 서비스 보안 주체를 알기 어렵습니다. 서비스의 보안 주체를 보려면 해당 서비스 링크된 역할 설명서 단원을 참조하십시오.

IAM 개체가 특정 서비스 연결 역할을 만들 수 있도록 허용하려면

서비스 연결 역할을 생성해야 하는 IAM 개체에 다음 정책을 추가합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/SERVICE-
NAME.amazonaws.com/SERVICE-LINKED-ROLE-NAME-PREFIX*",
```

```
            "Condition": {"StringLike": {"iam:AWSServiceName": "SERVICE-
NAME.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/SERVICE-
NAME.amazonaws.com/SERVICE-LINKED-ROLE-NAME-PREFIX*"
        }
    ]
}
```

IAM 개체가 서비스 연결 역할을 만들 수 있도록 허용하려면

서비스 연결 역할 또는 필요한 정책을 포함해야 하는 모든 서비스 역할을 생성해야 하는 IAM 개체의 권한 정책에 다음 명령문을 추가합니다. 이 정책 명령문은 IAM 개체가 역할에 정책을 연결하는 것을 허용하지 않습니다.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

IAM 개체가 서비스 역할의 설명을 편집할 수 있도록 허용하려면

서비스 연결 역할 또는 서비스 역할의 설명을 편집해야 하는 IAM 개체의 권한 정책에 다음 명령문을 추가합니다.

```
{
    "Effect": "Allow",
    "Action": "iam:UpdateRoleDescription",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

IAM 개체가 특정 서비스 연결 역할을 삭제하도록 허용하려면

서비스 연결 역할을 삭제해야 하는 IAM 개체의 권한 정책에 다음 문장을 추가합니다.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/SERVICE-NAME.amazonaws.com/SERVICE-
LINKED-ROLE-NAME-PREFIX*"
}
```

IAM 개체가 서비스 연결 역할을 삭제할 수 있도록 허용하려면

서비스 연결 역할만 삭제하고 서비스 역할은 삭제하지 않는 IAM 개체의 권한 정책에 다음 명령문을 추가합니다.

```
{
    "Effect": "Allow",
    "Action": [
```

```
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

IAM 엔터티가 기존 역할을 서비스에 전달하도록 허용하는 방법

일부 AWS 서비스를 사용하면 새 서비스에 연결된 역할을 생성하지 않고, 그 대신에 서비스에 기존 역할을 전달할 수 있습니다. 이렇게 하려면 사용자에게 서비스에 역할을 전달할 수 있는 권한이 있어야 합니다. 역할을 생성해야 하는 IAM 개체의 권한 정책에 다음 명령문을 추가합니다. 또한 이 정책 설명에서는 엔터티가 전달할 역할을 선택할 수 있는 역할 목록을 볼 수 있도록 허용합니다. 자세한 정보는 사용자에게 AWS 서비스에 역할을 전달할 권한 부여 (p. 254) 단원을 참조하십시오.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:ListRoles",
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::123456789012:role/my-role-for-XYZ"
}
```

서비스 연결 역할 권한 양도

서비스 연결 역할에서 부여한 권한은 간접적으로 다른 사용자 및 역할에게 양도할 수 있습니다. 임의의 서비스에게 다른 서비스 작업을 실행하도록 허용할 경우 해당 서비스는 앞으로 다른 서비스의 작업 권한을 사용할 수 있습니다. 다른 사용자 또는 역할에게 서비스 작업을 실행할 수 있는 권한이 있으면 서비스가 해당 역할까지 맡아서 다른 서비스의 리소스에 액세스할 수 있습니다. 이 말은 다른 사용자 또는 역할이 간접적으로 다른 서비스에 액세스할 수 있다는 것을 의미합니다.

예를 들어 Amazon RDS DB 인스턴스를 생성하면 RDS가 서비스 연결 역할을 생성합니다. 이렇게 생성된 서비스 연결 역할은 고객이 DB 인스턴스를 편집할 때마다 RDS에게 고객을 대신해서 Amazon EC2, Amazon SNS, Amazon CloudWatch Logs 및 Amazon Kinesis를 호출하도록 허용합니다. 고객 계정 또는 다른 계정에 속한 사용자 및 역할에게 Amazon RDS 인스턴스에 액세스하도록 허용하는 정책을 생성하더라도 RDS는 계속해서 해당 역할을 사용해 EC2, SNS, CloudWatch Logs 및 Kinesis를 변경합니다. 새로운 사용자 또는 역할도 이처럼 다른 서비스의 리소스를 간접적으로 편집할 수 있습니다.

서비스 연결 역할 만들기

서비스 연결 역할을 만드는 데 사용하는 방법은 서비스에 따라 다릅니다. 경우에 따라 서비스 연결 역할을 수동으로 만들 필요가 없습니다. 예를 들어 사용자가 서비스의 특정 작업(리소스 만들기 등)을 수행할 때 서비스가 서비스 연결 역할을 자동으로 생성할 수 있습니다. 또한, 서비스가 서비스 연결 역할 지원을 시작하기 전에 서비스를 사용한 경우에는 서비스가 자동으로 해당 계정에 역할을 생성했을 수 있습니다. 자세히 알아보려면 내 AWS 계정에 표시되는 새 역할 (p. 553) 단원을 참조하십시오.

다른 경우에는 서비스에서 서비스 콘솔, API 또는 CLI를 사용하여 서비스 연결 역할을 수동으로 만들도록 허용할 수 있습니다. 서비스 연결 역할의 사용을 지원하는 서비스에 대한 자세한 정보는 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 서비스가 서비스 연결 역할 생성을 지원하는지 여부를 알아보려면 예 링크를 선택하여 해당 서비스의 서비스 연결 역할 설명서 단원을 참조하십시오.

서비스가 역할 만들기를 지원하지 않는 경우에는 IAM을 사용하여 서비스 연결 역할을 만들 수 있습니다.

> **Important**
>
> 서비스 연결 역할은 AWS 계정의 IAM 역할 제한을 계산하는 데 포함되지만, 한도에 도달한 경우에도 계정에 서비스 연결 역할을 만들 수 있습니다. 한도를 초과해도 생성할 수 있는 역할은 서비스 연결 역할뿐입니다.

서비스 연결 역할 만들기(콘솔)

IAM에서 서비스 연결 역할을 만들기 전에, 연결된 서비스가 서비스 역할을 자동으로 생성하는지 확인하십시오. 또한 서비스의 콘솔, API, CLI 등에서 역할을 만들 수 있는지를 알아봅니다.

서비스 연결 역할을 만들려면(콘솔 사용)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다. 그런 다음 [Create role]을 선택합니다.
3. AWS 서비스 역할 유형을 선택한 후 이 역할로 수행하도록 허용하려는 서비스를 선택합니다.
4. 서비스의 사용 사례를 선택합니다. 지정한 서비스에 사용 사례가 하나뿐이면 자동으로 선택됩니다. 사용 사례는 서비스에 필요한 신뢰 정책을 포함하기 위해 서비스에서 정합니다. 그런 다음 [Next: Permissions]를 선택합니다.
5. 하나 이상의 권한 정책을 선택하여 역할에 연결합니다. 선택한 사용 사례에 따라 서비스에서 다음을 수행할 수 있습니다.

   - 역할이 사용하는 권한 정의
   - 제한된 권한 집합에서 선택할 수 있도록 허용
   - 모든 권한 집합에서 선택할 수 있도록 허용
   - 여기서 정책을 선택하지 않고, 나중에 정책을 만들어 역할에 연결할 수 있도록 허용합니다.

   역할에 부여하려는 권한을 할당하는 정책 옆의 확인란을 선택한 후 다음: 태그을 선택합니다.

   Note

   지정하는 권한은 역할을 사용하는 모든 주체가 사용할 수 있습니다. 기본적으로 역할은 권한이 없습니다.
6. [Next: Review]를 선택합니다. 생성하는 동안에는 서비스 연결 역할에 태그를 연결할 수 없습니다. IAM에서의 태그 사용에 대한 자세한 정보는 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
7. 역할 이름의 경우 역할 이름 사용자 지정 수준은 서비스에서 정합니다. 서비스에서 역할 이름을 정한 경우 이 옵션을 편집할 수 없습니다. 다른 경우에는 서비스에서 역할 이름의 접두사를 정의하고 사용자가 선택적으로 접미부를 입력하도록 할 수 있습니다.

   가능한 경우 기본 이름에 추가할 역할 이름 접미사를 입력합니다. 이 접미사는 이 역할의 목적을 파악하는 데 도움이 됩니다. 역할 이름은 AWS 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어, 이름이 **<service-linked-role-name>_SAMPLE**과 **<service-linked-role-name>_sample**, 두 가지로 지정된 역할을 만들 수는 없습니다. 다양한 주체가 역할을 참조할 수 있기 때문에 역할이 생성된 후에는 역할 이름을 편집할 수 없습니다.
8. (선택 사항) [Role description]에서 새로운 서비스 연결 역할에 대한 설명을 편집합니다.
9. 역할을 검토한 다음 [Create role]을 선택합니다.

서비스 연결 역할 만들기(AWS CLI)

IAM에서 서비스 연결 역할을 만들기 전에, 연결된 서비스가 서비스 역할을 자동으로 생성하는지 그리고 서비스의 CLI에서 사용자가 역할을 만들 수 있는지를 확인하십시오. 서비스 CLI가 지원되지 않는 경우 IAM 명령을 사용하여 서비스가 역할을 위임하는 데 필요한 인라인 정책과 신뢰 정책을 포함하는 서비스 연결 역할을 만들 수 있습니다.

서비스 연결 역할(AWS CLI)을 만들려면

다음 명령을 실행합니다.

```
$ aws iam create-service-linked-role --aws-service-name SERVICE-NAME.amazonaws.com
```

서비스 연결 역할 만들기(AWS API)

IAM에서 서비스 연결 역할을 만들기 전에, 연결된 서비스가 서비스 역할을 자동으로 생성하는지 그리고 서비스의 API에서 사용자가 역할을 만들 수 있는지를 확인하십시오. 서비스 API가 지원되지 않는 경우 AWS API를 사용하여 서비스가 역할을 위임하는 데 필요한 인라인 정책과 신뢰 정책을 포함하는 서비스 연결 역할을 만들 수 있습니다.

서비스 연결 역할(AWS API)을 만들려면

CreateServiceLinkedRole API 호출을 사용합니다. 요청 시 *SERVICE_NAME_URL*.amazonaws.com 서비스 이름을 지정합니다.

예를 들어 Lex 봇 서비스 연결 역할을 만들려면 lex.amazonaws.com을 사용합니다.

서비스 연결 역할 편집

서비스 연결 역할을 편집하는 데 사용하는 방법은 서비스에 따라 다릅니다. 일부 서비스는 사용자가 서비스 콘솔, API 또는 CLI에서 서비스 연결 역할의 권한을 편집할 수 있도록 허용합니다. 하지만 서비스 연결 역할을 만든 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. IAM 콘솔, API, CLI에서 역할의 설명을 편집할 수 있습니다.

서비스 연결 역할의 사용을 지원하는 서비스에 대한 자세한 정보는 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 서비스가 서비스 연결 역할 편집을 지원하는지 여부를 알아보려면 예 링크를 선택하여 해당 서비스의 서비스 연결 역할 설명서 단원을 참조하십시오.

서비스 연결 역할 설명 편집(콘솔 사용)

IAM 콘솔을 사용하여 서비스 연결 역할의 설명을 편집할 수 있습니다.

서비스 연결 역할의 설명을 편집하려면(콘솔 사용)

1. IAM 콘솔의 탐색 창에서 역할을 선택합니다.
2. 변경할 역할 이름을 선택합니다.
3. Role description(역할 설명)의 맨 오른쪽에서 편집을 선택합니다.
4. 상자에 새 설명을 입력하고 저장을 선택합니다.

서비스 연결 역할 설명 편집(AWS CLI)

AWS CLI에서 IAM 명령을 사용하여 서비스 연결 역할의 설명을 편집할 수 있습니다.

서비스 연결 역할의 설명을 변경하려면(AWS CLI)

1. (옵션) 역할의 현재 설명을 보려면 다음 명령 중 하나를 실행합니다.

   ```
   $ aws iam get-role --role-name ROLE-NAME
   ```

   CLI 명령에서 역할을 참조하려면 ARN이 아니라 역할 이름을 사용해야 합니다. 예를 들어, 어떤 역할의 ARN이 arn:aws:iam::123456789012:role/myrole인 경우 참조할 역할은 **myrole**입니다.
2. 서비스 연결 역할의 설명을 업데이트하려면 다음 명령을 실행합니다.

   ```
   $ aws iam update-role --role-name ROLE-NAME --description OPTIONAL-DESCRIPTION
   ```

서비스 연결 역할 설명 편집(AWS API)

AWS API를 사용하여 서비스 연결 역할의 설명을 편집할 수 있습니다.

서비스 연결 역할의 설명을 변경하려면(AWS API 사용)

1. (옵션) 역할의 현재 설명을 보려면 다음 작업을 호출하고 역할 이름을 지정합니다.

   AWS API: GetRole
2. 역할의 설명을 업데이트하려면 다음 작업을 호출하고 역할 이름 및 설명(선택 사항)을 지정합니다.

   AWS API: UpdateRole

서비스 연결 역할 삭제

서비스 연결 역할을 만드는 데 사용하는 방법은 서비스에 따라 다릅니다. 일부 경우에서는 서비스 연결 역할을 수동으로 삭제할 필요가 없습니다. 예를 들어, 서비스에서 특정 작업(예: 리소스 제거)을 완료하면 서비스에서 사용자의 서비스 연결 역할을 삭제할 수 있습니다.

서비스에서 서비스 연결 역할을 서비스 콘솔, API 또는 CLI에서 수동으로 삭제하는 것이 지원되지 않는 경우도 있을 수 있습니다.

서비스 연결 역할의 사용을 지원하는 서비스에 대한 자세한 정보는 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 서비스에서 서비스 연결 역할 삭제를 지원하는지 확인하려면 예 링크를 선택하여 해당 서비스의 서비스 연결 역할 문서를 확인하십시오.

서비스에서 역할 삭제를 지원하지 않는 경우에는 사용자가 IAM 콘솔, API 또는 CLI에서 서비스 연결 역할을 삭제할 수 있습니다. 서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 개체가 없도록 합니다. 단, 삭제 전에 서비스 연결 역할을 정리해야 합니다.

서비스 연결 역할 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에 활성 세션이 없는지 확인하고 역할에서 사용되는 리소스를 모두 제거해야 합니다.

IAM 콘솔에서 서비스 연결 역할에 활성 세션이 있는지 확인하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다. 그런 다음 서비스 연결 역할의 이름(확인란 아님)을 선택합니다.
3. 선택한 역할의 [Summary] 페이지에서 [Access Advisor] 탭을 선택합니다.
4. [Access Advisor] 탭에서 서비스 연결 역할의 최근 활동을 검토합니다.

   Note

   서비스에서 서비스 연결 역할을 사용하는지 잘 모를 경우에는 역할을 삭제해보십시오. 서비스에서 역할을 사용하는 경우에는 삭제가 안 되어 역할이 사용 중인 리전을 볼 수 있습니다. 역할이 사용 중인 경우에는 세션이 종료될 때까지 기다렸다가 역할을 삭제해야 합니다. 서비스 연결 역할에 대한 세션은 취소할 수 없습니다.

서비스 연결 역할에서 사용하는 리소스를 제거하려면

서비스 연결 역할의 사용을 지원하는 서비스에 대한 자세한 정보는 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 서비스에서 서비스 연결 역할 삭제를 지원하는지 확인하려면 예 링크를 선택하여 해당 서비스의 서비스 연결 역할 문서를 확인하십시오. 사용자의 서비스 연결 역할에서 사용되는 리소스를 제거하는 방법은 해당 서비스의 문서 단원을 참조하십시오.

서비스 연결 역할(콘솔) 삭제

IAM 콘솔을 사용하여 서비스 연결 역할을 삭제할 수 있습니다.

서비스 연결 역할을 삭제하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다. 그런 다음 삭제할 역할의 이름이나 행이 아닌 이름 옆에 있는 확인란을 선택합니다.
3. 페이지 상단의 [Role actions]에서 [Delete role]을 선택합니다.
4. 확인 대화 상자가 나타나면 서비스 마지막 액세스 데이터를 검토합니다. 이 데이터는 선택한 각 역할이 AWS 서비스를 마지막으로 액세스한 일시를 보여 줍니다. 이를 통해 역할이 현재 활동 중인지 여부를 확인할 수 있습니다. 계속 진행하려면 [Yes, Delete]을 선택하여 삭제할 서비스 연결 역할을 제출합니다.
5. IAM 콘솔 알림을 보고 서비스 연결 역할 삭제 진행 상황을 모니터링합니다. IAM 서비스 연결 역할 삭제는 비동기이므로 삭제할 역할을 제출한 후에 삭제 작업이 성공하거나 실패할 수 있습니다.

   - 작업에 성공하면 목록에서 역할이 제거되고 성공 알림이 페이지 상단에 나타납니다.
   - 작업에 실패할 경우 알림의 [View details] 또는 [View Resources]를 선택하면 삭제 실패 이유를 확인할 수 있습니다. 역할에서 서비스 리소스를 사용 중이어서 삭제에 실패한 경우에는 알림에 리소스 목록이 포함됩니다(서비스에서 해당 정보를 반환할 경우). 이후 리소스를 정리하고 (p. 223) 삭제를 다시 제출할 수 있습니다.

     Note

     서비스에서 반환하는 정보에 따라 이 과정을 여러 번 반복해야 할 수 있습니다. 예를 들어, 서비스 연결 역할에서 6개의 리소스를 사용할 수 있으며, 서비스에서 이중 5개에 관한 정보를 반환할 수 있습니다. 5개 리소스를 정리하고 삭제할 역할을 다시 제출할 경우 삭제에 실패하고 서비스에서 나머지 1개의 리소스를 보고합니다. 서비스에서 리소스 전부를 반환하거나, 일부만 반환하거나, 리소스를 보고하지 않을 수 있습니다.
   - 작업에 실패했는데 알림에 리소스 목록이 포함되지 않을 경우에는 서비스에서 해당 정보를 반환하지 않을 수 있습니다. 해당 서비스의 리소스를 정리하는 방법은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 표에서 서비스를 확인하고 예 링크를 선택하여 해당 서비스의 서비스 연결 역할 문서를 확인합니다.

서비스 연결 역할 삭제(AWS CLI)

AWS CLI에서 IAM 명령을 사용하여 서비스 연결 역할을 삭제할 수 있습니다.

서비스 연결 역할을 삭제하려면(AWS CLI)

1. 삭제할 서비스 연결 역할의 이름을 모를 경우에는 다음 명령을 입력하여 계정에 역할과 Amazon 리소스 이름(ARN)을 나열합니다.

   ```
   $ aws iam get-role --role-name role-name
   ```

   CLI 명령에서 역할을 참조하려면 ARN이 아니라 역할 이름을 사용해야 합니다. 예를 들어, 어떤 역할의 ARN이 `arn:aws:iam::123456789012:role/myrole`인 경우 참조할 역할은 **myrole**입니다.
2. 서비스 연결 역할이 사용되지 않거나 연결된 리소스가 없는 경우에는 서비스 연결 역할을 삭제할 수 없으므로 삭제 요청을 제출해야 합니다. 이러한 조건이 충족되지 않으면 요청이 거부될 수 있습니다. 삭제 작업 상태를 확인하려면 응답의 `deletion-task-id`를 캡처해야 합니다. 다음 명령을 입력하여 서비스 연결 역할 삭제 요청을 제출합니다.

   ```
   $ aws iam delete-service-linked-role --role-name role-name
   ```

3. 다음 명령을 입력하여 삭제 작업의 상태를 확인합니다.

```
$ aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

삭제 작업은 `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` 또는 `FAILED` 상태일 수 있습니다. 삭제에 실패할 경우 문제를 해결할 수 있도록 실패 이유가 호출에 반환됩니다. 역할에서 서비스 리소스를 사용 중이어서 삭제에 실패한 경우에는 알림에 리소스 목록이 포함됩니다(서비스에서 해당 정보를 반환할 경우). 이후 리소스를 정리하고 (p. 223) 삭제를 다시 제출할 수 있습니다.

Note

서비스에서 반환하는 정보에 따라 이 과정을 여러 번 반복해야 할 수 있습니다. 예를 들어, 서비스 연결 역할에서 6개의 리소스를 사용할 수 있으며, 서비스에서 이중 5개에 관한 정보를 반환할 수 있습니다. 5개 리소스를 정리하고 삭제할 역할을 다시 제출할 경우 삭제에 실패하고 서비스에서 나머지 1개의 리소스를 보고합니다. 서비스에서 리소스 전부를 반환하거나, 일부만 반환하거나, 리소스를 보고하지 않을 수 있습니다. 리소스를 보고하지 않는 서비스의 리소스를 정리하는 방법은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 표에서 서비스를 확인하고 예 링크를 선택하여 해당 서비스의 서비스 연결 역할 문서를 확인합니다.

서비스 연결 역할 삭제(AWS API)

AWS API를 사용하여 서비스 연결 역할을 삭제할 수 있습니다.

서비스 연결 역할을 삭제하려면(AWS API)

1. 서비스 연결 역할 삭제 요청을 제출하려면 DeleteServiceLinkedRole을 호출합니다. 요청에 역할 이름을 지정합니다.

   서비스 연결 역할이 사용되지 않거나 연결된 리소스가 없는 경우에는 서비스 연결 역할을 삭제할 수 없으므로 삭제 요청을 제출해야 합니다. 이러한 조건이 충족되지 않으면 요청이 거부될 수 있습니다. 삭제 작업 상태를 확인하려면 응답의 `DeletionTaskId`를 캡처해야 합니다.
2. 삭제 상태를 확인하려면 GetServiceLinkedRoleDeletionStatus를 호출합니다. 요청에 `DeletionTaskId`를 지정합니다.

   삭제 작업은 `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` 또는 `FAILED` 상태일 수 있습니다. 삭제에 실패할 경우 문제를 해결할 수 있도록 실패 이유가 호출에 반환됩니다. 역할에서 서비스 리소스를 사용 중이어서 삭제에 실패한 경우에는 알림에 리소스 목록이 포함됩니다(서비스에서 해당 정보를 반환할 경우). 이후 리소스를 정리하고 (p. 223) 삭제를 다시 제출할 수 있습니다.

   Note

   서비스에서 반환하는 정보에 따라 이 과정을 여러 번 반복해야 할 수 있습니다. 예를 들어, 서비스 연결 역할에서 6개의 리소스를 사용할 수 있으며, 서비스에서 이중 5개에 관한 정보를 반환할 수 있습니다. 5개 리소스를 정리하고 삭제할 역할을 다시 제출할 경우 삭제에 실패하고 서비스에서 나머지 1개의 리소스를 보고합니다. 서비스에서 리소스 전부를 반환하거나, 일부만 반환하거나, 리소스를 보고하지 않을 수 있습니다. 리소스를 보고하지 않는 서비스의 리소스를 정리하는 방법은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 표에서 서비스를 확인하고 예 링크를 선택하여 해당 서비스의 서비스 연결 역할 문서를 확인합니다.

IAM 역할 생성

역할을 생성하기 위해서는 AWS Management 콘솔, AWS CLI, Windows PowerShell용 도구 또는 IAM API를 사용할 수 있습니다.

AWS Management 콘솔을 사용하는 경우 마법사가 역할 생성 절차를 단계별로 안내합니다. 마법사의 진행 단계는 생성하는 역할 대상이 AWS 서비스일 때, AWS 계정일 때, 혹은 연동 사용자일 때에 따라 약간 다릅니다.

주제

역할을 만들어 IAM 사용자에게 권한 위임

IAM 역할을 사용해 AWS 리소스에 대한 액세스 권한을 위임할 수 있습니다. IAM 역할을 사용해 신뢰하는 계정과 다른 AWS 신뢰 받는 계정 간에 신뢰 관계를 설정할 수 있습니다. 신뢰하는 계정은 액세스되는 리소스를 소유하고 신뢰받는 계정은 리소스에 대한 액세스가 필요한 사용자를 저장합니다. 그러나, 다른 계정이 해당 계정의 리소스를 소유할 수 있는 가능성이 있습니다. 예를 들어, 신뢰받는 계정은 신뢰 계정이 Amazon S3 버킷의 새로운 객체를 생성하는 것처럼 새로운 리소스를 생성하도록 허용할 수 있습니다. 이러한 경우, 리소스를 생성하는 계정은 리소스를 소유하고 누구에게 리소스에 대한 액세스를 부여할지 제어합니다.

신뢰 관계를 생성한 후 IAM 사용자 또는 신뢰받는 계정의 애플리케이션은 AWS Security Token Service(AWS STS) `AssumeRole` API 작업을 사용할 수 있습니다. 이 작업은 계정의 AWS 리소스에 액세스할 수 있는 임시 보안 자격 증명을 제공합니다.

계정은 둘 다 직접 제어할 수 있거나 사용자가 속한 계정의 경우 타사가 제어할 수 있습니다. 사용자가 있는 다른 계정이 귀하가 제어하지 않는 AWS 계정에 있는 경우 `externalId` 속성을 사용할 수 있습니다. 외부 ID는 나와 타사 계정의 관리자 간에 합의한 숫자 또는 단어가 될 수 있습니다. 이 옵션은 요청에 올바른 `sts:ExternalID`가 포함된 경우에만 사용자가 역할을 맡을 수 있도록 허용하는 조건을 신뢰 정책에 자동으로 추가합니다. 자세한 내용은 AWS 리소스에 대한 액세스를 타사에 부여할 때 외부 ID를 사용하는 방법 (p. 229) 단원을 참조하십시오.

역할을 사용해 권한을 위임하는 방법에 대한 자세한 내용은 역할 용어 및 개념 (p. 175) 단원을 참조하십시오. 서비스 연결을 사용하여 서비스가 해당 계정의 리소스에 액세스할 수 있도록 허용하는 방법은 AWS 서비스에 대한 권한을 위임할 역할 생성 (p. 233) 단원을 참조하십시오.

IAM 역할 만들기(콘솔 사용)

AWS Management 콘솔을 사용해 IAM 사용자가 수임할 수 있는 역할을 만들 수 있습니다. 예를 들면 프로덕션 환경에서 개발 환경을 격리하기 위해 조직이 여러 개의 AWS 계정을 갖고 있다고 가정합시다. 개발 계정의 사용자가 프로덕션 계정의 리소스에 액세스하도록 허용하는 역할을 설정하고 사용하는데 필요한 단계에 대한 자세한 설명을 보려면, 분리된 개발 및 프로덕션 계정을 사용한 예제 시나리오 (p. 179) 단원을 참조하십시오.

역할을 만들려면(콘솔 사용)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 콘솔의 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. 다른 AWS 계정 역할 유형을 선택합니다.
4. 계정 ID에 리소스에 대한 액세스 권한을 부여하려는 AWS 계정 ID를 입력합니다.

   지정된 계정의 관리자는 해당 계정의 IAM 사용자에게 이 역할을 맡을 수 있는 권한을 부여할 수 있습니다. 이를 위해 관리자는 `sts:AssumeRole` 작업에 대한 권한을 부여하는 정책을 사용자나 그룹에 연결합니다. 이 정책은 역할의 ARN을 `Resource`로 지정해야 합니다.
5. 통제권이 없는 계정의 사용자에게 권한을 부여하려면 사용자는 이 역할을 프로그래밍 방식으로 가정하고 Require external ID(외부 ID 필요)를 선택합니다. 외부 ID는 나와 타사 계정의 관리자 간에 합의한 숫자 또는 단어가 될 수 있습니다. 이 옵션은 요청에 올바른 `sts:ExternalID`가 포함된 경우에만 사용자

가 역할을 맡을 수 있도록 허용하는 조건을 신뢰 정책에 자동으로 추가합니다. 자세한 내용은 AWS 리소스에 대한 액세스를 타사에 부여할 때 외부 ID를 사용하는 방법 (p. 229) 단원을 참조하십시오.

Important

이 옵션을 선택하면 AWS CLI, Windows PowerShell용 도구 또는 AWS API를 통해 이 역할로만 액세스가 제한됩니다. 이는 AWS 콘솔을 사용해 해당 신뢰 정책에 `externalId` 조건이 있는 역할로 전환할 수 없기 때문입니다. 하지만 관련 SDK를 통해 스크립트나 애플리케이션을 작성하여 프로그래밍 방식으로 이러한 종류의 액세스를 만들 수 있습니다. 자세한 내용 및 샘플 스크립트는 AWS 보안 블로그의 AWS Management 콘솔에 대한 교차 계정 액세스를 가능하게 하는 방법 단원을 참조하십시오.

6. 멀티 팩터 인증(MFA)으로 로그인하는 사용자로 역할을 제한하려면, Require MFA(MFA 필요)를 선택합니다. 이렇게 하면 MFA 로그인을 확인하는 역할의 신뢰 정책에 조건이 추가됩니다. 역할을 맡으려는 사용자는 구성된 MFA 디바이스에서 임시 일회용 암호로 로그인해야 합니다. MFA 인증을 사용하지 않는 사용자는 역할을 맡을 수 없습니다. MFA에 대한 자세한 내용은 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.
7. Next: Permissions(다음: 권한)을 선택하십시오.
8. IAM은 계정의 AWS 관리형 또는 사용자 관리형 정책 목록을 포함합니다. 권한 정책을 사용하기 위한 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 절차의 4단계 단원을 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아갑니다. 누구든지 역할에게 위임하려는 권한 정책 옆의 확인란을 선택합니다. 원할 경우, 여기서 정책을 선택하지 않고 나중에 정책을 만들어서 역할에 연결할 수 있습니다. 기본적으로 역할은 권한이 없습니다.
9. (선택 사항) 권한 경계 (p. 363)로서 설정됨. 이는 고급 기능입니다.

   Set permissions boundary(권한 경계 설정) 섹션을 열고 Use a permissions boundary to control the maximum role permissions(최대 역할 권한을 관리하기 위한 권한 경계 사용)을 선택합니다. 정책을 선택하여 권한 경계를 사용하십시오.
10. 다음: 태그를 선택합니다.
11. (선택 사항) 태그를 키–값 페어로 연결하여 메타데이터를 역할에 추가합니다. IAM에서의 태그 사용에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
12. [Next: Review]를 선택합니다.
13. Role name에 역할의 이름을 입력합니다. 역할 이름은 AWS 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어, 이름이 **`PRODROLE`**과 **`prodrole`**, 두 가지로 지정된 역할을 만들 수는 없습니다. 기타 AWS 리소스가 역할을 참조할 수 있기 때문에 역할이 생성된 후에는 역할 이름을 편집할 수 없습니다.
14. (선택 사항) [Role description]에 새 역할에 대한 설명을 입력합니다.
15. 역할을 검토한 다음 [Create role]을 선택합니다.

    Important

    필요한 구성의 절반이 끝났습니다. 이제 신뢰할 수 있는 계정의 개별 사용자에게 콘솔의 역할로 전환하거나 역할을 프로그래밍 방식으로 위임할 수 있는 권한을 부여해야 합니다. 이 단계에 대한 자세한 내용은 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

IAM 역할 생성(AWS CLI)

AWS CLI에서 역할을 만들려면 여러 단계를 거쳐야 합니다. 콘솔을 사용하여 역할을 만들 때는 많은 단계가 자동으로 수행되지만 AWS CLI를 사용하면 각 단계를 직접 명시적으로 수행해야 합니다. 역할을 만든 다음 권한 정책을 역할에 할당해야 합니다. 선택적으로 역할에 대한 권한 경계 (p. 363)를 설정할 수 있습니다.

교차 계정 액세스에 대한 역할을 만들려면(AWS CLI)

1. 역할 생성: aws iam create-role
2. 역할에 관리형 권한 정책 연결: aws iam attach-role-policy

또는

역할을 위한 인라인 권한 정책 생성: aws iam put-role-policy

3. (선택 사항) 태그를 연결하여 사용자 지정 속성을 역할에 추가: aws iam tag-role

   자세한 내용은 IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API) (p. 293) 단원을 참조하십시오.
4. (선택 사항) 역할(aws iam put-role-permissions-boundary)에 대한 권한 경계 (p. 363)를 설정합니다.

   이 권한 경계는 역할이 가질 수 있는 최대 권한을 관리합니다. 권한 경계는 고급 AWS 기능입니다.

다음 예는 단순한 환경에서 교차 계정 역할을 생성하는 가장 일반적인 단계 중 첫 두 단계를 보여줍니다. 이 예제는 `123456789012` 계정에 있는 모든 사용자가 역할을 가정하고 `example_bucket` Amazon S3 버킷을 볼 수 있도록 허용합니다. 이 예제에서도 Windows가 구동되는 클라이언트 컴퓨터를 사용 중이며 명령줄 인터페이스를 계정 자격 증명 및 리전으로 이미 구성했다고 가정합니다. 자세한 내용은 AWS 명령줄 인터페이스 구성 단원을 참조하십시오.

이 예제는 역할을 생성할 경우 첫 번째 명령의 다음 신뢰 정책을 포함합니다. 이 신뢰 정책은 `123456789012` 계정에서 사용자가 `AssumeRole` 작업을 사용하여 역할을 가정할 수 있도록 허용합니다. 단, 사용자가 `SerialNumber` 및 `TokenCode` 파라미터를 사용하는 MFA 인증을 제공하는 경우에만 허용합니다. MFA에 대한 자세한 내용은 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "AWS": "arn:aws:iam::123456789012:root" },
    "Action": "sts:AssumeRole",
    "Condition": { "Bool": { "aws:MultiFactorAuthPresent": "true" } }
  }
}
```

Important

`Principal` 요소에 특정 IAM 역할 또는 사용자에 대한 ARN이 포함되어 있으면, 정책을 저장할 때 해당 ARN이 고유 보안 주체 ID로 변환됩니다. 그러면 누군가가 해당 역할 또는 사용자를 제거하고 다시 만들어 본인의 권한을 에스컬레이션할 위험을 완화할 수 있습니다. 일반적으로 콘솔에서는 이 ID가 보이지 않습니다. 신뢰 정책이 표시될 때 해당 ARN으로 다시 역변환되기 때문입니다. 그러나 역할 또는 사용자를 삭제할 경우, 보안 주체 ID가 콘솔에 표시됩니다. AWS에서 더 이상 이를 ARN에 다시 매핑할 수 없기 때문입니다. 따라서 신뢰 정책의 `Principal` 요소에서 참조된 사용자 또는 역할을 삭제하고 다시 생성하는 경우, ARN을 바꾸도록 역할을 편집해야 합니다.

두 번째 명령을 사용할 경우, 기존 관리형 정책을 역할에 연결해야 합니다. 다음 권한 정책에서는 역할을 수임하는 사용자가 `example_bucket` Amazon S3 버킷에서 `ListBucket` 작업만 수행하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example_bucket"
  }
}
```

이 `Test-UserAccess-Role` 역할을 생성하기 위해서는 이전 신뢰 정책을 `trustpolicyforacct123456789012.json` 이름으로 로컬 `policies` 드라이브의 `C:` 폴더에 먼저 저장해야 합니다. 그런 다음 이전 권한 정책을 고객 관리형 정책으로서 `PolicyForRole` 이름으로 AWS 계정에 저장합니다. 그러고 나면 다음 명령을 사용하여 역할을 만들고 관리형 정책을 연결합니다.

```
# Create the role and attach the trust policy file that allows users in the specified
 account to assume the role.
$ aws iam create-role --role-name Test-UserAccess-Role --assume-role-policy-document
 file://C:\policies\trustpolicyforacct123456789012.json

# Attach the permissions policy (in this example a managed policy) to the role to specify
 what it is allowed to do.
$ aws iam attach-role-policy --role-name Test-UserAccess-Role --policy-arn
 arn:aws:iam::123456789012:role/PolicyForRole
```

Important

필요한 구성의 절반이 끝났습니다. 이제 신뢰할 수 있는 계정의 개별 사용자에게 역할로 전환할 수 있는 권한을 부여해야 합니다. 이 단계에 대한 자세한 내용은 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

역할을 만든 다음 AWS 작업을 수행하거나 AWS 리소스에 액세스할 수 있는 권한을 부여해야 `123456789012` 계정의 사용자가 역할을 위임할 수 있습니다. 자세한 내용은 IAM 역할로 전환하기(AWS CLI) (p. 258) 단원을 참조하십시오.

IAM 역할 만들기(AWS API)

AWS API에서 역할을 만들려면 여러 단계를 거쳐야 합니다. 콘솔을 사용하여 역할을 만들 때는 많은 단계가 자동으로 수행되지만 API를 사용하면 각 단계를 직접 명시적으로 수행해야 합니다. 역할을 만든 다음 권한 정책을 역할에 할당해야 합니다. 선택적으로 역할에 대한 권한 경계 (p. 363)를 설정할 수 있습니다.

코드로 역할을 만들려면(AWS API)

1. 역할 만들기: CreateRole

   역할의 신뢰 정책에 대해 파일 위치를 지정할 수 있습니다.
2. 역할에 관리형 권한 정책 연결: AttachRolePolicy

   또는

   역할을 위한 인라인 권한 정책 생성: PutRolePolicy

   Important

   필요한 구성의 절반이 끝났습니다. 이제 신뢰할 수 있는 계정의 개별 사용자에게 역할로 전환할 수 있는 권한을 부여해야 합니다. 이 단계에 대한 자세한 내용은 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.
3. (선택 사항) 태그를 연결하여 사용자 지정 속성을 사용자에게 추가: TagRole

   자세한 내용은 IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API) (p. 293) 단원을 참조하십시오.
4. (선택 사항) 역할(PutRolePermissionsBoundary)에 대한 권한 경계 (p. 363)를 설정합니다.

   이 권한 경계는 역할이 가질 수 있는 최대 권한을 관리합니다. 권한 경계는 고급 AWS 기능입니다.

역할을 만든 다음 AWS 작업을 수행하거나 AWS 리소스에 액세스할 수 있는 권한을 부여해야 계정의 사용자에게 권한을 부여하여 역할을 위임할 수 있습니다. 역할 위임하기에 대한 자세한 내용은 IAM 역할(AWS API)로 전환하기 (p. 263) 단원을 참조하십시오.

AWS 리소스에 대한 액세스를 타사에 부여할 때 외부 ID를 사용하는 방법

이따금 AWS 리소스에 대한 액세스를 타사에 부여해야 할 때가 있습니다(액세스 위임). 이 시나리오의 한 가지 중요한 부분은 IAM 역할 신뢰 정책에서 역할 수임자를 지정하는 데 사용할 수 있는 옵션 정보인 외부 ID입니다.

> **Important**
>
> AWS는 외부 ID를 비밀로 취급하지 않습니다. AWS에서 액세스 키 페어 또는 암호와 같은 비밀 정보를 만든 후에는 다시 볼 수 없습니다. 역할의 외부 ID는 해당 역할을 볼 수 있는 권한을 가진 사람만 볼 수 있습니다.

외부 ID를 사용하려면 선택한 외부 ID로 역할 신뢰 정책을 업데이트합니다. 그런 다음 AWS CLI 또는 AWS API를 사용하여 해당 역할을 수임할 때 외부 ID를 제공해야 합니다.

예를 들어 Example Corp이라는 타사를 고용해 AWS 계정을 모니터링하고 비용을 최적화하기로 했다고 가정해봅시다. 일일 경비를 추적하기 위해 Example Corp은 AWS 리소스에 접근해야 합니다. Example Corp 역시 다른 고객을 위해 다른 많은 AWS 계정을 모니터링합니다.

IAM 사용자 및 AWS 계정의 장기 자격 증명에 대한 액세스 권한을 Example Corp에게 제공하지 마십시오. 대신 IAM 역할과 임시 보안 자격 증명을 사용합니다. IAM 역할은 장기 자격 증명(예: IAM 사용자의 액세스 키)을 공유하지 않고도 AWS 리소스에 액세스할 수 있도록 허용하는 메커니즘을 타사에게 제공합니다.

IAM 역할을 사용하여 AWS 계정과 Example Corp 계정 사이에 신뢰 받는 관계를 설정할 수 있습니다. 이 관계가 설정된 후 Example Corp 계정의 멤버는 AWS STS AssumeRole API를 호출하여 임시 보안 자격 증명을 얻을 수 있습니다. Example Corp 멤버는 자격 증명을 사용하여 계정의 AWS 리소스에 액세스할 수 있습니다.

> **Note**
>
> 임시 보안 자격 증명을 얻기 위해 호출할 수 있는 AssumeRole 및 다른 AWS API 작업에 대한 자세한 내용은 다음(임시 보안 자격 증명 요청하기 (p. 304))을 참조하십시오.

이 시나리오에 대한 더 자세한 분석은 다음과 같습니다.

1. Example Corp을 고용해 고유한 사용자 지정 식별자를 생성하도록 합니다. 이 고유 고객 ID와 AWS 계정 번호를 제공합니다. 이 정보는 다음 단계에서 IAM 역할을 생성하는 데 필요합니다.

   > **Note**
   >
   > 이 식별자가 Example Corp의 각 고객에게 고유한 것이라면 Example Corp는 ExternalId에 대해 그들이 원하는 어떤 문자열 값이라도 사용할 수 있습니다. 두 고객이 같은 값을 갖지 않는 한, 고객 계정 번호 또는 임의 문자열이 될 수 있습니다. 이는 '보안 유지'를 위한 것은 아닙니다. Example Corp은 각 고객에게 ExternalId 값을 제공해야 합니다. 가장 중요한 것은 그들의 고객이 아닌 Example Corp이 그것을 생성해야 한다는 것입니다.

2. AWS에 로그인해 Example Corp에 리소스에 대한 액세스 권한을 부여하는 IAM 역할을 생성합니다. IAM 역할과 마찬가지로 해당 역할에도 권한 정책과 신뢰 정책이라는 2가지 정책이 있습니다. 그 역할의 신뢰 정책은 역할을 위임할 사용자를 지정합니다. 이 예시 시나리오에서 정책은 Example Corp의 AWS 계정 번호를 `Principal`로 지정합니다. 이렇게 하면 계정의 자격 증명이 그 역할을 수임하도록 허용합니다. 또한, `Condition` 요소를 신뢰 정책에 추가합니다. 이 `Condition`은 Example Corp의 고유 고객 ID와 일치하는지 확인하기 위해 `ExternalId` 컨텍스트 키를 테스트합니다. 예를 들면 다음과 같습니다.

```
   "Principal": {"AWS": "Example Corp's AWS Account ID"},
   "Condition": {"StringEquals": {"sts:ExternalId": "Unique ID Assigned by Example
Corp"}}
```

3. 역할에 대한 권한 정책은 해당 역할이 누군가가 수행하도록 허용할 수 있는 작업을 지정합니다. 예를 들어 그 역할은 누군가에게 IAM 사용자나 그룹이 아닌 Amazon EC2 또는 Amazon RDS 리소스만을 관리할 수 있게 허용하도록 지정할 수 있습니다. 이 예시 시나리오에서는 권한 정책을 사용하여 Example Corp에게 계정의 리소스 전체에 대한 읽기 전용 액세스 권한을 부여합니다.
4. 역할을 정의한 후에는 역할의 Amazon 리소스 이름(ARN)을 Example Corp에 제공합니다.
5. Example Corp이 AWS 리소스에 액세스해야 할 때는 그 회사의 누군가가 AWS`sts:AssumeRole` API를 호출합니다. 이 호출에는 수임할 역할의 ARN과 사용자 지정 ID에 해당하는 ExternalId 파라미터가 포함되어 있습니다.

Example Corp의 AWS 계정을 사용하는 사람이 요청을 하는 경우와 역할 ARN 및 외부 ID가 올바른 경우에 요청이 성공합니다. 그 경우 요청은 역할이 허용하는 AWS 리소스에 액세스하기 위해 Example Corp이 사용할 수 있는 임시 보안 자격 증명을 제공합니다.

다시 말해서 역할 정책에 외부 ID가 포함된다면 그 역할을 수임하고자 하는 사용자는 누구든지 그 역할에서 보안 주체로 지정되어야 하고 정확한 외부 ID를 포함해야 합니다.

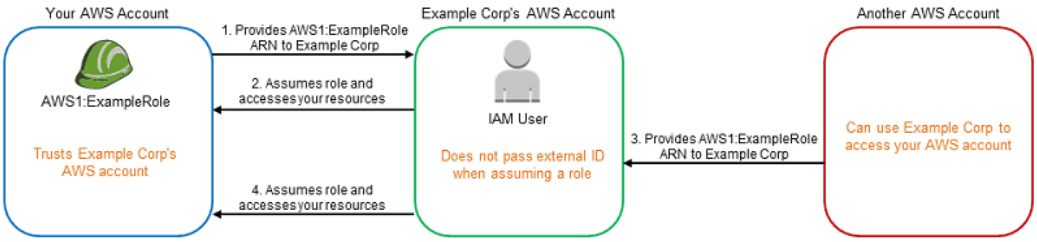
외부 ID를 사용해야 하는 이유는?

추상적인 용어로 말하자면 외부 ID는 그 역할을 위임하고 있는 사용자가 자신이 활동하고 있는 상황을 어설션할 수 있도록 허용합니다. 또한, 계정 소유자가 특정 상황에서만 역할이 위임되도록 허용할 수 있는 방법을 제공합니다. 외부 ID의 주된 기능은 "혼동된 대리자" 문제를 해결하고 방지하는 것입니다.

혼동된 대리자 문제

이전 예시에 이어서 Example Corp은 AWS 계정의 특정 리소스에 대한 액세스 권한이 필요합니다. 그러나 Example Corp에게는 다른 고객도 있으며 각 고객의 AWS 리소스에 액세스할 방법이 필요합니다. 고객들에게 결코 공유되어서는 안 될 비밀인 AWS 계정 액세스 키를 요구하는 대신 Example Corp은 각 사용자에게 역할 ARN을 요청합니다. 하지만 다른 Example Corp 고객은 사용자의 역할 ARN을 추측하거나 얻을 수 있습니다. 해당 고객은 역할 ARN을 사용해 Example Corp을 경유해 AWS 리소스에 대한 액세스 권한을 얻을 수 있습니다. 이러한 형태의 권한 상승은 혼동된 대리자 문제로 알려져 있습니다.

다음 다이어그램은 혼동된 대리자 문제를 보여줍니다.



이 다이어그램은 다음과 같이 가정합니다.

- AWS1은 AWS 계정입니다.
- AWS1:ExampleRole은 계정의 역할입니다. 이 역할의 신뢰 정책은 Example Corp의 AWS 계정의 역할을 위임할 수 있는 것으로 지정함으로써 Example Corp을 신뢰합니다.

다음은 무슨 일이 일어나는지에 대한 것입니다.

1. Example Corp 서비스 사용을 시작할 때 Example Corp에 AWS1:ExampleRole의 ARN을 제공합니다.
2. Example Corp은 그 ARN을 사용해 임시 보안 자격 증명을 얻어 AWS 계정의 리소스에 액세스합니다. 이러한 방식으로 Example Corp을 대신 행위할 수 있는 "대리자"로 신뢰합니다.
3. 또 다른 AWS 고객도 Example Corp의 서비스를 사용하기 시작하고, 이 고객 역시 Example Corp이 사용할 AWS1:ExampleRole의 ARN을 제공합니다. 아마도 그 다른 고객은 비밀이 아닌 AWS1:ExampleRole을 알거나 짐작했을 것입니다.
4. 다른 고객이 Example Corp에게 (자신의 것이라고 주장하는) 계정의 AWS 리소스에 액세스할 수 있는 권한을 요청하면, Example Corp은 AWS1:ExampleRole을 사용해 계정의 리소스에 액세스합니다.

이것이 바로 다른 고객이 리소스에 무단으로 액세스하는 과정입니다. 이 고객은 Example Corp이 자신도 모르게 리소스에 대한 작업을 하도록 속일 수 있었기 때문에 Example Corp은 이제 "혼동된 대리자"가 되었습니다.

외부 ID는 어떻게 혼동된 대리자 문제를 방지할까요?

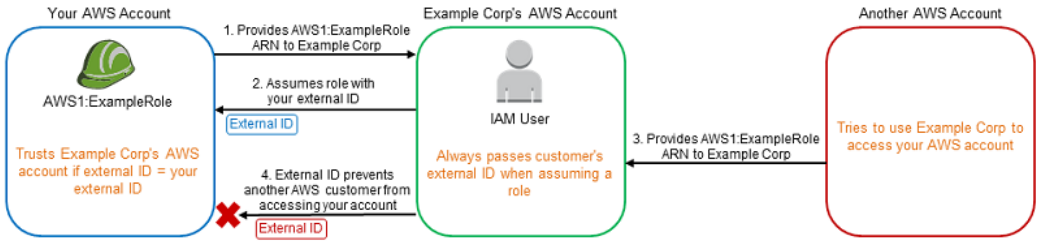
역할의 신뢰 정책에 `ExternalId` 조건 확인을 포함시킴으로써 혼동된 대리자 문제를 해결합니다. "대리자" 회사는 각 고객에 대한 고유 외부 ID 값을 AWS 자격 증명에 대한 요청에 삽입합니다. 외부 ID는 고객 ID 값으로서 Example Corp의 고객 사이에서 고유한 것이어야 하며 Example Corp 고객의 통제를 벗어나 있어야 합니다. 이것이 바로 Example Corp에서 외부 ID를 얻고 그것을 스스로 찾아내지 않는 이유입니다. 이는 다른 고객으로 가장하는 데 성공한 고객을 방지하는 데 도움이 됩니다. Example Corp은 항상 고객의 할당된 외부 ID를 삽입하므로 자신의 것을 제외한 어떤 외부 ID가 포함된 Example Corp의 요청도 결코 눈에 띄어서는 안 됩니다.

이 시나리오에서 Example Corp의 고유 식별자가 "12345"이고, 다른 고객에 대해서는 그 식별자가 "67890"이라고 가정합시다. 이러한 식별자는 이 시나리오를 위해 단순화된 것입니다. 일반적으로 이러한 식별자는 GUID입니다. 이 식별자가 Example Corp의 고객 사이에서 고유한 것이라고 가정할 때, 외부 ID를 위해 사용하기에 합리적인 값들입니다.

Example Corp은 "12345"라는 외부 ID 값을 부여합니다. 그런 다음 `Condition` 값이 12345가 되어야 한다고 요구하는 역할의 신뢰 정책에 `sts:ExternalId` 요소를 다음과 같이 추가해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Principal": {"AWS": "Example Corp's AWS Account ID"},
    "Condition": {"StringEquals": {"sts:ExternalId": "12345"}}
  }
}
```

이 정책의 조건 요소는 AssumeRole API 호출에 "12345"라는 외부 ID 값이 포함될 때만 Example Corp이 역할을 수임하도록 허용합니다. Example Corp은 고객을 대신해 역할을 위임할 때마다 항상 AssumeRole 호출에 해당 고객의 외부 ID 값을 포함하도록 보장합니다. 다른 고객이 Example Corp에게 ARN을 공급한다 하더라도 Example Corp이 AWS에 대한 요청 시 포함하는 외부 ID를 제어할 수 없습니다. 이는 다음 다이어그램에 나와 있듯이 권한을 부여받지 않은 고객이 리소스에 액세스하지 못하도록 방지하는 데 도움이 됩니다.



1. 전과 같이 Example Corp 서비스 사용을 시작할 때 Example Corp에 AWS1:ExampleRole의 ARN을 제공합니다.
2. Example Corp이 그 ARN을 사용해 AWS1:ExampleRole 역할을 위임하는 경우 Example Corp은 AssumeRole API 호출에 외부 ID("12345")를 포함시킵니다. 외부 ID는 역할의 신뢰 정책과 일치하므로 AssumeRole API 호출은 성공하고 Example Corp은 임시 보안 자격 증명을 획득해 AWS 계정의 리소스에 액세스합니다.
3. 또 다른 AWS 고객도 Example Corp의 서비스를 사용하기 시작하고, 전과 같이 이 고객 역시 Example Corp이 사용할 AWS1:ExampleRole의 ARN을 제공합니다.
4. 그러나 이번에는 Example Corp이 AWS1:ExampleRole이라는 역할을 위임하려 할 때 다른 고객과 연결된 외부 ID("67890")를 제공하므로 해당 고객은 이를 바꿀 방법이 없습니다. Example Corp이 이렇게 하는 이유는 역할을 사용하겠다는 요청이 다른 고객에게서 왔으므로, "67890"은 Example Corp이 작용하고 있는 상황을 나타내기 때문입니다. AWS1:ExampleRole의 신뢰 정책에 자신의 외부 ID("12345")가 있는 조건을 추가했기 때문에 AssumeRole API 호출은 실패하고 다른 고객이 계정 리소스에 무단으로 액세스하는 것을 막을 수 있습니다(다이어그램의 빨간색 "X" 참조).

외부 ID는 다른 고객이 Example Corp을 속여 자신도 모르게 리소스에 액세스하지 못하도록 방지함으로써 혼동된 대리자 문제를 완화합니다.

언제 외부 ID를 사용해야 하나요?

다음 상황에서 외부 ID를 사용합니다.

- AWS 계정 소유자이고 다른 AWS 계정에도 액세스하는 타사를 위한 역할을 구성했습니다. 이 경우 타사에 역할을 위임할 때 포함하는 외부 ID를 요청해야 합니다. 그런 다음 역할의 신뢰 정책에서 외부 ID를 확인합니다. 이렇게 하여 외부 사용자를 대신해서 수행하는 경우에만 역할을 맡을 수 있도록 해야 합니다.
- 이전 시나리오의 Example Corp와 같은 다른 고객을 대신하여 역할을 위임할 수 있습니다. 각 고객에게 고유한 외부 ID를 할당하고 외부 ID를 역할의 신뢰 정책에 추가하도록 지시해야 합니다. 그런 다음 역할 위임 요청에 정확한 외부 ID를 항상 포함하도록 해야 합니다.

  각 고객에 대한 고유한 식별자를 이미 갖고 있겠지만, 이 고유 ID는 외부 ID로 사용하기에 충분합니다. 외부 ID는 단지 이러한 목적을 위해 명시적으로 생성하거나 별도로 추적할 필요가 있는 특별한 값은 아닙니다.

  외부 ID는 항상 `AssumeRole` API 호출에 지정해야 합니다. 이 밖에도 고객이 역할 ARN을 부여할 때 정확한 외부 ID가 있든 없든 그 역할을 위임할 수 있는지 확인하십시오. 정확한 외부 ID 없이 역할을 위임할 수 있는 경우 시스템에 고객의 역할 ARN을 저장하지 마십시오. 고객이 정확한 외부 ID를 요구하도록 역할 신뢰 정책을 업데이트할 때까지 기다립니다. 이러한 방식으로 고객이 올바른 일을 할 수 있도록 돕고, 이는 양자 모두 혼동된 대리자 문제에서 보호받는 데 도움이 됩니다.

AWS 서비스에 대한 권한을 위임할 역할 생성

AWS 서비스는 역할을 사용하여 서비스가 사용자를 대신하여 다른 서비스의 리소스로 액세스할 수 있어야 합니다. 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임한 역할을 서비스 역할 (p. 175)이라고 합니다. 역할이 서비스에 대해 특수한 목적을 수행하는 경우 EC2 인스턴스의 서비스 역할 (p. 175) 또는 서비스 연결 역할 (p. 175)로 분류됩니다. 서비스 연결 역할을 사용하여 지원되는 서비스 또는 서비스가 임시 자격 증명의 형식을 지원하는지 여부를 확인하려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 개별 서비스가 역할을 사용하는 방법을 알아보려면 테이블에서 서비스 이름을 선택하여 해당 서비스의 설명서를 확인합니다.

역할을 통해 권한을 위임하는 방법에 대한 자세한 내용은 역할 용어 및 개념 (p. 175) 단원을 참조하십시오.

서비스 역할 권한

IAM 개체(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하거나 편집할 수 있도록 권한을 구성해야 합니다.

> **Note**
>
> 서비스 링크된 역할에 대한 ARN은 정책에서 *`SERVICE-NAME`*`.amazonaws.com`으로 나타내지는 서비스 보안 주체를 포함합니다. 각 경우마다 다르고 AWS 서비스에 따라 형식이 다양하기 때문에 서비스 보안 주체를 알기 어렵습니다. 서비스의 보안 주체를 보려면 해당 서비스 링크된 역할 설명서 단원을 참조하십시오.

IAM 개체가 특정 서비스 연결 역할을 만들 수 있도록 허용하려면

서비스 연결 역할을 생성해야 하는 IAM 개체에 다음 정책을 추가합니다. 이 정책으로 특정 서비스에 대하여 구체적인 이름이 있는 서비스 역할을 만들 수 있습니다. 그런 다음 관리형 또는 인라인 정책을 해당 역할에 연결할 수 있습니다.

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

```
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/SERVICE-ROLE-NAME"
        }
    ]
}
```

IAM 개체가 서비스 연결 역할을 만들 수 있도록 허용하려면

서비스 역할을 생성해야 하는 IAM 개체의 권한 정책에 다음 명령문을 추가합니다. 이 문으로 모든 서비스에 대하여 서비스 역할을 만든 후 관리형 또는 인라인 정책을 해당 역할에 연결할 수 있습니다.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "*"
}
```

IAM 개체가 서비스 역할을 편집할 수 있도록 허용하려면

서비스 연결 역할을 편집해야 하는 IAM 개체에 다음 정책을 추가합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EditSpecificServiceRole",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/SERVICE-ROLE-NAME"
        },
        {
            "Sid": "ViewRolesAndPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicy",
                "iam:ListRoles"
            ],
            "Resource": ""
        }
    ]
}
```

IAM 개체가 특정 서비스 역할을 삭제하도록 허용하려면

특정 서비스 역할을 삭제해야 하는 IAM 개체의 권한 정책에 다음 문장을 추가합니다.

```
{
    "Effect": "Allow",
    "Action": "iam:DeleteRole",
    "Resource": "arn:aws:iam::*:role/SERVICE-ROLE-NAME"
}
```

IAM 개체가 서비스 역할을 삭제하도록 허용하려면

서비스 역할을 삭제해야 하는 IAM 개체의 권한 정책에 다음 명령문을 추가합니다.

```
{
    "Effect": "Allow",
    "Action": "iam:DeleteRole",
    "Resource": "*"
}
```

AWS 서비스에 대한 역할 생성(콘솔)

AWS Management 콘솔을 사용하여 서비스의 역할을 만들 수 있습니다. 일부 서비스는 두 개 이상의 서비스 역할을 지원하기 때문에 어떤 사용 사례를 선택할지 확인하려면 해당 서비스의 AWS 설명서 단원을 참조하십시오. 서비스에서 역할을 위임할 수 있도록 역할에 필요한 신뢰 정책과 권한 정책을 할당하는 방법을 알아볼 수 있습니다. 역할에 대한 권한을 관리할 수 절차는 서비스가 어떻게 사용 사례를 정의하느냐와 서비스 링크된 역할을 생성할 수 있는지 여부에 따라 다양할 수 있습니다.

AWS 서비스에 대한 역할을 만들려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. 신뢰할 수 있는 유형의 엔터티 선택에서 AWS 서비스를 선택합니다.
4. 이 역할을 맡을 수 있게 하려는 서비스를 선택합니다.
5. 서비스의 사용 사례를 선택합니다. 지정한 서비스에 사용 사례가 하나뿐이면 자동으로 선택됩니다. 사용 사례는 서비스에 필요한 신뢰 정책을 포함하기 위해 서비스에서 정합니다. 그런 다음 [Next: Permissions]를 선택합니다.
6. 가능하다면, 권한 정책을 사용하기 위한 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 절차의 4단계 단원을 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아갑니다. 서비스에게 부여하려는 권한 정책 옆의 확인란을 선택합니다.

   선택한 사용 사례에 따라 서비스에서 다음을 수행할 수 있습니다.

   - 서비스에서 역할에 대한 권한을 정의하기 때문에 할 일이 아무것도 없습니다.
   - 제한된 권한 집합에서 선택할 수 있습니다.
   - 모든 권한 집합에서 선택할 수 있도록 허용
   - 여기서 정책을 선택하지 않고, 나중에 정책을 만들어 역할에 연결할 수 있도록 허용
7. (선택 사항) 권한 경계 (p. 363)로서 설정됨. 이는 서비스 역할에서 가능한 고급 기능이며 서비스 링크된 역할은 아닙니다.

   Set permissions boundary(권한 경계 설정) 섹션을 열고 Use a permissions boundary to control the maximum role permissions(최대 사용자 권한을 관리하기 위한 권한 경계 사용)을 선택합니다. IAM에는 계정의 AWS 관리형 또는 사용자 관리형 정책 목록이 있습니다. 권한 경계를 사용하기 위한 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 절차의 4단계 단원을 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아와 권한 경계에 사용할 정책을 선택합니다.

8. 다음: 태그를 선택합니다.
9. (선택 사항) 태그를 키–값 페어로 연결하여 메타데이터를 역할에 추가합니다. IAM에서의 태그 사용에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
10. [Next: Review]를 선택합니다.
11. 역할 이름의 경우 역할 이름 사용자 지정 수준은 서비스에서 정합니다. 서비스에서 역할 이름을 정한 경우 이 옵션을 편집할 수 없습니다. 다른 경우에는 서비스에서 역할 이름의 접두사를 정의하고 사용자가 선택적으로 접미부를 입력하도록 할 수 있습니다. 일부 서비스는 역할의 전체 이름을 지정할 수 있습니다.

    가능하다면 역할 이름 또는 역할 이름 접미사를 입력합니다. 역할 이름은 AWS 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어, 이름이 **`PRODROLE`**과 **`prodrole`**, 두 가지로 지정된 역할을 만들 수는 없습니다. 기타 AWS 리소스가 역할을 참조할 수 있기 때문에 역할이 생성된 후에는 역할 이름을 편집할 수 없습니다.
12. (선택 사항) [Role description]에 새 역할에 대한 설명을 입력합니다.
13. 역할을 검토한 다음 [Create role]을 선택합니다.

서비스에 대한 역할 생성(AWS CLI)

AWS CLI에서 역할을 만들려면 여러 단계를 거쳐야 합니다. 콘솔을 사용하여 역할을 만들 때는 많은 단계가 자동으로 수행되지만 AWS CLI를 사용하면 각 단계를 직접 명시적으로 수행해야 합니다. 역할을 만든 다음 권한 정책을 역할에 할당해야 합니다. 작업 중인 서비스가 Amazon EC2인 경우에도 인스턴스 프로파일을 만들어 거기에 역할을 추가해야 합니다. 선택적으로 역할에 대한 권한 경계 (p. 363)를 설정할 수 있습니다.

AWS CLI에서 AWS 서비스에 대한 역할을 만들려면

1. 역할 생성: aws iam create-role
2. 역할에 관리형 권한 정책 연결: aws iam attach-role-policy

    또는

    역할을 위한 인라인 권한 정책 생성: aws iam put-role-policy
3. (선택 사항) 태그를 연결하여 사용자 지정 속성을 역할에 추가: aws iam tag-role

    자세한 내용은 IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API) (p. 293) 단원을 참조하십시오.
4. (선택 사항) 역할(aws iam put-role-permissions-boundary)에 대한 권한 경계 (p. 363)를 설정합니다.

    이 권한 경계는 역할이 가질 수 있는 최대 권한을 관리합니다. 권한 경계는 고급 AWS 기능입니다.

Amazon EC2 또는 Amazon EC2를 사용하는 다른 AWS 서비스에 대해 역할을 사용할 경우 인스턴스 프로파일에 역할을 저장해야 합니다. 인스턴스 프로파일은 시작할 때 Amazon EC2 인스턴스에 연결할 수 있는 역할을 위한 컨테이너입니다. 하나의 인스턴스 프로파일은 하나의 역할만 포함할 수 있으며 이 제한은 늘릴 수 없습니다. AWS Management 콘솔을 사용하여 역할을 생성한 경우 역할과 동일한 이름을 지닌 인스턴스 프로파일이 자동으로 생성됩니다. 인스턴스 프로파일에 대한 자세한 내용은 인스턴스 프로파일 사용 (p. 271) 단원을 참조하십시오. 역할을 사용하여 EC2 인스턴스를 시작하는 방법에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서에서 Amazon EC2 리소스에 대한 액세스 제어 단원을 참조하십시오.

인스턴스 프로파일을 만들고 여기에 역할을 저장하려면(AWS CLI)

1. 인스턴스 프로파일 생성: aws iam create-instance-profile
2. 인스턴스 프로파일에 역할 추가: aws iam add-role-to-instance-profile

아래 AWS CLI 예제 명령 집합은 역할을 생성하고 권한을 연결하는 첫 두 단계를 보여줍니다. 인스턴스 프로파일을 생성하고 프로필에 역할을 추가하는 두 단계를 보여주기도 합니다. 이 예제 신뢰 정책은 Amazon

EC2 서비스가 역할을 맡고 example_bucket Amazon S3 버킷을 볼 수 있도록 허용합니다. 이 예제에서는 Windows를 실행하는 클라이언트 컴퓨터에서 실행 중이며 계정 자격 증명 및 리전으로 이미 명령줄 인터페이스를 구성했다고도 가정합니다. 자세한 정보는 AWS 명령줄 인터페이스 구성을 참조하십시오.

이 예제는 역할을 생성할 경우 첫 번째 명령의 다음 신뢰 정책을 포함합니다. 이 신뢰 정책은 Amazon EC2 서비스가 역할을 가정하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"Service": "ec2.amazonaws.com"},
    "Action": "sts:AssumeRole"
  }
}
```

두 번째 명령을 사용할 경우, 권한 정책을 역할에 연결해야 합니다. 다음 예제 권한 정책에서는 역할이 example_bucket Amazon S3 버킷에서 ListBucket 작업만 수행하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example_bucket"
  }
}
```

이 Test-Role-for-EC2 역할을 생성하기 위해서는 먼저 이전 신뢰 정책을 trustpolicyforec2.json 이름으로, 이전 권한 정책을 permissionspolicyforec2.json 이름으로 로컬 C: 드라이브의 policies 디렉터리에 저장해야 합니다. 그러고 나면 다음 명령을 사용하여 역할을 만들고 인라인 정책을 연결, 인스턴스 프로파일 생성 및 인스턴스 프로파일에 역할을 추가합니다.

```
# Create the role and attach the trust policy that allows EC2 to assume this role.
$ aws iam create-role --role-name Test-Role-for-EC2 --assume-role-policy-document file://C:
\policies\trustpolicyforec2.json

# Embed the permissions policy (in this example an inline policy) to the role to specify
 what it is allowed to do.
$ aws iam put-role-policy --role-name Test-Role-for-EC2 --policy-name Permissions-Policy-
For-Ec2 --policy-document file://permissionspolicyforec2.json

# Create the instance profile required by EC2 to contain the role
$ aws iam create-instance-profile --instance-profile-name EC2-ListBucket-S3

# Finally, add the role to the instance profile
$ aws iam add-role-to-instance-profile --instance-profile-name EC2-ListBucket-S3 --role-
name Test-Role-for-EC2
```

EC2 인스턴스를 시작할 때 AWS 콘솔을 사용하는 경우 인스턴스 세부 정보 구성 페이지에 인스턴스 프로파일 이름을 지정합니다. aws ec2 run-instances CLI 명령을 사용하는 경우 --iam-instance-profile 파라미터를 지정합니다.

서비스에 대한 역할 생성(AWS API)

AWS API에서 역할을 만들려면 여러 단계를 거쳐야 합니다. 콘솔을 사용하여 역할을 만들 때는 많은 단계가 자동으로 수행되지만 API를 사용하면 각 단계를 직접 명시적으로 수행해야 합니다. 역할을 만든 다음 권한 정책을 역할에 할당해야 합니다. 작업 중인 서비스가 Amazon EC2인 경우에도 인스턴스 프로파일을 만들어 거기에 역할을 추가해야 합니다. 선택적으로 역할에 대한 권한 경계 (p. 363)를 설정할 수 있습니다.

AWS 서비스에 대한 역학을 생성하려면(AWS API)

1. 역할 만들기: CreateRole

   역할의 신뢰 정책에 대해 파일 위치를 지정할 수 있습니다.
2. 역할에 관리형 권한 정책 연결: AttachRolePolicy

   또는

   역할을 위한 인라인 권한 정책 생성: PutRolePolicy
3. (선택 사항) 태그를 연결하여 사용자 지정 속성을 사용자에게 추가: TagRole

   자세한 내용은 IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API) (p. 293) 단원을 참조하십시오.
4. (선택 사항) 역할(PutRolePermissionsBoundary)에 대한 권한 경계 (p. 363)를 설정합니다.

   이 권한 경계는 역할이 가질 수 있는 최대 권한을 관리합니다. 권한 경계는 고급 AWS 기능입니다.

Amazon EC2 또는 Amazon EC2를 사용하는 다른 AWS 서비스에 대해 역할을 사용할 경우 인스턴스 프로파일에 역할을 저장해야 합니다. 인스턴스 프로파일은 역할에 대한 컨테이너입니다. 각 인스턴스 프로파일은 하나의 역할만 포함할 수 있으며 이 제한은 늘릴 수 없습니다. AWS Management 콘솔에서 역할을 생성한 경우 역할과 동일한 이름을 지닌 인스턴스 프로파일이 자동으로 생성됩니다. 인스턴스 프로파일에 대한 자세한 내용은 인스턴스 프로파일 사용 (p. 271) 단원을 참조하십시오. 역할을 사용하여 Amazon EC2 인스턴스를 시작하는 방법에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서에서 Amazon EC2 리소스에 대한 액세스 제어 단원을 참조하십시오.

인스턴스 프로파일을 만들고 여기에 역할을 저장하려면(AWS API)

1. 인스턴스 프로파일 생성: CreateInstanceProfile
2. 인스턴스 프로파일에 역할 추가: AddRoleToInstanceProfile

타사 자격 증명 공급자의 역할 만들기(연동)

AWS 계정에 속하는 IAM 사용자를 생성하는 대신에 자격 증명 공급자를 사용할 수 있습니다. 자격 증명 공급자(IdP)를 사용하면 AWS 외부의 사용자 자격 증명을 관리할 수 있고 이 외부 사용자 자격 증명에 계정의 AWS 리소스에 대한 사용 권한을 부여할 수 있습니다. 연동 및 자격 증명 공급자에 대한 자세한 내용은 자격 증명 공급자 및 연동 (p. 183) 단원을 참조하십시오.

연동 사용자의 역할 만들기(콘솔)

연동 사용자의 역할을 만드는 절차는 타사 공급자들의 선택에 따라 다릅니다.

- 웹 자격 증명 또는 OpenID Connect 연동(OIDC)을 위한 역할 생성은 웹 자격 증명 또는 OpenID Connect 연동을 위한 역할 생성(콘솔) (p. 240) 단원을 참조하십시오.
- SAML 2.0은 SAML 2.0 연동을 위한 역할 생성(콘솔) (p. 244) 단원을 참조하십시오.

연동 액세스의 역할 만들기(AWS CLI)

AWS CLI에서 지원되는 자격 증명 공급자(OIDC 또는 SAML)의 역할을 만드는 절차는 동일합니다. 차이는 필수 선행 단계에서 생성하는 신뢰 정책의 내용에 있습니다. 사용하고 있는 공급자의 유형에 대한 필수 선행 조건 섹션에 나와 있는 절차에서부터 시작하십시오.

- OIDC 공급자의 경우 웹 자격 증명 또는 OIDC의 역할 생성하기 위한 사전 조건 (p. 240) 단원을 참조하십시오.
- SAML 공급자의 경우 SAML 역할 생성하기 위한 사전 조건 (p. 244) 단원을 참조하십시오.

AWS CLI에서 역할을 만들려면 여러 단계를 거쳐야 합니다. 콘솔을 사용하여 역할을 만들 때는 많은 단계가 자동으로 수행되지만 AWS CLI를 사용하면 각 단계를 직접 명시적으로 수행해야 합니다. 역할을 만든 다음 권한 정책을 역할에 할당해야 합니다. 선택적으로 역할에 대한 권한 경계 (p. 363)를 설정할 수 있습니다.

자격 증명 연동의 역할을 만들려면(AWS CLI)

1. 역할 생성: aws iam create-role
2. 역할에 권한 정책 연결: aws iam attach-role-policy

   또는

   역할을 위한 인라인 권한 정책 생성: aws iam put-role-policy
3. (선택 사항) 태그를 연결하여 사용자 지정 속성을 역할에 추가: aws iam tag-role

   자세한 내용은 IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API) (p. 293) 단원을 참조하십시오.
4. (선택 사항) 역할(aws iam put-role-permissions-boundary)에 대한 권한 경계 (p. 363)를 설정합니다.

   이 권한 경계는 역할이 가질 수 있는 최대 권한을 관리합니다. 권한 경계는 고급 AWS 기능입니다.

다음 예는 단순한 환경에서 자격 증명 공급자를 생성하는 가장 일반적인 단계 중 첫 두 단계를 보여줍니다. 이 예제는 `123456789012` 계정에 있는 모든 사용자가 역할을 가정하고 `example_bucket` Amazon S3 버킷을 볼 수 있도록 허용합니다. 또한 이 예는 Windows가 구동중인 컴퓨터에서 AWS CLI를 실행하고 있으며 자격 증명으로 AWS CLI를 이미 구성했다고 가정합니다. 자세한 내용은 AWS Command Line Interface 구성 단원을 참조하십시오.

이 예제는 역할을 생성할 경우 첫 번째 명령의 다음 신뢰 정책을 포함합니다. 이 신뢰 정책은 `123456789012` 계정에서 사용자가 `AssumeRole` 작업을 사용하여 역할을 가정할 수 있도록 허용합니다. 단, 사용자가 `SerialNumber` 및 `TokenCode` 파라미터를 사용하는 MFA 인증을 제공하는 경우에만 허용합니다. MFA에 대한 자세한 내용은 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.

다음 예는 사용자가 Amazon Cognito을 사용하여 로그인하는 경우 모바일 앱에 대해 설계되는 신뢰 정책을 보여줍니다. 이 예시에서 *`us-east:12345678-ffff-ffff-ffff-123456`*은 Amazon Cognito에 의해 할당된 자격 증명 풀 ID를 나타냅니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "RoleForCognito",
        "Effect": "Allow",
        "Principal": {"Federated": "cognito-identity.amazonaws.com"},
        "Action": "sts:AssumeRoleWithWebIdentity",
        "Condition": {"StringEquals": {"cognito-identity.amazonaws.com:aud": "us-
east:12345678-ffff-ffff-ffff-123456"}}
    }
}
```

다음 권한 정책에서는 역할을 수임하는 사용자가 `example_bucket` Amazon S3 버킷에서 `ListBucket` 작업만 수행하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example_bucket"
  }
}
```

이 `Test-Cognito-Role` 역할을 생성하기 위해서는 이전 신뢰 정책을 `trustpolicyforcognitofederation.json` 이름으로 이전 권한 정책을 `permspolicyforcognitofederation.json` 이름으로 로컬 `policies` 드라이브의 `C:` 폴더에 먼저 저장해야 합니다. 그러고 나면 다음 명령을 사용하여 역할을 만들고 인라인 정책을 연결합니다.

```
# Create the role and attach the trust policy that enables users in an account to assume
 the role.
$ aws iam create-role --role-name Test-Cognito-Role --assume-role-policy-document file://C:
\policies\trustpolicyforcognitofederation.json

# Attach the permissions policy to the role to specify what it is allowed to do.
aws iam put-role-policy --role-name Test-Cognito-Role --policy-name Perms-Policy-For-
CognitoFederation --policy-document file://C:\policies\permspolicyforcognitofederation.json
```

연동 액세스의 역할 만들기(AWS API)

AWS CLI에서 지원되는 자격 증명 공급자(OIDC 또는 SAML)의 역할을 만드는 절차는 동일합니다. 차이는 필수 선행 단계에서 생성하는 신뢰 정책의 내용에 있습니다. 사용하고 있는 공급자의 유형에 대한 필수 선행 조건 섹션에 나와 있는 절차에서부터 시작하십시오.

- OIDC 공급자의 경우 웹 자격 증명 또는 OIDC의 역할 생성하기 위한 사전 조건 (p. 240) 단원을 참조하십시오.
- SAML 공급자의 경우 SAML 역할 생성하기 위한 사전 조건 (p. 244) 단원을 참조하십시오.

자격 증명 연동의 역할(AWS API)을 만들려면

1. 역할 만들기: CreateRole
2. 역할에 권한 정책 연결: AttachRolePolicy

   또는

   역할을 위한 인라인 권한 정책 생성: PutRolePolicy
3. (선택 사항) 태그를 연결하여 사용자 지정 속성을 사용자에게 추가: TagRole

   자세한 내용은 IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API) (p. 293) 단원을 참조하십시오.
4. (선택 사항) 역할(PutRolePermissionsBoundary)에 대한 권한 경계 (p. 363)를 설정합니다.

   이 권한 경계는 역할이 가질 수 있는 최대 권한을 관리합니다. 권한 경계는 고급 AWS 기능입니다.

웹 자격 증명 또는 OpenID Connect 연동을 위한 역할 생성(콘솔)

AWS 계정에 IAM 사용자를 생성하는 대신에 웹 자격 증명 연동 또는 OpenID Connect Federation(OIDC) 자격 증명 공급자를 사용할 수 있습니다. 자격 증명 공급자(IdP)를 사용하면 AWS 외부의 사용자 자격 증명을 관리할 수 있고 이 외부 사용자 자격 증명에 계정의 AWS 리소스에 대한 사용 권한을 부여할 수 있습니다. 연동 및 자격 증명 공급자에 대한 자세한 내용은 자격 증명 공급자 및 연동 (p. 183) 단원을 참조하십시오.

웹 자격 증명 또는 OIDC의 역할 생성하기 위한 사전 조건

웹 자격 증명 연동을 위한 역할을 만들기 전에 먼저 다음 필수 선행 단계를 완료해야 합니다.

웹 자격 증명 연동을 위한 역할 만들기를 준비하려면

1. 하나 이상의 IdP를 사용해 개발자로 로그인합니다. AWS 리소스로 액세스가 필요한 앱을 생성하면 공급자 정보로 앱도 구성합니다. 이렇게 하면 공급자는 앱의 고유한 애플리케이션 및 시청자 ID를 제공합니다. 서로 다른 공급자는 이 과정에 대해 서로 다른 용어를 사용합니다. 이 가이드는 앱을 공급자와 동일시하는 과정에 대해 구성이라는 용어를 사용합니다). 각 공급자로 여러 개의 앱을 구성하거나 단일 앱을 통해 다양한 공급자를 구성할 수 있습니다. 자격 증명 공급자에 대한 정보 보기

- Login with Amazon 개발자 센터
- Facebook 개발자 사이트의 앱 또는 웹 사이트에 Facebook 로그인 추가하기
- Google 개발자 사이트의 OAuth 2.0을 사용한 로그인(OpenID Connect)

2. IAM의 자격 증명 공급자로부터 필요한 정보를 가져온 다음 의 자격 증명 공급자를 만들 수 있습니다. 자세한 내용은 OpenID Connect(OIDC) 자격 증명 공급자의 생성 (p. 192) 단원을 참조하십시오.
3. IdP를 통해 인증된 사용자가 맡을 역할에 대한 정책을 준비합니다. 다른 어떤 역할과 마찬가지로 모바일 앱을 위한 역할에는 2개의 정책이 포함됩니다. 하나는 역할을 위임할 사용자를 지정하는 신뢰 정책입니다. 다른 하나는 모바일 앱의 액세스가 허용 또는 거부되는 AWS 작업 및 리소스를 지정하는 권한 정책입니다.

   웹 자격 증명 공급자의 경우, Amazon Cognito를 사용하여 자격 증명을 관리하는 것이 좋습니다. 이 경우 이 예제와 비슷한 신뢰 정책을 사용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {"Federated": "cognito-identity.amazonaws.com"},
        "Action": "sts:AssumeRoleWithWebIdentity",
        "Condition": {
            "StringEquals": {"cognito-identity.amazonaws.com:aud": "us-east-2:12345678-
abcd-abcd-abcd-123456"},
            "ForAnyValue:StringLike": {"cognito-identity.amazonaws.com:amr":
 "unauthenticated"}
        }
    }
}
```

   `us-east-2:12345678-abcd-abcd-abcd-123456`을 Amazon Cognito에서 할당한 자격 증명 풀 ID로 대치합니다.

   신뢰 정책을 생성할 시 웹 자격 증명 IdP를 수동으로 구성하려면 자체 앱만이 이 역할을 수임한다고 보장하는 세 가지 값을 사용해야 합니다.

   - `Action` 요소에 대해서는 `sts:AssumeRoleWithWebIdentity` 작업을 사용하십시오.
   - `Principal` 요소에 대해서는 `{"Federated":`*`providerUrl/providerArn`*`}` 문자열을 사용하십시오.
     - 일부 범용 OpenID Connect(OIDC) IdP의 경우, *`providerUrl`*이 URL입니다. 다음 예제는 일부 범용 IdP에 대해 보안 주체를 지정하는 방법을 포함합니다.

       ```
       "Principal":{"Federated":"cognito-identity.amazonaws.com"}

       "Principal":{"Federated":"www.amazon.com"}

       "Principal":{"Federated":"graph.facebook.com"}

       "Principal":{"Federated":"accounts.google.com"}
       ```

     - 다른 OIDC 공급자의 경우, 다음 예시와 같이 Step 2에서 생성한 OIDC 자격 증명 공급자의 ARN을 사용합니다.

       ```
       "Principal":{"Federated":"arn:aws:iam::123456789012:oidc-provider/
       server.example.com"}
       ```

   - 권한을 제한하려면 `Condition` 요소에 `StringEquals` 조건을 사용합니다. 자격 증명 풀 ID(Amazon Cognito용) 또는 앱 ID(다른 공급자용)를 테스트합니다. 이는 IdP를 통해 앱을 구성할 때 얻은 앱 ID와 일치해야 합니다. 이로써 그 요청이 앱으로부터 오는 것임을 확인합니다. 사용하는 IdP에 따라 다음 예제와 비슷한 조건 요소를 생성합니다.

```
"Condition": {"StringEquals": {"cognito-identity.amazonaws.com:aud": "us-
east:12345678-ffff-ffff-ffff-123456"}}

"Condition": {"StringEquals": {"www.amazon.com:app_id":
"amzn1.application-oa2-123456"}}

"Condition": {"StringEquals": {"graph.facebook.com:app_id":
"111222333444555"}}

"Condition": {"StringEquals": {"accounts.google.com:aud":
"66677788899900pro0"}}
```

OIDC 공급자의 경우 다음 예시와 같이 `aud` 컨텍스트 키로 OIDC IdP의 정규화된 URL을 사용합니다.

```
"Condition": {"StringEquals": {"server.example.com:aud":
"appid_from_oidc_idp"}}
```

역할의 신뢰 정책에서 보안 주체에 대한 값은 하나의 IdP에 고유한 것이라는 점에 유의하십시오. 하나의 역할은 오직 하나의 보안 주체만을 지정할 수 있습니다. 따라서 모바일 앱이 사용자에게 1개 이상의 IdP에서 로그인할 수 있게 허용한다면 지원하고자 하는 각각의 IdP에 대한 개별 역할을 만들어야 합니다. 따라서, 각 IdP에 대한 개별 신뢰 정책을 생성해야 합니다.

다음 예는 사용자가 Login with Amazon에서 로그인하는 경우 모바일 앱에 대해 설계되는 신뢰 정책을 보여줍니다. 예시에서 *amzn1.application-oa2-123456*은 Login with Amazon을 이용해 앱을 구성할 때 Amazon이 할당한 앱 ID를 나타냅니다.

```
{
      "Version": "2012-10-17",
      "Statement": [{
          "Sid": "RoleForLoginWithAmazon",
          "Effect": "Allow",
          "Principal": {"Federated": "www.amazon.com"},
          "Action": "sts:AssumeRoleWithWebIdentity",
          "Condition": {"StringEquals": {"www.amazon.com:app_id": "amzn1.application-
oa2-123456"}}
      }]
  }
```

다음 예는 사용자가 Facebook에서 로그인하는 경우 모바일 앱에 대해 설계되는 신뢰 정책을 보여줍니다. 이 예시에서 *111222333444555*는 Facebook에 의해 할당된 앱 ID를 나타냅니다.

```
{
      "Version": "2012-10-17",
      "Statement": [{
          "Sid": "RoleForFacebook",
          "Effect": "Allow",
          "Principal": {"Federated": "graph.facebook.com"},
          "Action": "sts:AssumeRoleWithWebIdentity",
          "Condition": {"StringEquals": {"graph.facebook.com:app_id":
 "111222333444555"}}
      }]
  }
```

다음 예는 사용자가 Google에서 로그인하는 경우 모바일 앱에 대해 설계되는 신뢰 정책을 보여줍니다. 이 예시에서 *666777888999000*은 Google에 의해 할당된 앱 ID를 나타냅니다.

```
{
      "Version": "2012-10-17",
      "Statement": [{
          "Sid": "RoleForGoogle",
          "Effect": "Allow",
          "Principal": {"Federated": "accounts.google.com"},
          "Action": "sts:AssumeRoleWithWebIdentity",
          "Condition": {"StringEquals": {"accounts.google.com:aud": "666777888999000"}}
      }]
  }
```

다음 예는 사용자가 Amazon Cognito을 사용하여 로그인하는 경우 모바일 앱에 대해 설계되는 신뢰 정책을 보여줍니다. 이 예시에서 *us-east:12345678-ffff-ffff-ffff-123456*은 Amazon Cognito에 의해 할당된 자격 증명 풀 ID를 나타냅니다.

```
{
      "Version": "2012-10-17",
      "Statement": [{
          "Sid": "RoleForCognito",
          "Effect": "Allow",
          "Principal": {"Federated": "cognito-identity.amazonaws.com"},
          "Action": "sts:AssumeRoleWithWebIdentity",
          "Condition": {"StringEquals": {"cognito-identity.amazonaws.com:aud": "us-
east:12345678-ffff-ffff-ffff-123456"}}
      }]
  }
```

웹 자격 증명/OIDC를 위한 역할 생성

사전 요구 사항을 완료한 후에는 IAM에서 역할을 만들 수 있습니다. 다음 절차는 AWS Management 콘솔에서 웹 자격 증명/OIDC에 대한 역할을 만드는 방법을 설명합니다. AWS CLI 또는 AWS API에 역할을 만들려면 타사 자격 증명 공급자의 역할 만들기(연동) (p. 238)의 절차 단원을 참조하십시오.

> **Important**
>
> Amazon Cognito를 사용하고 있는 경우 Amazon Cognito 콘솔을 사용해 역할을 설정해야 합니다. 그렇지 않다면 IAM 콘솔을 사용하여 웹 자격 증명 연동의 역할을 만듭니다.

웹 자격 증명 연동의 IAM 역할을 만들려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 [Roles]를 선택한 후 [Create role]을 선택합니다.
3. 웹 ID 역할 유형을 선택합니다.
4. 자격 증명 공급자에서 역할의 자격 증명 공급자를 선택합니다.
   - 개별 웹 자격 증명 공급자에 대한 역할을 만들 경우, Login with Amazon, Facebook 또는 Google을 선택합니다.

     > **Note**
     >
     > 지원할 각 자격 증명 공급자에 대해 별도의 역할을 만들어야 합니다.

   - Amazon Cognito의 고급 역할을 만드는 경우 Amazon Cognito를 선택합니다.

Note

고급 시나리오에서 작업할 때는 Amazon Cognito로 사용할 역할을 수동으로 만들기만 하면 됩니다. 그렇지 않은 경우 Amazon Cognito가 역할을 대신 만들 수 있습니다. Amazon Cognito에 대한 자세한 내용은 AWS iOS용 Mobile SDK 개발자 안내서의 Amazon Cognito 자격 증명 및 AWS Android용 Mobile SDK 개발자 안내서의 Amazon Cognito 자격 증명 단원을 참조하십시오.

5. 애플리케이션의 ID를 입력합니다. ID의 라벨은 선택한 공급자에 따라 변경됩니다.
   - Login with Amazon에 대한 역할을 만드는 경우 Application ID(애플리케이션 ID) 상자에 애플리케이션 ID를 입력합니다.
   - Facebook에 대한 역할을 만드는 경우 Application ID(애플리케이션 ID) 상자에 애플리케이션 ID를 입력합니다.
   - Google에 대한 역할을 만드는 경우 대상 상자에 대상 사용자 이름을 입력합니다.
   - Amazon Cognito의 역할을 만드는 경우, Amazon Cognito 애플리케이션에 대해 만든 자격 증명 풀의 ID를 자격 증명 풀 ID 상자에 입력합니다.
6. (선택 사항) 애플리케이션 사용자가 역할에서 부여한 권한을 사용하기 위해 충족해야 하는 추가 조건을 만들려면 조건 추가(선택 사항)을 클릭합니다. 예를 들어, 특정 IAM 사용자 ID에만 AWS 리소스에 대한 액세스 권한을 부여하는 조건을 추가할 수 있습니다.
7. 웹 자격 증명 정보를 검토한 후 Next: Permissions(다음: 권한)을 선택합니다.
8. IAM은 계정의 AWS 관리형 또는 사용자 관리형 정책 목록을 포함합니다. 권한 정책을 사용하기 위한 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 절차의 4단계 단원을 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아갑니다. 웹 ID 사용자에게 부여하려는 권한 정책 옆의 확인란을 선택합니다. 원할 경우, 여기서 정책을 선택하지 않고 나중에 정책을 만들어서 역할에 연결할 수 있습니다. 기본적으로 역할은 권한이 없습니다.
9. (선택 사항) 권한 경계 (p. 363)로서 설정됨. 이는 고급 기능입니다.

   Set permissions boundary(권한 경계 설정) 섹션을 열고 Use a permissions boundary to control the maximum role permissions(최대 역할 권한을 관리하기 위한 권한 경계 사용)을 선택합니다. 정책을 선택하여 권한 경계를 사용하십시오.
10. 다음: 태그를 선택합니다.
11. (선택 사항) 태그를 키–값 페어로 연결하여 메타데이터를 역할에 추가합니다. IAM에서의 태그 사용에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
12. [Next: Review]를 선택합니다.
13. 역할 이름에 역할 이름을 입력합니다. 역할 이름은 AWS 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어, 이름이 **`PRODROLE`**과 **`prodrole`**, 두 가지로 지정된 역할을 만들 수는 없습니다. 기타 AWS 리소스가 역할을 참조할 수 있기 때문에 역할이 생성된 후에는 역할 이름을 편집할 수 없습니다.
14. (선택 사항) [Role description]에 새 역할에 대한 설명을 입력합니다.
15. 역할을 검토한 다음 [Create role]을 선택합니다.

SAML 2.0 연동을 위한 역할 생성(콘솔)

AWS 계정에 속하는 IAM 사용자를 생성하는 대신에 SAML 2.0 연동을 사용할 수 있습니다. 자격 증명 공급자(IdP)를 사용하면 AWS 외부의 사용자 자격 증명을 관리할 수 있고 이 외부 사용자 자격 증명에 계정의 AWS 리소스에 대한 사용 권한을 부여할 수 있습니다. 연동 및 자격 증명 공급자에 대한 자세한 내용은 자격 증명 공급자 및 연동 (p. 183) 단원을 참조하십시오.

SAML 역할 생성하기 위한 사전 조건

SAML 2.0 연동을 위한 역할을 만들기 전에 먼저 다음 필수 선행 단계를 완료해야 합니다.

SAML 2.0 연동을 위한 역할 생성을 준비하려면

1. SAML 기반 연동 역할을 만들기 전에 IAM에서 SAML 공급자를 만들어야 합니다. 자세한 내용은 IAM SAML 자격 증명 공급자 생성 (p. 198) 단원을 참조하십시오.
2. SAML 2.0 인증 사용자들이 맡을 역할에 대한 정책을 준비합니다. 다른 어떤 역할과 마찬가지로 SAML 연동을 위한 역할에는 2개의 정책이 포함됩니다. 하나는 역할을 맡을 수 있는 사용자를 지정하는 역할 신뢰 정책이고, 다른 하나는 연동 사용자의 액세스가 허용 또는 거부되는 AWS 작업 및 리소스를 지정하는 IAM 권한 정책입니다.

   역할에 대한 신뢰 정책을 생성할 시 애플리케이션에만 위임될 수 있는 역할을 보장하는 세 가지 값을 사용해야 합니다.

   - `Action` 요소에 대해서는 `sts:AssumeRoleWithSAML` 작업을 사용하십시오.
   - `Principal` 요소에 대해서는 `{"Federated":`*`ARNofIdentityProvider`*`}` 문자열을 사용하십시오. *`ARNofIdentityProvider`*를 Step 1에서 만든 SAML 자격 증명 공급자 (p. 188)의 ARN으로 바꿉니다.
   - `Condition` 요소에 대해서는 `StringEquals` 조건을 사용하여 SAML 응답의 `saml:aud` 속성이 AWS에 대한 SAML 연동 엔드포인트와 일치하는지 테스트하십시오.

   다음 예는 SAML 연동 사용자를 위해 설계된 신뢰 정책입니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
      "Effect": "Allow",
      "Action": "sts:AssumeRoleWithSAML",
      "Principal": {"Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-
provider/PROVIDER-NAME"},
      "Condition": {"StringEquals": {"SAML:aud": "https://signin.aws.amazon.com/saml"}}
    }
  }
```

   보안 주체 ARN을 IAM에서 만든 SAML 공급자의 실제 ARN으로 바꿉니다. ARN에는 고유의 계정 ID와 공급자 이름이 있습니다.

SAML 역할 생성

사전 조건 단계를 완료한 후에는 SAML 기반 연동을 위한 역할을 생성합니다.

SAML 기반 연동을 위한 역할을 생성하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. SAML 2.0 federation(SAML 2.0 연동) 역할 유형을 선택합니다.
4. SAML provider(SAML 공급자)에서 역할의 공급자를 선택합니다.
5. SAML 2.0 액세스 수준 방법을 선택합니다.

   - Allow programmatic access only(프로그래밍 방식의 액세스만 허용)을 선택하여 AWS API 또는 AWS CLI에서 프로그래밍 방식으로 위임할 수 있는 역할을 만듭니다.
   - 그런 다음 Allow programmatic and AWS Management 콘솔 access(프로그래밍 방식 및 콘솔 액세스 허용)를 선택하여 콘솔에서 프로그래밍 방식으로 수임할 수 있는 역할을 생성합니다.

이렇게 생성된 두 역할은 비슷하지만 콘솔에서 위임할 수도 있는 역할에는 특정 조건을 포함하는 신뢰 정책을 포함합니다. 이 조건은 SAML 대상(`SAML:aud` 속성)이 SAML에 대한 AWS 로그인 엔드포인트(https://signin.aws.amazon.com/saml)로 설정되도록 명시적으로 보장합니다.

6. 프로그래밍 방식 액세스를 위한 역할을 만드는 경우, 속성 목록에서 속성을 선택합니다. 그런 다음 값 상자에 역할에 포함시킬 값을 입력합니다. 이렇게 하면 지정한 속성을 포함하는 SAML 인증 응답(어설션)을 소유한 자격 증명 공급자의 사용자로 역할 액세스가 제한됩니다. 하나 이상의 속성을 지정해야 역할이 조직의 일부 사용자 집합으로 제한됩니다.

   프로그래밍 방식 액세스 및 콘솔 액세스를 위한 역할을 만드는 경우, `SAML:aud` 속성이 자동으로 추가되고 AWS SAML 엔드포인트의 URL(https://signin.aws.amazon.com/saml)로 설정됩니다.
7. 신뢰 정책에 속성 관련 조건을 더 추가하려면 조건 추가(선택 사항)을 선택하고 추가 조건을 선택한 후 값을 지정합니다.

   Note

   이 목록에는 가장 많이 사용되는 SAML 속성을 포함합니다. IAM은 조건을 만드는 데 사용할 수 있는 추가 속성을 지원합니다. (지원되는 속성 목록은 IAM JSON 정책 요소 참조 (p. 586) 주제의 SAML 연동에 사용할 수 있는 키 단원을 참조하십시오.) 목록에는 없지만 지원되는 SAML 속성의 조건이 필요한 경우, 해당 조건을 수동으로 추가할 수 있습니다. 이렇게 하려면 역할을 만든 후 신뢰 정책을 편집합니다.
8. SAML 2.0 신뢰 정보를 검토한 후 Next: Permissions(다음: 권한)을 선택합니다.
9. IAM은 계정의 AWS 관리형 또는 사용자 관리형 정책 목록을 포함합니다. 권한 정책을 사용하기 위한 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 정책 만들기(콘솔) (p. 436) 절차의 4단계 단원을 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아갑니다. 웹 ID 사용자에게 부여하려는 권한 정책 옆의 확인란을 선택합니다. 원할 경우, 여기서 정책을 선택하지 않고 나중에 정책을 만들어서 역할에 연결할 수 있습니다. 기본적으로 역할은 권한이 없습니다.
10. (선택 사항) 권한 경계 (p. 363)로서 설정됨. 이는 고급 기능입니다.

    Set permissions boundary(권한 경계 설정) 섹션을 열고 Use a permissions boundary to control the maximum role permissions(최대 역할 권한을 관리하기 위한 권한 경계 사용)을 선택합니다. 정책을 선택하여 권한 경계를 사용하십시오.
11. 다음: 태그를 선택합니다.
12. (선택 사항) 태그를 키–값 페어로 연결하여 메타데이터를 역할에 추가합니다. IAM에서의 태그 사용에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
13. [Next: Review]를 선택합니다.
14. 역할 이름에 역할 이름을 입력합니다. 역할 이름은 AWS 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어, 이름이 **`PRODROLE`**과 **`prodrole`**, 두 가지로 지정된 역할을 만들 수는 없습니다. 기타 AWS 리소스가 역할을 참조할 수 있기 때문에 역할이 생성된 후에는 역할 이름을 편집할 수 없습니다.
15. (선택 사항) [Role description]에 새 역할에 대한 설명을 입력합니다.
16. 역할을 검토한 다음 [Create role]을 선택합니다.

역할을 만든 후, AWS에 대한 정보로 자격 증명 공급자 소프트웨어를 구성하여 SAML 신뢰를 완료합니다. 이 정보는 연합된 사용자가 사용했으면 하는 역할을 포함합니다. 이를 가리켜 IdP와 AWS 간 신뢰 당사자 신뢰 구성이라고 합니다. 자세한 내용은 신뢰 당사자 신뢰로 SAML 2.0 IdP를 구성하고 클레임 추가하기 (p. 201) 단원을 참조하십시오.

액세스 권한 위임을 위한 정책의 예

다음 예제는 AWS 계정의 리소스에 대한 액세스를 AWS 계정에게 허용 또는 부여하는 방법을 보여줍니다. 이러한 예제 JSON 정책 문서를 사용하여 IAM 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

주제

역할을 사용하여 다른 AWS 계정의 리소스에 대한 액세스 권한 위임하기

IAM역할을 사용하여 한 계정의 사용자에게 다른 계정의 AWS 리소스에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 자습서: IAM 역할을 사용한 AWS 계정 간 액세스 권한 위임 (p. 30) 단원을 참조하십시오.

> **Important**
>
> 역할 신뢰 정책의 `Principal` 요소에 특정 역할이나 사용자에 대한 ARN을 포함할 수 있습니다. 정책을 저장하면 AWS가 ARN을 고유한 보안 주체 ID로 변환합니다. 그러면 누군가가 해당 역할 또는 사용자를 제거하고 다시 만들어 본인의 권한을 에스컬레이션할 위험을 완화할 수 있습니다. 일반적으로 콘솔에서는 이 ID가 보이지 않습니다. 신뢰 정책이 표시될 때 해당 ARN으로 다시 역변환되기 때문입니다. 그러나 해당 역할 또는 사용자를 삭제하면 관계가 깨집니다. 사용자 또는 역할을 다시 만들더라도 해당 정책이 더 이상 적용되지 않습니다. 신뢰 정책에 저장된 보안 주체 ID와 일치하지 않기 때문입니다. 이 경우 보안 주체 ID가 콘솔에 표시됩니다. AWS에서 더 이상 이를 ARN에 다시 매핑할 수 없기 때문입니다. 결과적으로 신뢰 정책의 `Principal` 요소에서 참조된 사용자 또는 역할을 삭제하고 다시 생성하는 경우, ARN을 바꾸도록 역할을 편집해야 합니다. 그러면 정책을 저장할 때 ARN이 새 보안 주체 ID로 변환됩니다.

정책을 사용하여 서비스에 대한 액세스 권한 위임

다음 예제는 역할에 연결할 수 있는 정책을 보여줍니다. 이 정책은 Amazon EMR 서비스와 AWS Data Pipeline 서비스가 역할을 수행할 수 있도록 합니다. 그러면 서비스가 해당 역할에 할당된 권한 정책에서 부여한 모든 작업을 수행할 수 있습니다(표시되지 않음). 여러 서비스 보안 주체를 지정할 때 `Service` 요소를 두 개 지정하면 안 됩니다. 하나만 지정할 수 있습니다. 대신 여러 서비스 보안 주체의 배열을 하나의 `Service` 요소의 값으로 사용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "elasticmapreduce.amazonaws.com",
          "datapipeline.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

리소스 기반의 정책을 사용하여 다른 계정의 Amazon S3 버킷에 대한 액세스 권한 위임하기

이 예에서 계정 A는 리소스 기반 정책(Amazon S3 버킷 정책)을 사용하여 계정 B에게 계정 A의 S3 버킷에 액세스할 수 있는 완전한 권한을 부여합니다. 그런 다음 계정 B는 IAM 사용자 정책을 생성하여 계정 A의 버킷에 대한 해당 액세스 권한을 계정 B의 사용자 중 하나에게 위임합니다.

계정 A의 S3 버킷 정책은 다음 정책과 같을 수 있습니다. 이 예에서 계정 A의 S3 버킷 이름은 mybucket이고, 계정 B의 계정 번호는 111122223333입니다. 계정 B에서는 개별 사용자 또는 그룹을 지정하지 않고 오직 계정 자체만 지정할 뿐입니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AccountBAccess1",
    "Effect": "Allow",
    "Principal": {"AWS": "111122223333"},
    "Action": "s3:*",
    "Resource": [
      "arn:aws:s3:::mybucket",
      "arn:aws:s3:::mybucket/*"
    ]
  }
}
```

또는 계정 A가 Amazon S3 액세스 제어 목록(ACL)을 사용하여 계정 B에 S3 버킷 또는 버킷 내 단일 객체에 대한 액세스 권한을 부여할 수 있습니다. 이 경우 유일한 변경 사항은 계정 A가 계정 B에게 액세스 권한을 부여하는 방식입니다. 이 예의 다음 부분에서 설명한 것처럼 계정 B는 여전히 정책을 사용하여 계정 B의 IAM 그룹에게 액세스 권한을 위임합니다. S3 버킷과 객체에 대한 액세스를 제어하는 자세한 방법을 보려면 Amazon Simple Storage Service 개발자 가이드의 액세스 제어를 참조하십시오.

계정 B의 관리자는 다음 정책 샘플을 생성할 수 있습니다. 이 정책은 계정 B의 그룹 또는 사용자에게 읽기 액세스를 허용하며, 이전 정책은 B 계정에 대한 액세스 권한을 부여합니다. 하지만 계정 B의 개별 그룹과 사용자는 그룹 또는 사용자 정책이 리소스에 대한 권한을 명시적으로 부여할 때까지는 그 리소스에 액세스할 수 없습니다. 이 정책의 권한은 이전 교차 계정 정책에 있는 권한의 하위 집합에 불과할 수 있습니다. 계정 B는 첫 번째 정책에서 계정 A가 계정 B에게 부여한 권한보다 더 많은 권한을 자신의 그룹 또는 사용자에게 위임할 수 없습니다. 이 정책에서 `Action` 요소는 `List` 작업만을 허용하도록 명시적으로 정의되고 이 정책의 `Resource` 요소는 계정 A에 의해 적용되는 버킷 정책의 `Resource`와 일치합니다.

이 정책을 적용하기 위해 계정 B는 IAM을 사용하여 이 정책을 계정 B의 해당 사용자(또는 그룹)에게 연결합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:List*",
    "Resource": [
      "arn:aws:s3:::mybucket",
      "arn:aws:s3:::mybucket/*"
    ]
  }
}
```

리소스 기반의 정책을 사용하여 다른 계정의 Amazon SQS 대기열에 대한 액세스 권한 위임하기

다음 예에서 계정 A에는 계정 B에 대한 액세스 권한을 대기열에 부여하기 위해 대기열에 연결된 리소스 기반 정책을 사용하는 Amazon SQS 대기열이 있습니다. 그러면 계정 B는 IAM 그룹 정책을 사용하여 계정 B의 그룹에게 액세스 권한을 위임합니다.

다음 대기열 정책의 예는 계정 A의 queue1 대기열에서 2014년 11월 30일 정오부터 오후 3시까지만 `SendMessage` 및 `ReceiveMessage` 작업을 수행할 수 있는 권한을 계정 B에 부여합니다. 계정 B의 계정 번호는 1111-2222-3333입니다. 계정 A는 Amazon SQS를 사용하여 이 정책을 적용합니다.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"AWS": "111122223333"},
    "Action": [
      "sqs:SendMessage",
      "sqs:ReceiveMessage"
    ],
    "Resource": ["arn:aws:sqs:*:123456789012:queue1"],
    "Condition": {
      "DateGreaterThan": {"aws:CurrentTime": "2014-11-30T12:00Z"},
      "DateLessThan": {"aws:CurrentTime": "2014-11-30T15:00Z"}
    }
  }
}
```

계정 B의 그룹에게 액세스 권한을 위임하기 위한 계정 B의 정책은 다음 예와 같을 수 있습니다. 계정 B는 IAM을 사용하여 이 정책을 그룹(또는 사용자)에게 연결합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sqs:*",
    "Resource": "arn:aws:sqs:*:123456789012:queue1"
  }
}
```

앞의 IAM 사용자 정책에 대한 예시에서 계정 B는 와일드카드를 사용하여 해당 사용자에게 계정 A의 대기열에서 모든 Amazon SQS 작업을 수행할 수 있는 액세스 권한을 부여했습니다. 하지만 계정 B는 액세스 권한이 부여된 범위까지만 액세스 권한을 위임할 수 있습니다. 두 번째 정책이 있는 계정 B 그룹은 2014년 11월 30일 정오부터 오후 3시까지만 대기열에 액세스할 수 있습니다. 사용자는 계정 A 및 Amazon SQS 대기열 정책에 정의된 대로 `SendMessage` 및 `ReceiveMessage` 작업만 수행할 수 있습니다.

계정이 액세스 거부될 경우 액세스 권한을 위임할 수 없음

다른 계정에서 사용자의 상위 계정에 대한 액세스를 명시적으로 거부할 경우 AWS 계정은 다른 계정의 리소스에 대한 액세스 권한을 위임할 수 없습니다. 이 거부는 사용자가 액세스 권한을 부여하는 기존 정책을 가지고 있는지 여부에 상관없이 해당 계정의 사용자에게 전파됩니다.

계정 A가 계정 A의 S3 버킷에 계정 A의 버킷에 대한 계정 B의 액세스를 명시적으로 거부하는 버킷 정책을 계정 A의 S3 버킷에 작성하는 경우를 예로 들어 보겠습니다. 계정 B는 계정 B의 사용자에게 계정 A의 버킷에 대한 액세스 권한을 부여하는 IAM 사용자 정책을 작성합니다. 계정 A의 S3 버킷에 적용된 명시적 거부는 계정 B의 사용자에게 전파되고 계정 B의 사용자에게 액세스 권한을 부여하는 IAM 사용자 정책보다 우선합니다. (권한 평가 방식에 대한 자세한 내용은 정책 평가 로직 (p. 622)을 참조하십시오.)

계정 A의 버킷 정책은 다음과 같을 수 있습니다. 이 예에서 계정 A의 S3 버킷 이름은 mybucket이고, 계정 B의 계정 번호는 1111-2222-3333입니다. 계정 A는 Amazon S3를 사용하여 이 정책을 적용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AccountBDeny",
    "Effect": "Deny",
    "Principal": {"AWS": "111122223333"},
    "Action": "s3:*",
    "Resource": "arn:aws:s3:::mybucket/*"
  }
}
```

이 명시적 거부는 계정 A의 S3 버킷에 액세스할 수 있는 권한을 제공하는 계정 B의 모든 정책을 재정의합니다.

IAM 역할 사용

IAM 사용자, 애플리케이션 또는 서비스에서 이전에 생성한 역할을 사용하려면 그 역할로 전환할 수 있는 권한을 부여해야 합니다. IAM 사용자 그룹 중 하나 또는 사용자 자신에게 추가된 어떤 정책도 필요한 권한을 부여하는 데 사용할 수 있습니다. 이 단원에서는 역할 사용 권한을 사용자에게 부여하는 방법과 사용자가 AWS Management 콘솔, Windows PowerShell용 도구, AWS Command Line Interface(AWS CLI) 및 `AssumeRole` API를 사용하여 원하는 역할로 전환하는 방법을 살펴보겠습니다.

> **Important**
>
> IAM 콘솔 대신 프로그래밍 방식으로 역할을 생성하는 경우에는 사용자의 선택에 따라 최대 64자인 `RoleName`뿐만 아니라 최대 512자인 `Path`도 추가할 수 있습니다. 그러나 AWS 콘솔에서 Switch Role(역할 전환) 기능이 있는 역할을 사용하려면 `Path`와 `RoleName`을 합해 64자를 초과할 수 없습니다.

AWS Management 콘솔에서 역할을 전환할 수 있습니다. AWS CLI 또는 API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 위임할 수 있습니다. 사용한 방법에 따라 역할을 수임할 수 있는 사용자와 역할 세션의 지속 가능 기간이 결정됩니다.

역할 사용을 위한 방법 비교

방법	역할을 위임할 수 있는 사용자	자격 증명의 수명을 지정하는 방법	자격 증명의 수명 (최소 | 최대 | 기본)
AWS Management 콘솔	IAM 사용자(역할 전환을 통해 (p. 256))	없음	1시간 | 1시간 | 1시간
`assume-role` CLI 또는 `AssumeRole` API 작업	IAM 사용자 또는 역할[1]	`duration-seconds` CLI 또는 `DurationSeconds` API 파라미터	15분 | 최대 세션 기간 설정[2] | 1시간
`assume-role-with-saml` CLI 또는 `AssumeRoleWithSAML` API 작업	SAML을 사용하여 인증된 모든 사용자	`duration-seconds` CLI 또는 `DurationSeconds` API 파라미터	15분 | 최대 세션 기간 설정[2] | 1시간
`assume-role-with-web-identity` CLI 또는 `AssumeRoleWithWebIdentity` API 작업	웹 자격 증명 공급자를 사용하여 인증된 모든 사용자	`duration-seconds` CLI 또는 `DurationSeconds` API 파라미터	15분 | 최대 세션 기간 설정[2] | 1시간
`AssumeRole`로 구성된 콘솔 URL (p. 210)	IAM 사용자 또는 역할	URL의 `SessionDuration` HTML 파라미터	15분 | 12시간 | 1시간
`AssumeRoleWithSAML`로 구성된 콘솔 URL (p. 210)	SAML을 사용하여 인증된 모든 사용자	URL의 `SessionDuration` HTML 파라미터	15분 | 12시간 | 1시간
`AssumeRoleWithWebIdentity`로 구성된 콘솔 URL (p. 210)	웹 자격 증명 공급자를 사용하여 인증된 모든 사용자	URL의 `SessionDuration` HTML 파라미터	15분 | 12시간 | 1시간

[1] 하나의 역할이 자격 증명을 사용하여 다른 역할을 위임하는 것을 역할 함께 묶기 (p. 176)라고 합니다. 역할 함께 묶기를 사용하는 경우 새 자격 증명의 유효 기간은 최대 1시간으로 제한됩니다. 역할을 사용하여 EC2 인스턴스에서 실행되는 애플리케이션에 권한을 부여 (p. 265)하는 경우, 이러한 애플리케이션에는 이 제한이 적용되지 않습니다.

[2] 최대 세션 기간은 콘솔 AWS CLI 또는 API에서 역할에 적용할 수 있는 설정입니다. 이 설정은 CLI 또는 API에서 역할을 수임할 때 역할에 대한 최대 세션 기간을 지정합니다. 이 설정에는 1~12시간의 값을 지정할 수 있습니다. 최대 세션 기간 설정에 대한 자세한 내용은 역할 변경 (p. 274) 단원을 참조하십시오. 이 설정은 역할 자격 증명을 얻을 때 요청할 수 있는 최대 세션 기간을 결정합니다. 예를 들어 AssumeRole* API 작업을 사용하여 역할을 위임할 때 `DurationSeconds` 파라미터를 사용하여 세션 길이를 지정할 수 있습니다. 이 파라미터를 사용하여 역할 세션 기간을 900초(15초)에서 해당 역할에 대한 최대 세션 기간 설정까지 지정합니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 이 페이지 뒷부분에 나오는 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오.

> **Note**
>
> 최대 세션 기간은 `AssumeRole*` API 작업 또는 `assume-role*` CLI 명령을 사용하여 생성된 세션에만 적용됩니다. 이 설정은 AWS 서비스에서 수임하는 세션을 제한하지 않습니다.

주제

역할에 대한 최대 세션 기간 설정 보기

AWS CLI 또는 API 작업을 사용하여 역할을 위임하는 경우 `DurationSeconds` 파라미터에 대한 값을 지정할 수 있습니다. 이 파라미터를 사용하여 역할 세션 기간을 900초(15초)에서 해당 역할에 대한 Maximum CLI/API session duration(최대 CLI/API 세션 기간) 설정까지 지정할 수 있습니다. 이 파라미터를 지정하기 전에 역할에 대한 이 설정을 확인해야 합니다. `DurationSeconds` 파라미터의 값을 최대 설정보다 높게 지정하면 작업에 실패합니다.

역할의 최대 세션 기간을 보려면(콘솔)

1. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다.
2. 보려는 역할의 이름을 선택합니다.
3. Maximum CLI/API session duration(최대 CLI/API 세션 기간) 옆에서 AWS CLI 또는 API 작업에서 지정할 수 있는 최대 세션 길이를 확인합니다.

역할의 최대 세션 기간 설정을 보려면(AWS CLI)

1. 수임할 역할의 이름을 모르는 경우 다음 명령을 실행하여 계정의 역할을 나열합니다.
   - aws iam list-roles
2. 역할에 대한 현재 최대 세션 기간 설정을 확인하려면 다음 명령을 실행합니다. 그런 다음 최대 세션 기간 파라미터를 확인합니다.
   - aws iam get-role

역할의 최대 세션 기간 설정을 보려면(AWS API)

1. 수임할 역할의 이름을 모르는 경우 다음 연산을 호출하여 계정의 역할을 나열합니다.
   - ListRoles
2. 역할에 대한 현재 최대 세션 기간 설정을 확인하려면 다음 연산을 실행합니다. 그런 다음 최대 세션 기간 파라미터를 확인합니다.
   - GetRole

사용자에 대한 역할 전환 권한 부여

교차 계정 액세스가 가능한 역할을 생성하려면 (p. 226) 역할 및 리소스가 저장된 계정(신뢰하는 계정)에서 사용자가 저장된 계정(신뢰 받는 계정)으로 신뢰를 구성합니다. 이 작업을 수행하려면 역할의 신뢰 정책에서 신뢰할 수 있는 계정 번호를 `Principal`로 지정합니다. 이렇게 하면 신뢰할 수 있는 계정의 잠재적 사용자라면 누구든지 역할을 위임할 수 있습니다. 구성을 완료하려면 신뢰 받는 계정의 관리자는 계정에 속한 특정 그룹 또는 사용자에게 역할 전환 권한을 부여해야 합니다.

사용자에게 역할 전환 권한을 부여하려면 새로운 사용자 정책을 생성하거나 기존 정책을 편집하여 필요한 요소를 추가해야 합니다. 그런 다음 이미 세부 정보가 모두 작성되어 있는 Switch Role(역할 전환) 페이지로 이동할 수 있는 링크를 사용자에게 보낼 수 있습니다. 그 밖에도 계정 ID 번호 또는 역할이 저장된 계정 별칭 및 역할 이름을 사용자에게 제공할 수 있습니다. 이제 사용자는 Switch Role(역할 전환) 페이지로 이동하여 세부 정보를 직접 입력합니다. 사용자의 역할 전환 방법에 대한 세부 정보는 역할 전환(콘솔) (p. 256)을 참조하십시오.

IAM 사용자로 로그인할 때만 역할을 바꿀 수 있다는 점에 유의하십시오. AWS 계정 루트 사용자로 로그인할 때는 역할을 바꿀 수 없습니다.

> Important
>
> AWS Management 콘솔에서의 역할을 ExternalId (p. 229) 값이 필요한 역할로 전환할 수 없습니다. `ExternalId` 파라미터를 지원하는 AssumeRole API를 호출해야만 이러한 역할로 변경할 수 있습니다.
>
> 참고
>
> - 이 주제는 사용자에 대한 정책들을 다루고 있는데, 이는 AWS가 사용자에게 작업을 완수할 수 있는 권한을 최종적으로 부여하고 있기 때문입니다. 그러나 개별 사용자에게 직접 권한을 부여하지 않는 것이 최상의 관행 (p. 61)입니다. 관리를 더 쉽게 하려면 IAM 그룹에 정책을 배정하고 권한을 부여한 다음 적절한 그룹들의 구성원인 사용자들을 생성하도록 권장합니다.
> - AWS Management 콘솔에서 역할을 전환하는 경우, 콘솔은 항상 원래 자격 증명을 사용하여 전환을 승인합니다. 이는 IAM 사용자, SAML 연동 역할 또는 웹 자격 증명 연동 역할 중 어느 것으로 로그인하는지 여부에 관계없이 적용됩니다. 예를 들어, RoleA로 전환하는 경우 원래 사용자 자격 증명 또는 연동 역할 자격 증명을 사용하여 RoleA를 부여할지 여부를 결정합니다. RoleA를 사용하는 중에 RoleB로 전환하려는 경우, RoleA의 자격 증명이 아닌, 원래 사용자 또는 연동 역할 자격 증명이 인증에 사용됩니다.

주제

- 정책 생성 또는 편집 (p. 252)
- 사용자에 대한 정보 제공 (p. 253)

정책 생성 또는 편집

역할을 맡기 위한 사용자 권한을 부여하는 정책에는 다음에 적용되는 `Allow` 문이 포함되어야 합니다.

- `sts:AssumeRole` 작업

- `Resource` 요소에 있는 역할의 ARN(Amazon Resource Name)

다음 예제를 참조하십시오. 그 정책을 가져오는(그룹 멤버십 또는 직접 첨부를 통해) 사용자들은 지정된 역할로 전환하도록 허용됩니다.

> **Note**
>
> `Resource`가 `*`로 설정된 경우에는 사용자 계정을 신뢰하는 어떤 계정의 어떤 역할이라도 사용자가 수임할 수 있다는 점에 유의하십시오(역할의 신뢰 정책은 사용자의 계정을 `Principal`로 지정합니다). 최소 권한의 원칙에 따라 사용자에게 필요한 역할에 대해서만 완전한 ARN을 지정하는 것이 좋습니다.

다음 예제에서는 단 한 개의 계정에서 사용자가 역할을 맡을 수 있는 정책을 보여 줍니다. 또한 이 정책은 와일드카드(*)를 사용하여 역할 이름이 `Test` 문자로 시작할 경우에만 사용자가 역할을 전환할 수 있도록 지정합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/Test*"
  }
}
```

> **Note**
>
> 이 역할이 사용자에게 부여하는 권한은 사용자에게 이미 부여된 권한에 추가되지는 않습니다. 사용자가 어떤 역할로 전환할 때는 일시적으로 자신의 원래 권한을 버리고 그 역할이 부여하는 권한으로 갈아탑니다. 사용자가 역할을 끝내면 원래 사용자 권한이 자동으로 회복됩니다. 사용자 권한에서 Amazon EC2 인스턴스 작업을 허용하지만, 역할의 권한 정책이 해당 권한을 부여하지 않는 경우를 예로 들어 보겠습니다. 이 경우 역할을 사용할 때 사용자가 콘솔에서 Amazon EC2 인스턴스 작업을 수행할 수 없습니다. 또한 `AssumeRole`을 통해 받은 임시 자격 증명은 프로그래밍 방식으로 Amazon EC2 인스턴스 작업을 수행할 수 없습니다.

사용자에 대한 정보 제공

역할을 만들어 이 역할로 전환하는 권한을 사용자에게 부여한 후, 사용자에게 다음을 제공해야 합니다.

- 역할 이름
- 해당 역할을 포함하는 계정 ID 번호 또는 계정 별칭

계정 ID와 역할 이름이 미리 구성되어 있는 링크를 사용자에게 보내주는 것이 더 간편합니다. 이 역할 링크는 역할 생성 마법사의 마지막 페이지, 또는 교차 계정 역할의 Role Summary(역할 요약) 페이지에 있습니다.

> **Note**
>
> AWS CLI, Windows PowerShell용 도구, 또는 AWS API로 역할을 생성하는 경우에는, 이름뿐만 아니라 경로도 지닌 역할을 생성할 수 있습니다. 이렇게 하기 위해서는 AWS Management 콘솔의 역할 전환 페이지에 입력할 수 있도록 사용자에게 전체 경로와 역할 이름을 제공해야 합니다. 예: `division_abc/subdivision_efg/role_XYZ`.

> **Important**
>
> IAM 콘솔 대신 프로그래밍 방식으로 역할을 생성하는 경우에는 `RoleName` 외에 `Path`(최대 512자)도 추가할 수 있습니다. `RoleName` 길이는 최대 64자입니다. 그러나 AWS 콘솔에서 역할 전환 기능이 있는 역할을 사용하려면 `Path`와 `RoleName`을 합해 64자를 초과할 수 없습니다.

다음 형식을 사용해 링크를 수동으로 구축할 수도 있습니다. 다음과 같이 계정 ID 또는 별칭과 역할 이름을 요청의 파라미터 2개로 대치하십시오.

```
https://signin.aws.amazon.com/switchrole?
account=YourAccountIDorAliasHere&roleName=pathIfAny/YourRoleNameHere
```

사용자가 역할 전환(콘솔) (p. 256) 주제에서 프로세스를 살펴볼 수 있도록 기회를 제공하는 것이 좋습니다.

> **Note**
>
> 보안상의 목적으로 AWS CloudTrail을 사용해 역할 전환을 감사할 수 있습니다. CloudTrail이 계정에서 활성화되어 있는 경우 IAM이 역할의 임시 보안 자격 증명을 사용해 수행되는 작업을 로깅합니다. 자세한 내용은 AWS CloudTrail User Guide의 CloudTrail이벤트 참조를 참조하십시오.

사용자에게 AWS 서비스에 역할을 전달할 권한 부여

다수의 AWS 서비스를 구성하려면 IAM 역할을 서비스에 전달해야 합니다. 그러면 서비스가 나중에 역할을 수임하고 사용자 대신 작업을 수행할 수 있습니다. 서비스가 역할을 수임할 때마다가 아니라 설정 중에 한 번만 역할을 서비스에 전달해야 합니다. 예를 들어 Amazon EC2 인스턴스에서 실행 중인 애플리케이션이 있다고 가정합니다. 해당 애플리케이션에는 인증을 위한 임시 자격 증명과 AWS에서 작업을 수행할 수 있는 애플리케이션을 승인할 권한이 필요합니다. 애플리케이션을 설정할 때는 역할을 EC2에 전달하여 해당 자격 증명을 제공하는 인스턴스와 함께 사용해야 합니다. IAM 정책을 역할에 연결하여 인스턴스에서 실행 중인 애플리케이션에 대한 권한을 정의합니다. 애플리케이션은 역할이 허용하는 작업을 수행해야 할 때마다 역할을 수임합니다.

AWS 서비스에 역할(및 그 권한)을 전달하려면 사용자에게 서비스에 역할을 전달할 권한이 있어야 합니다. 이를 통해 관리자는 승인된 사용자만 권한이 부여된 역할을 통해 서비스를 구성하도록 할 수 있습니다. 사용자가 AWS 서비스에 역할을 전달하도록 하려면 해당 사용자의 IAM 사용자, 역할 또는 그룹에 `PassRole` 권한을 부여해야 합니다.

> **Note**
>
> `ResourceTag/`*`key-name`* 조건 키를 사용하는 역할에 연결된 태그를 기반으로 하는 역할을 전달할 권한을 제한할 수는 없습니다. 자세한 내용은 AWS 리소스에 대한 액세스 제어 (p. 385) 단원을 참조하십시오.

서비스 연결 역할을 생성하는 경우 해당 역할을 서비스에 전달할 권한도 있어야 합니다. 일부 서비스는 서비스에서 작업을 수행할 때 계정에 서비스 연결 역할을 자동으로 생성합니다. 예를 들어 Amazon EC2 Auto Scaling에서는 사용자가 Auto Scaling 그룹을 처음으로 생성할 때 사용자를 대신해 `AWSServiceRoleForAutoScaling` 서비스 연결 역할을 생성합니다. `PassRole` 권한 없이 Auto Scaling 그룹을 생성하려고 하면 오류가 발생합니다. 서비스 연결 역할을 지원하는 서비스를 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 서비스에서 작업 수행 시 자동으로 서비스 연결 역할을 생성하는 서비스를 알아보려면 예 링크를 선택하고 해당 서비스에 대한 서비스 연결 역할 설명서를 확인합니다.

사용자는 역할을 사용하여 서비스에 권한을 할당하는 API 작업에서 파라미터로 역할 ARN을 전달할 수 있습니다. 그런 다음 서비스는 해당 사용자에게 `iam:PassRole` 권한이 있는지 확인합니다. 사용자가 승인된 역할만 전달하도록 제한하려면 IAM 정책 문의 `Resources` 요소로 `iam:PassRole` 권한을 필터링하면 됩니다.

예 1

인스턴스를 시작한 후 사용자에게 Amazon EC2 서비스에 승인된 역할 집합을 전달할 수 있는 권한을 부여하려 한다고 가정하겠습니다. 다음 세 가지 요소가 필요합니다.

- 역할이 수행할 수 있는 작업을 결정하는, 역할에 연결된 IAM권한 정책입니다. 역할이 수행해야 하는 작업 및 역할이 그러한 작업을 수행하는 데 필요한 리소스만으로 권한을 한정할 수 있습니다. AWS 관리형 또는 고객이 생성한 IAM 권한 정책을 사용할 수 있습니다.

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

```
        "Effect": "Allow",
        "Action": [ "A list of the permissions the role is allowed to use" ],
        "Resource": [ "A list of the resources the role is allowed to access" ]
    }
}
```

- 서비스에서 역할을 위임하도록 허용하는 역할에 대한 신뢰 정책입니다. 예를 들어, `UpdateAssumeRolePolicy` 작업이 있는 역할에 다음과 같은 신뢰 정책을 연결할 수 있습니다. 이 신뢰 정책을 통해 Amazon EC2는 해당 역할 및 해당 역할과 연결된 권한을 사용할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "TrustPolicyStatementThatAllowsEC2ServiceToAssumeTheAttachedRole",
        "Effect": "Allow",
        "Principal": { "Service": "ec2.amazonaws.com" },
       "Action": "sts:AssumeRole"
    }
}
```

- 사용자가 승인된 역할만 전달하도록 허용하는 IAM 사용자에 연결된 IAM 권한 정책입니다. 사용자가 전달할 역할의 세부 정보를 얻을 수 있도록 `iam:PassRole`은 일반적으로 `iam:GetRole`과 함께 제공됩니다. 이 예제에서 사용자는 지정된 계정에 있으며 다음과 같이 이름이 `EC2-roles-for-XYZ-`로 시작하는 역할만 전달할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:GetRole",
            "iam:PassRole"
        ],
        "Resource": "arn:aws:iam::<account-id>:role/EC2-roles-for-XYZ-*"
    }]
}
```

이제 사용자는 할당된 역할로 Amazon EC2 인스턴스를 시작할 수 있습니다. 이 인스턴스에서 실행되는 애플리케이션은 인스턴스 프로파일 메타데이터를 통해 역할의 임시 자격 증명에 액세스할 수 있습니다. 역할과 연결된 권한 정책은 인스턴스가 수행할 수 있는 작업을 결정합니다.

예 2

Amazon Relational Database Service(Amazon RDS)는 확장 모니터링이라는 기능을 지원합니다. 이 기능을 사용하면 Amazon RDS에서 에이전트를 사용하여 데이터베이스 인스턴스를 모니터링할 수 있습니다. 또한 Amazon RDS에서 Amazon CloudWatch Logs에 측정치를 기록할 수도 있습니다. 이 기능을 사용하려면 서비스 역할을 생성하여 로그에 대한 측정치를 모니터링하고 작성할 수 있는 권한을 Amazon RDS에 부여해야 합니다.

Amazon RDS Enhanced Monitoring에 대한 역할을 만들려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 역할을 선택한 다음 역할 생성을 선택합니다.
3. AWS 서비스 역할 유형을 선택한 후 확장 모니터링을 위한 Amazon RDS 역할(Amazon RDS Role for Enhanced Monitoring) 서비스를 선택합니다. 그런 다음 [Next: Permissions]를 선택합니다.
4. AmazonRDSEnhancedMonitoringRole, 권한 정책을 선택합니다.
5. 다음: 태그를 선택합니다.

6. (선택 사항) 태그를 키-값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서의 태그 사용에 대한 자세한 정보는 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오.
7. [Next: Review]를 선택합니다.
8. 역할 이름에서 이 역할의 목적을 나타내는 역할 이름을 입력합니다. 역할 이름은 AWS 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어, 이름이 **PRODROLE**과 **prodrole**, 두 가지로 지정된 역할을 만들 수는 없습니다. 다양한 주체가 역할을 참조할 수 있기 때문에 역할이 생성된 후에는 역할 이름을 편집할 수 없습니다.
9. (선택 사항) 역할 설명에 새 역할에 대한 설명을 입력합니다.
10. 역할을 검토한 다음 [Create role]을 선택합니다.

그러면 역할이 `monitoring.rds.amazonaws.com` 서비스에 해당 역할을 수임할 권한을 부여하는 신뢰 정책을 자동으로 얻습니다. 그러면 Amazon RDS는 `AmazonRDSEnhancedMonitoringRole` 정책에서 허용하는 모든 작업을 수행할 수 있습니다.

사용자가 Enhanced Monitoring을 활성화하려면 이 사용자가 역할을 전달하도록 허용하는 다음과 같은 문이 포함된 정책이 필요합니다. 계정 번호를 사용하여 역할 이름을 3단계에서 입력한 이름으로 바꿉니다.

```
{
    "Sid": "PolicyStatementToAllowUserToPassOneSpecificRole",
    "Effect": "Allow",
    "Action": [ "iam:PassRole" ],
    "Resource": "arn:aws:iam:::role/RDS-Monitoring-Role"
}
```

이 문을 다른 정책의 문과 결합하거나 고유 정책에 포함시킬 수 있습니다. 사용자가 `RDS-`로 시작하는 모든 역할을 전달할 수 있도록 지정하려면 다음과 같이 리소스 ARN의 역할 이름을 와일드카드로 바꿉니다.

```
    "Resource": "arn:aws:iam:::role/RDS-*"
```

역할 전환(콘솔)

역할은 필요한 AWS 리소스에 액세스하는 데 사용할 수 있는 일련의 권한을 지정합니다. 이러한 의미에서 AWS Identity and Access Management(IAM) 사용자와 비슷하다고 할 수 있습니다. 사용자로 로그인할 때는 특정 권한이 부여됩니다. 하지만 역할로 로그인하지는 못하기 때문에 일단 로그인한 후에 역할로 전환할 수 있습니다. 이 경우 초기의 사용자 권한은 잠시 무효화되고 역할에게 할당된 권한이 부여됩니다. 역할은 자신의 계정에나 그 밖에 다른 AWS 계정에도 속할 수 있습니다. 역할, 역할의 이점 및 생성 방법에 대한 자세한 내용은 다음(IAM역할 (p. 174) 및 IAM 역할 생성 (p. 225))을 참조하십시오.

> **Important**
>
> IAM 사용자의 권한과 전환 대상인 역할의 권한은 누적되지 않습니다. 한 번에 오직 하나의 권한 집합만이 활성화됩니다. 어떤 역할로 전환할 때 사용자 권한은 일시적으로 포기하고 역할에 할당된 권한을 가지고 작업합니다. 역할을 끝내면 사용자 권한이 자동으로 회복됩니다.

기본적으로 AWS Management 콘솔 세션은 한 시간 동안 지속됩니다.

AWS Management 콘솔에서 역할을 전환하는 경우, 콘솔은 항상 원래 자격 증명을 사용하여 전환을 승인합니다. 이는 IAM 사용자, SAML 연동 역할 또는 웹 자격 증명 연동 역할 중 어느 것으로 로그인하는지 여부에 관계없이 적용됩니다. 예를 들어, RoleA로 전환하는 경우 IAM에서는 원래 사용자 자격 증명 또는 연동 역할 자격 증명을 사용하여 RoleA를 부여할지 여부를 결정합니다. RoleA를 사용하는 중에 RoleB로 전환하는 경우에도 IAM에서는 RoleA의 자격 증명이 아닌, 원래 사용자 자격 증명 또는 연동된 역할 자격 증명을 사용하여 전환을 승인합니다.

이 단원에서는 IAM 콘솔을 사용한 역할 전환 방법을 설명합니다.

- IAM 사용자로 로그인할 때만 역할을 바꿀 수 있습니다. AWS 계정 루트 사용자로 로그인할 경우 역할을 바꿀 수 없습니다.

- 관리자가 링크를 제공하는 경우 다음 절차에서 링크를 선택하여 Step 5 단계로 넘어갑니다. 링크를 클릭하면 적절한 웹 페이지로 이동하고 계정 ID(또는 별칭)와 역할 이름이 채워집니다.
- 링크를 수동으로 구성한 후 다음 절차의 Step 5 단계로 건너뛸 수 있습니다. 링크를 구성하려면 다음 형식을 사용합니다.

  ```
  https://signin.aws.amazon.com/switchrole?
  account=account_id_number&roleName=role_name&displayName=text_to_display
  ```

  여기서 다음 텍스트를 바꿉니다.

  - *account_id_number*–관리자가 제공한 12자리 계정 식별자. 또는 URL에 계정 ID 대신 계정 이름이 포함되도록 관리자가 계정 별칭을 생성할 수 있습니다. 자세한 내용은 AWS 계정 ID 및 별칭 (p. 77)를 참조하십시오.
  - *role_name*–수임하려는 역할의 이름입니다. 이 이름은 역할의 ARN 끝에서 가져올 수 있습니다. 예를 들어 역할 ARN: `TestRole`에서 수임하려는 역할의 이름은 `namearn:aws:iam::403299380220:role/TestRole`입니다.
  - (선택 사항) *text_to_display*–이 역할이 활성화되었을 때 탐색 표시줄에 사용자 이름 대신 표시되도록 하고 싶은 텍스트를 입력할 수 있습니다.
- 관리자가 제공하는 정보를 사용하여 아래 절차를 통해 역할을 수동으로 전환할 수 있습니다.

역할을 수임할 때 발생할 수 있는 일반적인 문제를 해결하려면 역할을 위임할 수 없음 (p. 552) 단원을 참조하십시오.

역할을 전환하려면(콘솔)

1. IAM 사용자로 AWS Management 콘솔에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔에서 상단 오른쪽 모서리에 있는 탐색 표시줄에서 사용자 이름을 선택합니다. 일반적인 형식은 ***username*@*account_ID_number_or_alias***입니다.
3. [Switch Role]을 선택합니다. 이 옵션을 처음 선택하면 자세한 정보를 제공하는 페이지가 나타납니다. 그 정보를 읽은 후에 역할 전환(Switch Role)을 클릭합니다. 브라우저 쿠키를 청소하면 이 페이지가 다시 나타나게 할 수 있습니다.
4. 역할 전환 페이지에서 계정 ID 번호 또는 계정 별칭 및 관리자가 제공한 역할 이름을 입력합니다.

   Note

   관리자가 경로를 포함하여 역할을 생성한 경우(예: `division_abc/subdivision_efg/roleToDoX`)에는 역할 상자에 전체 경로와 이름을 입력해야 합니다. 역할 이름만 입력하는 경우 또는 결합된 `Path` 및 `RoleName`이 64자를 초과하는 경우 역할 전환에 실패합니다. 이것은 역할 이름을 저장하는 브라우저 쿠키의 한계입니다. 이러한 경우 관리자에게 문의해 경로 및 역할 이름의 크기를 줄여 달라고 요청하십시오.
5. (선택 사항) 이 역할이 활성화되었을 때 탐색 표시줄에 사용자 이름 대신 표시되도록 하려는 텍스트를 입력할 수 있습니다. 이름은 계정 및 역할 정보에 따라 다르게 제시되지만 특별한 의미를 갖도록 직접 변경하는 것도 가능합니다. 또한, 표시되는 이름이 돋보이도록 색상을 선택할 수도 있습니다. 이름과 색상은 이 역할이 활성화되어 권한이 변경되는 시점을 다시 한 번 알려줍니다. 예를 들어 테스트 환경에 대한 액세스 권한을 부여하는 역할에 대해 표시 이름을 **`Test`**로 지정하고 색상은 녹색으로 선택합니다. 프로덕션에 대한 액세스 권한을 부여하는 역할에 대해서는 표시 이름을 **`Production`**으로 지정하고 색상은 빨간색으로 선택합니다.
6. [Switch Role]을 선택합니다. 표시 이름과 색상이 탐색 표시줄에 사용자 이름 대신 나타나고, 역할에서 부여하는 권한을 사용하여 시작할 수 있습니다.

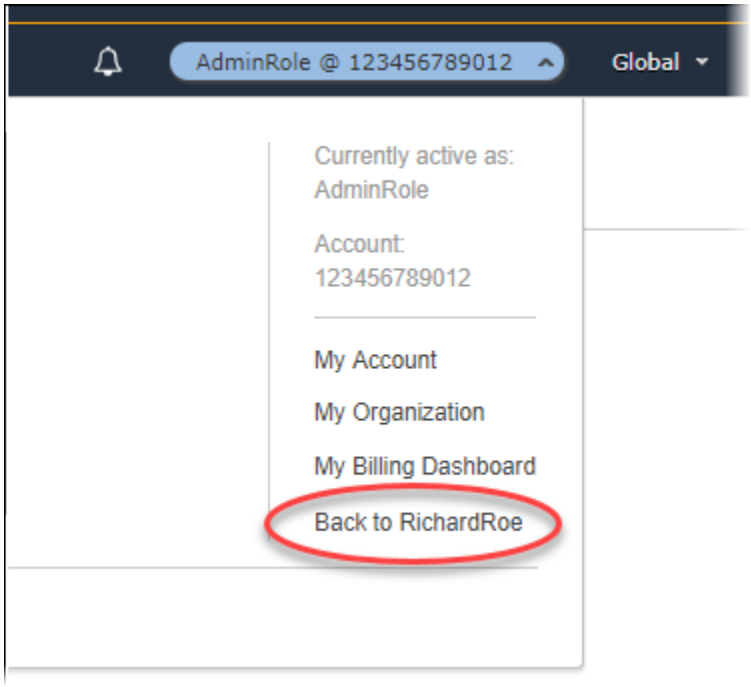
   도움말

   마지막으로 사용한 몇 가지 역할은 [ ] 메뉴에 표시됩니다. 다음에 이 중 하나로 역할을 전환해야 할 때는 원하는 역할을 선택하기만 하면 됩니다. 역할이 자격 증명 메뉴에 표시되지 않으면 계정 및 역할 정보를 수동으로 입력하면 됩니다.

역할 사용을 중지하려면(콘솔)

1. IAM 콘솔의 탐색 모음 오른쪽 위쪽에서 역할의 표시 이름을 선택합니다. 일반적인 형식은 ***rolename*@*account_ID_number_or_alias***입니다.
2. Back to ***username***(***username***으로 돌아가기)을 선택합니다. 역할과 그 권한이 비활성화되면서 IAM 사용자 및 그룹에 연결된 권한이 자동으로 복구됩니다.

   예를 들어, 사용자 이름 `123456789012`을 사용하여 계정 번호 `RichardRoe`로 로그인했다고 가정하십시다. `AdminRole` 역할을 사용한 후, 사용자가 역할 사용을 중지하고 원래 사용자 권한으로 돌아가고자 합니다. 역할 사용을 중지하려면 AdminRole @ 123456789012을 선택한 후 Back to RichardRoe(RichardRoe로 돌아가기)를 선택합니다.



IAM 역할로 전환하기(AWS CLI)

역할은 필요한 AWS 리소스에 액세스하는 데 사용할 수 있는 일련의 권한을 지정합니다. 이러한 의미에서 AWS Identity and Access Management(IAM) 사용자와 비슷하다고 할 수 있습니다. 사용자로 로그인할 때는 특정 권한이 부여됩니다. 하지만 역할로 로그인하지는 못하기 때문에 일단 사용자로 로그인한 후에 역할로 전환할 수 있습니다. 이 경우 초기의 사용자 권한은 잠시 무효화되고 역할에게 할당된 권한이 부여됩니다. 역할은 자신의 계정 또는 그 밖의 다른 AWS 계정에 속한 것일 수 있습니다. 역할과 역할의 이점, 역할 생성 및 구성 방법에 대한 자세한 내용은 IAM역할 (p. 174) 및 IAM 역할 생성 (p. 225) 단원을 참조하십시오. 역할을 수임하는 데 사용할 수 있는 여러 방법을 알아보려면 IAM 역할 사용 (p. 250) 단원을 참조하십시오.

> Important
>
> IAM 사용자의 권한과 수임한 역할의 권한은 누적되지 않습니다. 한 번에 오직 하나의 권한 집합만이 활성화됩니다. 어떤 역할을 수임할 때 이전 사용자 또는 역할 권한은 일시적으로 포기하고 해당 역할에 할당된 권한을 가지고 작업합니다. 역할을 끝내면 사용자 권한이 자동으로 회복됩니다.

IAM 사용자로 로그인한 경우 역할을 사용하여 AWS CLI 명령을 실행할 수 있습니다. 이미 사용 중인 외부 인증 사용자 (p. 183)(SAML (p. 188) 또는 OIDC (p. 183))로 로그인하는 경우에도 역할을 사용해 AWS CLI명령을 실행할 수 있습니다. 또한 역할을 사용해 인스턴스 프로파일 전체에서 명령에 연결된 Amazon EC2 인스턴스 내에서 AWS CLI 명령을 실행할 수 있습니다. 또한 역할을 사용해 두 번째 역할을 수임하는 역할 함께 묶기 (p. 176)를 사용할 수도 있습니다. AWS 계정 루트 사용자로 로그인되어 있을 때는 역할을 수임할 수 없습니다.

기본적으로 역할 세션은 한 시간 동안 지속됩니다. `assume-role*` CLI 작업을 사용하여 역할을 수임하는 경우 `duration-seconds` 파라미터에 대한 값을 지정할 수 있습니다. 이 값의 범위는 900초(15분)에서 해당 역할에 대한 최대 세션 기간 설정까지일 수 있습니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오.

역할 함께 묶기를 사용하는 경우 세션 기간은 최대 1시간으로 제한됩니다. 그런 다음 `duration-seconds` 파라미터를 사용하여 1시간보다 큰 값을 입력하면 이 작업에 실패합니다.

예제 시나리오: 프로덕션 역할로 전환

개발 환경에서 IAM 사용자를 하나 갖고 있는데 이따금 AWS CLI 명령줄에서 프로덕션 환경으로 작업해야 할 때가 있다고 가정합니다. 사용할 수 있는 액세스 키 자격 증명 세트가 이미 하나 있습니다. 이 세트는 표준 IAM 사용자에게 할당된 액세스 키 페어일 수도 있고, 연동 사용자로 로그인한 경우에는 초기에 할당된 역할에 대한 액세스 키 페어일 수도 있습니다. 현재 권한에 의해 특정 IAM 역할을 수임할 수 있는 능력이 부여되는 경우, AWS CLI 구성 파일의 "profile"에서 해당 역할을 식별할 수 있습니다. 그런 다음 해당 명령은 원래 자격 증명이 아닌 지정된 IAM 역할의 권한으로 실행됩니다. AWS CLI 명령에서 해당 프로파일을 지정하는 경우에는 새 역할을 사용하게 됩니다. 이 경우 개발 계정의 원래 권한을 동시에 사용할 수 없습니다. 한 번에 한 가지 권한 세트만 적용될 수 있기 때문입니다.

> **Note**
>
> 계정에서 보안을 목적으로 AWS CloudTrail을 사용해 계정의 역할 사용을 감사할 수 있습니다. CloudTrail 로그에서 역할의 작업을 식별하기 위해 역할 세션 이름을 사용할 수 있습니다. 이 항목에서 설명하는 것처럼 AWS CLI에서 사용자를 대신해 역할을 수임하면 역할 세션 이름이 `AWS-CLI-session-`*`nnnnnnnn`*으로 자동으로 생성됩니다. 여기서 *`nnnnnnnn`*은 Unix epoch time(1970년 1월 1일 자정 UTC 이후 경과된 초 수)으로 시간을 나타낸 정수입니다. 자세한 내용은 AWS CloudTrail User Guide의 CloudTrail 이벤트 참조를 참조하십시오.

프로덕션 역할로 전환(AWS CLI)

1. AWS CLI를 사용한 적이 없을 경우 먼저 기본 CLI 프로필을 구성해야 합니다. 명령 프롬프트를 열고 IAM 사용자 또는 연동 역할에서 액세스 키를 사용하도록 AWS CLI 설치를 설정하십시오. 자세한 내용은 AWS Command Line Interface 사용 설명서의 AWS Command Line Interface 구성을 참조하십시오.

   ```
   $ aws configure
       AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
       AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
       Default region name [None]: us-east-2
       Default output format [None]: json
   ```

2. Unix 또는 Linux의 `.aws/config` 파일, 또는 Windows의 `C:\Users\USERNAME\.aws\config` 파일에서 역할에 대한 새 프로필을 만듭니다. 다음 예에서는 `123456789012` 계정의 *`ProductionAccessRole`* 역할로 전환하는 `prodaccess`라는 프로필을 만듭니다. 해당 역할을 만든 계정 관리자에게서 역할 ARN을 받습니다. 이 프로필이 호출되면 AWS CLI에서는 `source_profile`의 자격 증명을 사용하여 해당 역할의 자격 증명을 요청합니다. 이로 인해 `role_arn`로 참조되는 자격 증명에는 `source_profile`에 지정된 역할에 대한 `sts:AssumeRole` 권한이 있어야 합니다.

   ```
   [profile prodaccess]
       role_arn = arn:aws:iam::123456789012:role/ProductionAccessRole
       source_profile = default
   ```

3. 새 프로필을 만든 후 `--profile prodaccess` 파라미터를 지정하는 AWS CLI 명령은 기본 사용자 대신 IAM 역할 `ProductionAccessRole`에 연결된 권한에 따라 실행됩니다.

   ```
   $ aws iam list-users --profile prodaccess
   ```

   이 명령은 `ProductionAccessRole`에 할당된 권한이 현재 AWS 계정에 사용자를 나열하는 것을 가능하게 하는 경우에 작동합니다.

4. 원래 자격 증명에 의해 부여된 권한으로 돌아가려면 명령을 `--profile` 파라미터 없이 실행합니다. AWS CLI에서 다시 기본 프로필의 자격 증명(Step 1에서 구성)이 사용됩니다.

역할 위임하기에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서 단원을 참조하십시오.

에제 시나리오: 인스턴스 프로파일 역할이 다른 계정의 역할로 전환하도록 허용

2개의 AWS 계정을 사용하는 경우, 그리고 Amazon EC2 인스턴스에서 실행 중인 특정 애플리케이션에서 두 계정 모두에 있는 AWS CLI 명령을 실행하도록 허용하고자 하는 경우를 가정합니다. EC2 인스턴스가 `111111111111` 계정에 존재한다고 가정합니다. 해당 인스턴스에는 `abcd` 인스턴스 프로파일 역할이 포함되어 애플리케이션이 동일한 `111111111111` 계정 내에 있는 `my-bucket-1` 버킷에서 읽기 전용 Amazon S3 작업을 수행하도록 허용합니다. 하지만 애플리케이션은 `efgh` 교차 계정 역할을 수임하여 `222222222222` 계정에서 작업을 수행하도록 허용되어야 합니다. 이를 위해 `abcd` EC2 인스턴스 프로파일 역할에 다음과 같은 권한 정책이 있어야 합니다.

계정 111111111111 ***abcd*** 역할 권한 정책

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccountLevelS3Actions",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:HeadBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowListAndReadS3ActionOnMyBucket",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket-1/*",
                "arn:aws:s3:::my-bucket-1"
            ]
        },
        {
            "Sid": "AllowIPToAssumeCrossAccountRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::222222222222:role/efgh"
        }
    ]
}
```

`efgh` 교차 계정 역할이 동일한 `222222222222` 계정 내에 있는 `my-bucket-2` 버킷에서 읽기 전용 Amazon S3 작업 수행을 허용한다고 가정합니다. 이를 위해 `efgh` 교차 계정 역할에 다음과 같은 권한 정책이 있어야 합니다.

계정 222222222222 ***efgh*** 역할 권한 정책

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccountLevelS3Actions",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:HeadBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowListAndReadS3ActionOnMyBucket",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket-2/*",
                "arn:aws:s3:::my-bucket-2"
            ]
        }
    ]
}
```

efgh 역할은 abcd 인스턴스 프로파일 역할이 이를 수임하도록 허용해야 합니다. 이를 위해 efgh 역할에 다음과 같은 신뢰 정책이 있어야 합니다.

계정 222222222222 ***efgh*** 역할 신뢰 정책

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "efghTrustPolicy",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {"AWS": "arn:aws:iam::111111111111:role/abcd"}
        }
    ]
}
```

계정 222222222222에서 AWS CLI 명령을 실행하려면 CLI 구성 파일을 업데이트해야 합니다. AWS CLI 구성 파일에서 efgh 역할을 "프로파일"로 식별하고 abcd EC2 인스턴스 프로파일 역할을 "자격 증명 소스"로 식별합니다. 그런 다음 CLI 명령은 기존의 abcd 역할이 아닌 efgh 역할의 권한을 사용하여 실행됩니다.

> **Note**
>
> 계정에서 보안을 목적으로 AWS CloudTrail을 사용해 계정의 역할 사용을 감사할 수 있습니다. CloudTrail 로그에서 역할의 작업을 식별하기 위해 역할 세션 이름을 사용할 수 있습니다. 이 항목에서 설명하는 것처럼 AWS CLI에서 사용자를 대신해 역할을 수임하면 역할 세션 이름이 AWS-CLI-session-*nnnnnnnn*으로 자동으로 생성됩니다. 여기서 *nnnnnnnn*은 Unix epoch time(1970년 1월 1일 자정 UTC 이후 경과된 초 수)으로 시간을 나타낸 정수입니다. 자세한 내용은 AWS CloudTrail User Guide의 CloudTrail 이벤트 참조를 참조하십시오.

EC2 인스턴스 프로파일 역할의 교차 계정 역할 전환 허용(AWS CLI)

1. 기본 CLI 프로파일을 구성할 필요가 없습니다. 대신 EC2 인스턴스 프로파일 메타데이터에서 자격 증명을 불러올 수 있습니다. .aws/config 파일에서 역할에 대한 새 프로파일을 만듭니다. 다음 예에서는 222222222222 계정의 *efgh* 역할로 전환하는 instancecrossaccount라는 프로필을 만듭니다. 이 프로필이 호출되면 AWS CLI에서는 EC2 인스턴스 프로파일 메타데이터의 자격 증명을 사용하여 해당 역할의 자격 증명을 요청합니다. 이로 인해 EC2 인스턴스 프로파일 역할에는 role_arn에 지정된 역할에 대한 sts:AssumeRole 권한이 있어야 합니다.

   ```
   [profile instancecrossaccount]
   ```

```
role_arn = arn:aws:iam::222222222222:role/efgh
credential_source = Ec2InstanceMetadata
```

2. 새 프로필을 만든 후 `--profile instancecrossaccount` 파라미터를 지정하는 AWS CLI 명령은 `222222222222` 계정의 `efgh` 역할에 연결된 권한에 따라 실행됩니다.

```
$ aws s3 ls my-bucket-2 --profile instancecrossaccount
```

   이 명령은 `efgh` 역할에 할당된 권한이 현재 AWS 계정에 사용자를 나열하는 것을 허용하는 경우에 작동합니다.

3. `111111111111` 계정의 원래 EC2 인스턴스 프로파일 권한을 반환하려면 `--profile` 파라미터 없이 CLI 명령을 실행합니다.

역할 위임하기에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서 단원을 참조하십시오.

IAM 역할로 전환하기(Windows PowerShell용 도구)

역할은 필요한 AWS 리소스에 액세스하는 데 사용할 수 있는 일련의 권한을 지정합니다. 이러한 의미에서 AWS Identity and Access Management(IAM) 사용자와 비슷하다고 할 수 있습니다. 사용자로 로그인할 때는 특정 권한이 부여됩니다. 하지만 역할로 로그인하지는 못하기 때문에 일단 로그인한 후에 역할로 전환할 수 있습니다. 이 경우 초기의 사용자 권한은 잠시 무효화되고 역할에게 할당된 권한이 부여됩니다. 역할은 자신의 계정 또는 그 밖의 다른 AWS 계정에 속한 것일 수 있습니다. 역할과 역할의 이점, 역할 생성 및 구성 방법에 대한 자세한 내용은 IAM역할 (p. 174) 및 IAM 역할 생성 (p. 225) 단원을 참조하십시오.

> **Important**
>
> IAM 사용자의 권한과 전환 대상인 역할의 권한은 누적되지 않습니다. 한 번에 오직 하나의 권한 집합만이 활성화됩니다. 어떤 역할로 전환할 때 사용자 권한은 일시적으로 포기하고 역할에 할당된 권한을 가지고 작업합니다. 역할을 끝내면 사용자 권한이 자동으로 회복됩니다.

이 섹션에서는 Windows PowerShell용 AWS 도구에서 명령줄로 작업할 때 역할을 전환하는 방법에 대해 기술합니다.

개발 환경에서 계정을 하나 갖고 있는데 이따금 Windows PowerShell용 도구을 사용하는 명령줄에서 프로덕션 환경으로 작업해야 할 때가 있다고 가정합시다. 사용할 수 있는 액세스 키 자격 증명 세트가 이미 하나 있습니다. 이 세트는 표준 IAM 사용자에게 할당된 액세스 키 페어일 수도 있고, 연동 사용자로 로그인한 경우에는 초기에 할당된 역할에 대한 액세스 키 페어일 수도 있습니다. 이 자격 증명을 사용해 새 역할의 ARN을 파라미터로 전달하는 `Use-STSRole` cmdlet을 실행할 수 있습니다. 해당 명령은 요청된 역할에 대한 임시 보안 자격 증명을 반환합니다. 그런 다음 생산 중인 리소스에 액세스할 수 있는 해당 역할의 권한으로 후속 PowerShell 명령에서 이 자격 증명을 사용할 수 있습니다. 한 번에 한 가지 권한 세트만 적용될 수 있기 때문에 해당 역할을 사용하는 동안에는 개발 계정의 사용자 권한을 사용할 수 없습니다.

> **Note**
>
> 계정에서 보안을 목적으로 AWS CloudTrail을 사용해 계정의 역할 사용을 감사할 수 있습니다. cmdlet `Use-STSRole`에는 반드시 2~64자의 문자, 숫자 및 `-RoleSessionName` 기호로 된 값과 함께 `=,.@-` 파라미터가 포함되어야 합니다. 역할 세션 이름은 임시 보안 자격 증명으로 수행되는 CloudTrail 로그 작업을 식별합니다. 자세한 내용은 AWS CloudTrail User Guide의 CloudTrail 이벤트 참조를 참조하십시오.

모든 액세스 키와 토큰은 예제일 뿐이며 표시된 대로 사용할 수 없습니다. 라이브 환경의 적절한 값으로 바꾸십시오.

역할을 전환하려면(Windows PowerShell용 도구)

1. PowerShell 명령 프롬프트를 열고 현재 IAM 사용자 또는 연동 역할에서 액세스 키를 사용하도록 기본 프로필을 구성하십시오. 이전에 Windows PowerShell용 도구를 사용했다면 이미 그렇게 한 것이나 다름

없습니다. AWS 계정 루트 사용자가 아닌 IAM 사용자로 로그인한 경우에 한해 역할을 바꿀 수 있다는 것에 유의하십시오.

```
PS C:\> Set-AWSCredentials -AccessKey AKIAIOSFODNN7EXAMPLE -SecretKey wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY -StoreAs MyMainUserProfile
PS C:\> Initialize-AWSDefaults -ProfileName MyMainUserProfile -Region us-east-2
```

자세한 내용은 Windows PowerShell용 AWS 도구 사용 설명서의 AWS 자격 증명 사용을 참조하십시오.

2. 새 역할에 대한 자격 증명을 가져오려면, 다음 명령을 실행해 123456789012 계정의 *RoleName* 역할로 전환합니다. 해당 역할을 만든 계정 관리자에게서 역할 ARN을 받습니다. 그 명령은 세션 이름도 제공할 것을 요구합니다. 세션 이름에 대해서는 어떤 텍스트도 선택 가능합니다. 다음 명령은 자격 증명을 요청한 다음, 반환된 결과 객체로부터 `Credentials` 속성 객체를 캡쳐해 `$Creds` 변수에 저장합니다.

```
PS C:\> $Creds = (Use-STSRole -RoleArn "arn:aws:iam::123456789012:role/RoleName" -
RoleSessionName "MyRoleSessionName").Credentials
```

`$Creds`는 다음 절차에서 필요한 `AccessKeyId`, `SecretAccessKey` 및 `SessionToken` 요소를 포함하는 객체입니다. 다음 샘플 명령은 전형적인 값을 보여줍니다.

```
PS C:\> $Creds.AccessKeyId
AKIAIOSFODNN7EXAMPLE

PS C:\> $Creds.SecretAccessKey
wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

PS C:\> $Creds.SessionToken
AQoDYXdzEGcaEXAMPLE2gsYULo+Im5ZEXAMPLEeYjs1M2FUIgIJx9tQqNMBEXAMPLECvSRyh0FW7jEXAMPLEW
+vE/7s1HRp
XviG7b+qYf4nD00EXAMPLEmj4wxS04L/uZEXAMPLECihzFB5lTYLto9dyBgSDyEXAMPLE9/
g7QRUhZp4bqbEXAMPLENwGPy
Oj59pFA4lNKCIkVgkREXAMPLEjlzxQ7y52gekeVEXAMPLEDiB9ST3UuysgsKdEXAMPLE1TVastU1A0SKFEXAMPLEiywCC/
C
s8EXAMPLEpZgOs+6hz4AP4KEXAMPLERbASP+4eZScEXAMPLEsnf87eNhyDHq6ikBQ==

PS C:\> $Creds.Expiration
Thursday, June 18, 2018 2:28:31 PM
```

3. 후속 명령에 대해 이 자격 증명을 사용하려면 `-Credentials` 파라미터로 자격 증명을 포함시키십시오. 예를 들어 다음 명령은 그 역할에 `iam:ListRoles` 권한이 부여되고, 따라서 `Get-IAMRoles` cmdlet을 실행할 수 있는 경우에 한해 역할에서 얻은 자격 증명을 사용하고 작동됩니다.

```
PS C:\> get-iamroles -Credential $Creds
```

4. 원래 자격 증명으로 돌아가려면 `-Credentials $Creds` 파라미터 사용을 중지하고 PowerShell이 기본 프로필에 저장된 자격 증명으로 복귀할 수 있도록 허용하기만 하면 됩니다.

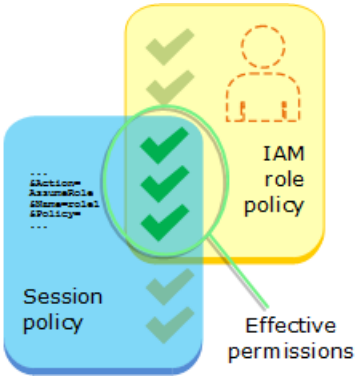
IAM 역할(AWS API)로 전환하기

역할은 AWS 리소스에 액세스하는 데 사용할 수 있는 일련의 권한을 지정합니다. 이러한 면에서 IAM 사용자와 비슷합니다. 보안 주체(개인 또는 애플리케이션)은 역할을 수임하여 필요한 작업을 수행하고 AWS 리소스와 상호작용할 수 있는 임시 권한을 부여받습니다. 역할은 자신의 계정 또는 그 밖의 다른 AWS 계정에 속한 것일 수 있습니다. 역할과 그 이점, 역할 생성 및 구성 방법에 대한 자세한 정보는 IAM역할 (p. 174) 및 IAM 역할 생성 (p. 225) 단원을 참조하십시오. 역할을 수임하는 데 사용할 수 있는 여러 방법을 알아보려면 IAM 역할 사용 (p. 250) 단원을 참조하십시오.

> **Important**
>
> IAM 사용자의 권한과 수임한 역할의 권한은 누적되지 않습니다. 한 번에 오직 하나의 권한 집합만이 활성화됩니다. 어떤 역할을 수임할 때 이전 사용자 또는 역할 권한은 일시적으로 포기하고 해당 역할에 할당된 권한을 가지고 작업합니다. 이 역할을 끝내면 원래 권한이 자동으로 회복됩니다.

이때 역할 위임을 위해 애플리케이션은 AWS STS `AssumeRole` API 작업을 호출하고 사용할 역할의 ARN을 전달합니다. 이 작업은 임시 자격 증명으로 사용하여 새 세션을 생성합니다. 이 세션에는 해당 역할에 대한 자격 증명 기반 정책과 동일한 권한이 지정됩니다.

`AssumeRole` 호출 시 선택적으로 인라인 또는 관리형 세션 정책 (p. 351)을 전달할 수 있습니다. 세션 정책은 역할 또는 연합된 사용자에 대해 임시 자격 증명 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. `Policy` 파라미터를 사용하여 단일 JSON 인라인 세션 정책 문서를 전달할 수 있습니다. `PolicyArns` 파라미터를 사용하여 최대 10개까지 관리형 세션 정책을 지정할 수 있습니다. 결과적으로 얻는 세션의 권한은 엔터티의 자격 증명 기반 정책과 세션 정책의 교집합입니다 세션 정책은 다른 사람에게 역할의 임시 보안 자격 증명을 부여할 필요가 있을 때 유용합니다. 후속 AWS API 호출 시에도 역할의 임시 자격 증명을 사용하여 역할이 속한 계정의 리소스에 액세스할 수 있습니다. 세션 정책을 사용하여 자격 증명 기반 정책에서 허용되는 권한을 부여할 수는 없습니다. 이 역할의 효과적인 권한을 AWS가 어떻게 결정하는지 자세히 알아보려면 정책 평가 로직 (p. 622) 단원을 참조하십시오.



IAM 사용자 또는 역할을 이미 사용 중인 외부 인증 사용자 (p. 183)(SAML (p. 188) 또는 OIDC (p. 183))로 로그인한 경우 `AssumeRole`을 호출할 수 있습니다. 또한 역할을 사용해 두 번째 역할을 수임하는 역할 함께 묶기 (p. 176)를 사용할 수도 있습니다. AWS 계정 루트 사용자로 로그인되어 있을 때는 역할을 수임할 수 없습니다.

기본적으로 역할 세션은 한 시간 동안 지속됩니다. AWS STS `AssumeRole*` API 작업을 사용하여 역할을 수임하는 경우 `DurationSeconds` 파라미터에 대한 값을 지정할 수 있습니다. 이 값의 범위는 900초(15분)에서 해당 역할에 대한 최대 세션 기간 설정까지일 수 있습니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오.

역할 함께 묶기를 사용하는 경우 세션은 최대 1시간으로 제한됩니다. 그런 다음 `DurationSeconds` 파라미터를 사용하여 1시간보다 큰 값을 입력하면 이 작업에 실패합니다.

> **Note**
>
> 계정에서 보안을 목적으로 AWS CloudTrail을 사용해 계정의 역할 사용을 감사할 수 있습니다. `AssumeRole` 호출에는 반드시 2~64자의 문자, 숫자, 그리고 `=,.@-` 기호로 구성된 역할 세션 이름이 포함되어야 합니다. 역할 세션 이름은 임시 보안 자격 증명에 의해 수행되는 작업을 식별하기 위해 CloudTrail 로그에서 사용됩니다. 자세한 내용은 AWS CloudTrail User Guide의 CloudTrail 이벤트 참조를 참조하십시오.

AWS에 대한 Boto3 인터페이스(AWS SDK for Python (Boto) V3)를 사용하여 Python으로 작성된 다음 예제에서는 `AssumeRole`을 호출하는 방법을 보여줍니다. 또한 `AssumeRole`에서 반환한 임시 보안 자격 증명을 사용하여 해당 역할을 소유한 계정의 모든 Amazon S3 버킷을 나열하는 방법도 보여줍니다.

```
import boto3
```

```
# The calls to AWS STS AssumeRole must be signed with the access key ID
# and secret access key of an existing IAM user or by using existing temporary
# credentials such as those from another role. (You cannot call AssumeRole
# with the access key for the root account.) The credentials can be in
# environment variables or in a configuration file and will be discovered
# automatically by the boto3.client() function. For more information, see the
# Python SDK documentation:
# http://boto3.readthedocs.io/en/latest/reference/services/sts.html#client

# create an STS client object that represents a live connection to the
# STS service
sts_client = boto3.client('sts')

# Call the assume_role method of the STSConnection object and pass the role
# ARN and a role session name.
assumed_role_object=sts_client.assume_role(
    RoleArn="arn:aws:iam::account-of-role-to-assume:role/name-of-role",
    RoleSessionName="AssumeRoleSession1"
)

# From the response that contains the assumed role, get the temporary
# credentials that can be used to make subsequent API calls
credentials=assumed_role_object['Credentials']

# Use the temporary credentials that AssumeRole returns to make a
# connection to Amazon S3
s3_resource=boto3.resource(
    's3',
    aws_access_key_id=credentials['AccessKeyId'],
    aws_secret_access_key=credentials['SecretAccessKey'],
    aws_session_token=credentials['SessionToken'],
)

# Use the Amazon S3 resource object that is now configured with the
# credentials to access your S3 buckets.
for bucket in s3_resource.buckets.all():
    print(bucket.name)
```

IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기

EC2 인스턴스에서 실행되는 애플리케이션에는 AWS API 요청에 AWS 자격 증명이 포함되어 있어야 합니다. 개발자들로 하여금 AWS 자격 증명을 EC2 인스턴스 내부에 직접 저장하고 그 인스턴스의 애플리케이션이 그 자격 증명의 사용을 허용하도록 했을 수도 있습니다. 그러면 개발자는 자격 증명을 관리하고 각 인스턴스에 자격 증명을 안전하게 전달해야 하며, 자격 증명을 교체할 때가 되면 각 EC2 인스턴스를 업데이트해야 할 것입니다. 이처럼 여기에는 많은 작업이 요구됩니다.

이렇게 하는 대신 IAM 역할을 사용하여 EC2 인스턴스에서 실행되는 애플리케이션의 임시 자격 증명을 관리할 수 있고 또 그렇게 해야 합니다. 역할을 사용할 때 EC2 인스턴스에 장기 자격 증명(예: 사용자 이름, 암호 또는 액세스 키)을 배포하지 않아도 됩니다. 그 대신 역할은 애플리케이션에서 다른 AWS 리소스에 호출할 때 사용할 수 있는 임시 권한을 제공합니다. EC2 인스턴스를 시작할 때 IAM 역할을 지정해 인스턴스에 연결합니다. 그러면 이 인스턴스에서 실행되는 애플리케이션은 역할 제공 임시 자격 증명을 사용하여 API 요청에 서명할 수 있습니다.

역할을 사용하여 EC2 인스턴스에서 실행되는 애플리케이션에 권한을 부여하기 위해서는 약간의 추가적인 구성이 필요합니다. EC2 인스턴스에서 실행되는 애플리케이션은 가상화된 운영 체제에 의해 AWS에서 추상화됩니다. 이러한 추가적인 분리로 인해 EC2 인스턴스에 AWS 역할 및 관련 권한을 할당하고 이를 그 애플리케이션도 사용 가능하게 만들려면 추가 절차가 필요합니다. 여기서 추가 절차란 인스턴스에 연결된 인스턴스 프로파일을 생성하는 것입니다. 그러면 인스턴스 프로필은 해당 역할을 포함하게 되며 인스턴스에서 실행되는 애플리케이션에 이 역할의 임시 자격 증명을 제공할 수 있습니다. 이 임시 자격 증명은 애플리케이션의

API 호출에 사용되어 리소스에 액세스하고 이 역할이 지정하는 리소스에 대해서만 액세스를 제한할 수 있습니다. 한 번에 하나의 역할만 EC2 인스턴스에 할당할 수 있으며, 인스턴스의 모든 애플리케이션은 동일한 역할과 권한을 공유한다는 것에 유의하십시오.

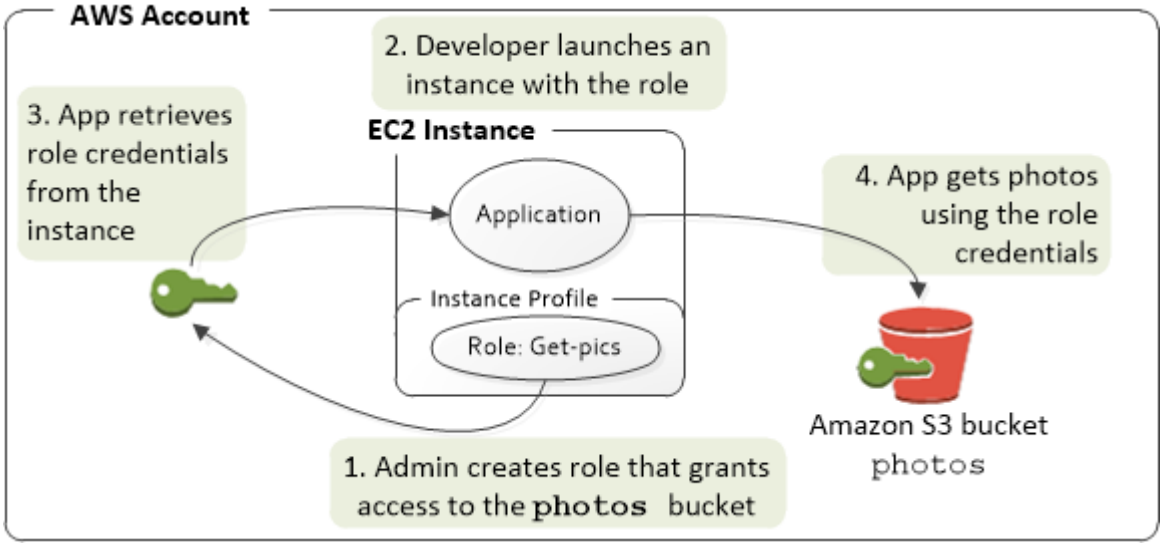
이러한 방식으로 역할을 사용하면 여러 가지 장점이 있습니다. 역할 자격 증명은 임시적이고 자동으로 교체되므로 자격 증명을 관리하지 않아도 될 뿐만 아니라 장기적인 보안 위험을 염려하지 않아도 됩니다. 또한, 여러 인스턴스에 대해 역할을 하나만 사용하는 경우 그 역할을 변경할 수 있는데, 변경 사항은 모든 인스턴스에 자동으로 전파됩니다.

> **Note**
>
> 일반적으로 역할은 EC2 인스턴스를 시작할 때 할당되지만, 이미 실행 중인 EC2 인스턴스에도 연결될 수 있습니다. 실행 중인 인스턴스에 역할을 연결하는 방법을 알아보려면 Amazon EC2의 IAM 역할 단원을 참조하십시오.

주제

EC2 인스턴스의 역할은 어떻게 작동하나요?

다음 그림에서는 개발자가 `photos`라는 S3 버킷에 대한 액세스 권한이 필요한 EC2 인스턴스에서 애플리케이션을 실행하고 있습니다. 관리자가 `Get-pics` 서비스 역할을 생성해 EC2 인스턴스에 연결합니다. 이 역할에는 지정된 S3 버킷에 대한 읽기 전용 액세스 권한을 부여하는 권한 정책이 포함되어 있습니다. 또한 EC2 인스턴스가 해당 역할을 수임하고 임시 자격 증명을 가져오도록 허용하는 신뢰 정책도 포함되어 있습니다. 애플리케이션이 인스턴스에서 실행되면 역할의 임시 자격 증명을 사용하여 photos 버킷에 액세스할 수 있습니다. 관리자는 개발자 권한을 부여하지 않아도 photos 버킷에 액세스할 수 있고 개발자는 자격 증명을 공유하거나 관리할 필요가 전혀 없습니다.



1. 관리자는 IAM을 사용하여 **`Get-pics`** 역할을 만듭니다. 역할의 신뢰 정책에서 관리자는 EC2 인스턴스만 이 역할을 맡을 수 있도록 지정합니다. 역할의 권한 정책에서 관리자는 `photos` 버킷에 읽기 전용 권한을 지정합니다.
2. 개발자는 EC2 인스턴스를 시작하고 이 인스턴스에 `Get-pics` 역할을 할당합니다.

Note

IAM 콘솔을 사용하는 경우, 인스턴스 프로파일은 사용자를 위해 관리되고 대개 사용자가 파악하기 쉽습니다. 그러나 AWS CLI 또는 API를 사용하여 역할 및 EC2 인스턴스를 만들고 관리하는 경우 사용자는 인스턴스 프로파일을 만들고 별도 절차에 따라 여기에 역할을 할당해야 합니다. 그런 다음 인스턴스를 시작할 때 역할 이름이 아닌 인스턴스 프로파일 이름을 지정해야 합니다.

3. 애플리케이션이 실행되면 인스턴스 메타데이터에서 보안 자격 증명 검색에 설명된 대로 Amazon EC2 인스턴스 메타데이터에서 임시 보안 자격 증명을 가져옵니다. 이러한 자격 증명은 제한된 시간 동안에만 유효한 임시 보안 자격 증명 (p. 302)으로 역할을 나타냅니다.

   개발자는 일부 AWS SDK를 통해 임시 보안 자격 증명을 명료하게 관리하는 공급자를 사용할 수 있습니다. (개별 AWS SDK에 대한 설명서에 자격 증명을 관리하기 위해 SDK에서 지원하는 기능이 설명되어 있습니다.)

   또는 애플리케이션이 EC2 인스턴스의 인스턴스 메타데이터에서 임시 자격 증명을 얻을 수 있습니다. 자격 증명과 관련 값은 메타데이터의 `iam/security-credentials/role-name` 범주(이 경우 `iam/security-credentials/Get-pics`)에서 구할 수 있습니다. 애플리케이션이 인스턴스 메타데이터에서 자격 증명을 가져오면 자격 증명을 캐시할 수 있습니다.

4. 애플리케이션은 가져온 임시 자격 증명을 사용하여 photo 버킷에 액세스합니다. **`Get-pics`** 역할에 연결된 정책으로 인해 이 애플리케이션에는 읽기 전용 권한만 있습니다.

   인스턴스에서 제공되는 임시 보안 자격 증명은 만료되기 전에 자동으로 교체되므로 항상 유효한 설정을 사용할 수 있습니다. 애플리케이션은 현재 자격 증명이 만료되기 전에 인스턴스 메타데이터에서 새 자격 증명을 가져와야 합니다. AWS SDK에서 자격 증명을 관리하는 경우 애플리케이션은 자격 증명을 갱신하기 위해 로직을 추가로 포함하지 않아도 됩니다. 그러나 애플리케이션이 인스턴스 메타데이터에서 임시 보안 자격 증명을 가져와 캐시한 경우, 현재 자격 증명이 만료되기 전에 한 시간 또는 최소 15분마다 갱신한 자격 증명을 가져와야 합니다. 만료 시간은 `iam/security-credentials/role-name` 카테고리에 반환되는 정보에 포함되어 있습니다.

Amazon EC2로 역할을 사용하는 데 필요한 권한

역할을 사용하여 인스턴스를 시작하려면 개발자에게 EC2 인스턴스를 시작할 수 있는 권한과 IAM 역할을 전달할 수 있는 권한이 있어야 합니다.

다음과 같은 샘플 정책은 사용자가 AWS Management 콘솔을 사용하여 역할로 인스턴스를 시작할 수 있도록 허용합니다. 이 정책에는 와일드카드(*)가 포함되어 있어 사용자가 어떤 역할이든 전달하고 어떤 Amazon EC2 작업도 수행할 수 있도록 허용합니다. `ListInstanceProfiles` 작업을 수행하면 사용자는 AWS 계정에서 제공되는 모든 역할을 볼 수 있습니다.

Example 사용자에게 Amazon EC2 콘솔을 사용하여 임의의 역할로 인스턴스를 시작할 권한을 부여하는 정책

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:PassRole",
      "iam:ListInstanceProfiles",
      "ec2:*"
    ],
    "Resource": "*"
  }]
}
```

(PassRole을 사용하여) EC2 인스턴스로 전달할 수 있는 역할 제한

`PassRole` 권한을 사용하여 사용자가 EC2 인스턴스를 시작할 때 이 인스턴스에 전달할 수 있는 역할을 제한할 수 있습니다. 이를 통해 사용자가 자신이 받은 권한 보다 더 많은 권한이 있는 애플리케이션을 실행하지 않도록, 즉 높은 권한을 가져오지 않도록 할 수 있습니다. 예를 들어 사용자 Alice는 EC2 인스턴스를 시작하고 Amazon S3 버킷을 사용할 권한만 갖고 있지만, 그녀가 인스턴스에 전달하는 역할에는 IAM 및 Amazon DynamoDB를 사용할 권한이 있다고 가정해 봅시다. 이 경우 Alice는 인스턴스를 시작하고 여기에 로그인하여 임시 보안 자격 증명을 가져온 다음 그녀에게 권한이 없는 IAM 또는 DynamoDB 작업을 수행할 수도 있습니다.

사용자가 EC2 인스턴스에 전달할 수 있는 역할 중 어떤 것을 제한하려면 `PassRole` 작업을 허용하는 정책을 생성합니다. 그런 다음 그 정책을 EC2 인스턴스를 시작할 사용자(또는 사용자가 소속된 IAM 그룹)에게 연결합니다. 이 정책의 `Resource` 요소에서 사용자가 EC2 인스턴스에 전달할 수 있는 역할을 나열합니다. 사용자가 인스턴스를 시작하고 역할을 인스턴스에 연결하면 Amazon EC2에서 사용자가 해당 역할을 전달할 수 있는지 확인합니다. 물론 사용자가 전달할 수 있는 역할에 사용자가 보유하고 있을 것으로 추정되는 권한보다 더 많은 권한이 포함되어 있지 않은지도 확인해야 합니다.

> **Note**
>
> `PassRole`은 `RunInstances` 또는 `ListInstanceProfiles`와 동일한 방식의 API 작업이 아닙니다. 역할 ARN이 API에 대한 파라미터로 전달될 때마다 AWS에서 검사하는 권한입니다(또는 사용자 대신 콘솔이 이 기능을 수행). 관리자가 어느 사용자가 어느 역할을 전달할 수 있는지를 제어할 수 있습니다. 이 경우 사용자가 Amazon EC2 인스턴스에 특정 역할을 연결할 수 있습니다.

Example 사용자에게 특정 역할로 EC2 인스턴스를 시작할 권한을 부여하는 정책

다음과 같은 샘플 정책은 사용자가 Amazon EC2 API를 사용하여 역할로 인스턴스를 시작할 수 있도록 허용합니다. `Resource` 요소는 역할의 Amazon 리소스 이름(ARN)을 지정합니다. ARN을 지정함으로써 정책은 사용자에게 `Get-pics` 역할만을 전달할 권한을 부여합니다. 사용자가 인스턴스를 시작할 때 다른 역할을 지정하려는 경우 작업이 실패합니다. 사용자는 역할을 전달하는지 여부에 관계없이 모든 인스턴스를 실행할 권한이 있습니다.

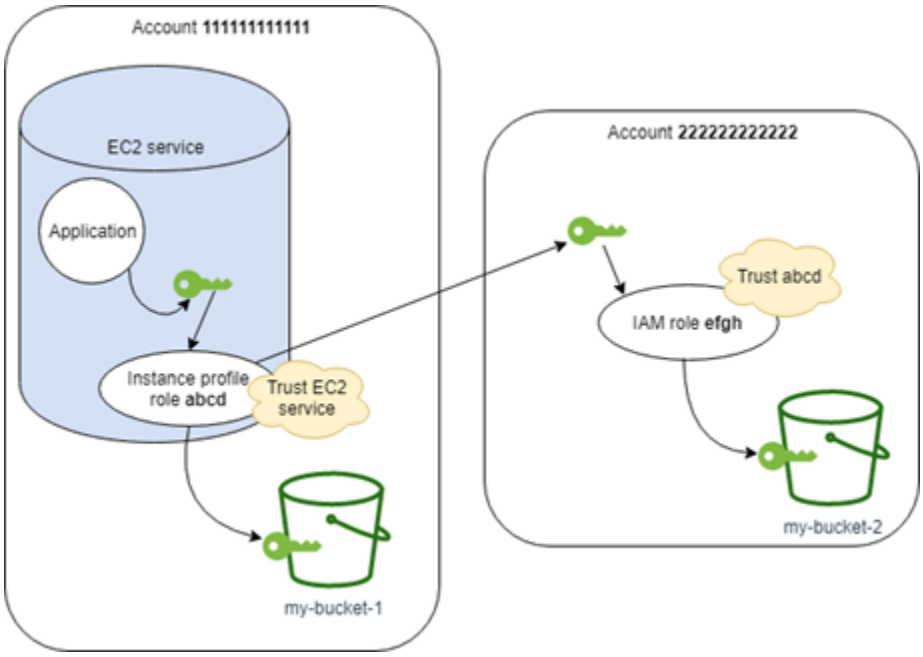
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/Get-pics"
    }
  ]
}
```

인스턴스 프로파일 역할이 다른 계정의 역할로 전환하도록 허용

Amazon EC2 인스턴스에서 실행 중인 애플리케이션에서 다른 계정에 있는 명령을 실행하도록 허용할 수 있습니다. 이를 위해 첫 번째 계정에 있는 EC2 인스턴스 역할이 두 번째 계정의 역할로 전환하도록 허용해야 합니다.

2개의 AWS 계정을 사용하는 경우, 그리고 Amazon EC2 인스턴스에서 실행 중인 특정 애플리케이션에서 두 계정 모두에 있는 AWS CLI 명령을 실행하도록 허용하고자 하는 경우를 가정합니다. EC2 인스턴스가 `111111111111` 계정에 존재한다고 가정합니다. 해당 인스턴스에는 `abcd` 인스턴스 프로파일 역할이 포함되어 애플리케이션이 동일한 `111111111111` 계정 내에 있는 `my-bucket-1` 버킷에서 읽기 전

용 Amazon S3 작업을 수행하도록 허용합니다. 하지만 애플리케이션은 `efgh` 교차 계정 역할을 수임하여 `222222222222` 계정의 `my-bucket-2` Amazon S3 버킷에 액세스하도록 허용되어야 합니다.



애플리케이션이 `my-bucket-1` Amazon S3 버킷에 액세스하도록 허용하려면 `abcd` EC2 인스턴스 프로파일 역할에 다음과 같은 권한 정책이 있어야 합니다.

계정 111111111111 ***abcd*** 역할 권한 정책

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccountLevelS3Actions",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:HeadBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowListAndReadS3ActionOnMyBucket",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket-1/*",
                "arn:aws:s3:::my-bucket-1"
            ]
        },
        {
            "Sid": "AllowIPToAssumeCrossAccountRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::222222222222:role/efgh"
        }
    ]
```

```
}
```

abcd 역할은 Amazon EC2 서비스가 역할을 수임하도록 신뢰해야 합니다. 이를 위해 abcd 역할에 다음과 같은 신뢰 정책이 있어야 합니다.

계정 111111111111 ***abcd*** 역할 신뢰 정책

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "abcdTrustPolicy",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {"Service": "ec2.amazonaws.com"}
        }
    ]
}
```

efgh 교차 계정 역할이 동일한 222222222222 계정 내에 있는 my-bucket-2 버킷에서 읽기 전용 Amazon S3 작업 수행을 허용한다고 가정합니다. 이를 위해 efgh 교차 계정 역할에 다음과 같은 권한 정책이 있어야 합니다.

계정 222222222222 ***efgh*** 역할 권한 정책

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccountLevelS3Actions",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:HeadBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowListAndReadS3ActionOnMyBucket",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket-2/*",
                "arn:aws:s3:::my-bucket-2"
            ]
        }
    ]
}
```

efgh 역할은 abcd 인스턴스 프로파일 역할이 이를 수임하도록 신뢰해야 합니다. 이를 위해 efgh 역할에 다음과 같은 신뢰 정책이 있어야 합니다.

계정 222222222222 ***efgh*** 역할 신뢰 정책

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

```
            "Sid": "efghTrustPolicy",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {"AWS": "arn:aws:iam::111111111111:role/abcd"}
        }
    ]
}
```

어떻게 시작할 수 있습니까?

역할이 EC2 인스턴스를 사용하는 방식을 이해하려면 IAM 콘솔을 사용하여 역할을 만들고 해당 역할을 사용하는 EC2 인스턴스를 시작한 다음, 실행 중인 인스턴스를 검사해야 합니다. 해당 역할의 임시 자격 증명이 인스턴스에서 사용되는 방식을 보기 위해 인스턴스 메타데이터를 검토할 수 있습니다. 또한, 인스턴스에서 실행되는 애플리케이션이 어떻게 역할을 사용하는지도 알 수 있습니다. 다음 리소스에서 자세히 알아보십시오.

-
- SDK 설명입니다. AWS SDK 설명서에는 역할에 대한 임시 자격 증명을 사용하여 Amazon S3 버킷을 읽는 EC2 인스턴스에서 실행되는 애플리케이션에 대한 자세한 안내가 있습니다. 다음과 같은 각 설명에서는 여러 프로그래밍 언어를 사용하여 비슷한 절차를 제시합니다.
  - AWS SDK for Java Developer Guide의 Java용 SDK를 사용하여 Amazon EC2용 IAM 역할 구성
  - .NET용 AWS SDK Developer Guide의 .NET용 SDK를 사용하여 EC2 인스턴스 시작
  - Ruby용 AWS SDK Developer Guide의 Ruby용 SDK를 사용하여 Amazon EC2 인스턴스 생성

관련 정보

역할 생성 및 EC2 인스턴스의 역할에 대한 자세한 내용은 다음 정보를 참조하십시오.

- Amazon EC2 인스턴스로 IAM 역할을 사용하는 방법에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서 단원을 참조하십시오.
- 역할을 만들려면 IAM 역할 생성 (p. 225) 단원을 참조하십시오.
- 임시 보안 자격 증명의 사용에 관한 자세한 내용은 임시 보안 자격 증명 (p. 302)을 확인하십시오.
- IAM API 또는 CLI를 사용하는 경우, IAM 인스턴스 프로필을 생성 및 관리해야 합니다. 인스턴스 프로파일에 대한 자세한 내용은 인스턴스 프로파일 사용 (p. 271) 단원을 참조하십시오.
- 인스턴스 메타데이터의 역할에 대한 임시 보안 자격 증명에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 인스턴스 메타데이터에서 보안 자격 증명 검색을 참조하십시오.

인스턴스 프로파일 사용

인스턴스 프로파일은 IAM 역할을 위한 컨테이너로서 인스턴스 시작 시 EC2 인스턴스에 역할 정보를 전달하는 데 사용됩니다.

인스턴스 프로파일 관리(콘솔)

AWS Management 콘솔을 사용하여 Amazon EC2 역할을 생성하는 경우, 콘솔이 자동으로 인스턴스 프로파일을 생성하여 해당 역할과 동일한 이름을 부여합니다. 그런 다음 Amazon EC2 콘솔을 사용해 IAM 역할과 연동하여 인스턴스를 실행할 때는 인스턴스와 연동할 역할을 선택할 수 있습니다. 콘솔에 표시되는 목록이 실제로 인스턴스 프로파일 이름의 목록입니다. 콘솔은 Amazon EC2와 연결되지 않은 역할에 대한 인스턴스 프로파일은 생성하지 않습니다.

인스턴스 프로파일(AWS CLI 또는 AWS API) 관리

AWS CLI 또는 AWS API에서 역할을 관리할 경우 별도의 작업으로 역할 및 인스턴스 프로파일을 생성합니다. 역할 및 인스턴스 프로파일의 이름이 서로 다를 수 있으므로 인스턴스 프로파일 이름은 물론이고 프로파

일이 속하는 역할 이름까지 알고 있어야 합니다. 그러면 EC2 인스턴스를 시작할 때 올바른 인스턴스 프로파일을 선택할 수 있습니다.

> Note
>
> 하나의 인스턴스 프로파일은 하나의 IAM 역할만 포함할 수 있습니다. 하지만 한 역할이 여러 인스턴스 프로파일에 포함될 수 있습니다. 이 인스턴스 프로파일당 역할 1개 제한은 늘릴 수 없습니다. 기존 역할을 제거하고 나서 인스턴스 프로파일에 다른 역할을 추가할 수 있습니다. 최종 일관성으로 인해 모든 AWS에 변경 사항이 적용될 때까지 기다려야 합니다. 변경을 적용하려면 인스턴스 프로파일 연결을 해제하고 나서 인스턴스 프로파일을 연결하거나, 인스턴스를 중지했다가 다시 시작합니다.

인스턴스 프로파일 관리(AWS CLI)

AWS 계정의 인스턴스 프로파일 작업을 할 때는 다음 AWS CLI 명령을 사용할 수 있습니다.

- 인스턴스 프로파일을 생성합니다: `aws iam create-instance-profile`
- 인스턴스 프로파일에 역할 추가: `aws iam add-role-to-instance-profile`
- 인스턴스 프로파일 표시: `aws iam list-instance-profiles`, `aws iam list-instance-profiles-for-role`
- 인스턴스 프로파일 정보 가져오기: `aws iam get-instance-profile`
- 인스턴스 프로파일에서 역할 제거: `aws iam remove-role-from-instance-profile`
- 인스턴스 프로파일 삭제: `aws iam delete-instance-profile`

다음 명령을 사용하여 이미 실행 중인 EC2 인스턴스에 역할을 연결할 수도 있습니다. 자세한 내용은 Amazon EC2의 IAM 역할을 참조하십시오.

- 역할이 있는 인스턴스 프로파일을 중지되었거나 실행 중인 EC2 인스턴스에 연결: `aws ec2 associate-iam-instance-profile`
- EC2 인스턴스에 연결된 인스턴스 프로파일에 대한 정보 가져오기: `aws ec2 describe-iam-instance-profile-associations`
- 역할이 있는 인스턴스 프로파일을 중지되었거나 실행 중인 EC2 인스턴스에서 분리: `aws ec2 disassociate-iam-instance-profile`

인스턴스 프로파일 관리(AWS API)

AWS 계정의 인스턴스 프로파일 작업을 할 때는 다음 AWS API 연산을 호출할 수 있습니다.

- 인스턴스 프로파일을 생성합니다: `CreateInstanceProfile`
- 인스턴스 프로파일에 역할 추가: `AddRoleToInstanceProfile`
- 인스턴스 프로파일 표시: `ListInstanceProfiles`, `ListInstanceProfilesForRole`
- 인스턴스 프로파일 정보 가져오기: `GetInstanceProfile`
- 인스턴스 프로파일에서 역할 제거: `RemoveRoleFromInstanceProfile`
- 인스턴스 프로파일 삭제: `DeleteInstanceProfile`

다음 연산을 호출하여 이미 실행 중인 EC2 인스턴스에 역할을 연결할 수도 있습니다. 자세한 내용은 Amazon EC2의 IAM 역할을 참조하십시오.

- 역할이 있는 인스턴스 프로파일을 중지되었거나 실행 중인 EC2 인스턴스에 연결: `AssociateIamInstanceProfile`
- EC2 인스턴스에 연결된 인스턴스 프로파일에 대한 정보 가져오기: `DescribeIamInstanceProfileAssociations`

- 역할이 있는 인스턴스 프로파일을 중지되었거나 실행 중인 EC2 인스턴스에서 분리: `DisassociateIamInstanceProfile`

IAM 역할의 임시 보안 자격 증명 취소

> Warning
>
> 이 페이지의 단계대로 수행하면, 역할을 수임하여 만들어진 현재 세션의 모든 사용자는 모든 AWS 작업 및 리소스에 액세스할 수 없게 됩니다. 이로 인해 사용자가 저장하지 않은 작업이 사라질 수 있습니다.

세션 지속 시간을 길게 하여(예: 12시간) 사용자가 AWS Management 콘솔에 액세스할 수 있도록 하면 사용자의 임시 자격 증명이 금방 만료되지 않습니다. 사용자가 허가 받지 않은 타사에게 실수로 자격 증명을 노출한 경우, 해당 타사는 세션의 지속 기간 동안 액세스 권한을 가지게 됩니다. 그러나 필요하다면 특정 시점 이전에 발행된 역할의 자격 증명에 대한 모든 권한을 즉시 취소할 수 있습니다. 그러면 지정한 시점 이전에 발행된 해당 역할의 임시 자격 증명은 모두 무효가 됩니다. 이에 따라 모든 사용자는 다시 인증을 받고 새 자격 증명을 요청해야 합니다.

> Note
>
> 서비스 연결 역할 (p. 175)에 대한 세션은 취소할 수 없습니다.

이 주제의 절차에 따라 역할의 권한을 취소하면 AWS는 모든 작업에 대한 모든 권한을 거부하는 새 인라인 정책을 만들어 해당 역할에 연결합니다. 여기에는 권한을 취소한 시점 이전에 역할을 위임한 사용자에게만 제한을 가하는 조건이 포함됩니다. 권한을 취소한 이후에 역할을 위임한 사용자에게는 거부 정책이 적용되지 않습니다.

> Important
>
> 이 거부 정책은 콘솔 세션의 지속 기간이 긴 사용자만이 아니라 지정된 역할의 모든 사용자에게 적용됩니다.

역할의 세션 권한을 취소하기 위한 최소 권한

역할의 세션 권한을 취소하려면 해당 역할에 대한 `PutRolePolicy` 권한이 있어야 합니다. 이렇게 하면 해당 역할에 `AWSRevokeOlderSessions` 인라인 정책을 연결할 수 있게 됩니다.

세션 권한 취소

역할에서 세션 권한을 취소할 수 있습니다.

역할 자격 증명의 현재 사용자에 대해 모든 권한을 즉시 거부하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM Dashboard(IAM 대시보드)의 탐색 창에서 역할을 선택한 다음, 권한을 취소할 역할의 이름(확인란 아님)을 선택합니다.
3. 선택한 역할의 요약 페이지에서 Revoke sessions(세션 취소) 탭을 선택합니다.
4. Revoke sessions(세션 취소) 탭에서 Revoke active sessions(활성 세션 취소)를 선택합니다.
5. AWS에 작업 확인 메시지가 나타납니다. 대화 상자에서 Revoke active sessions(활성 세션 취소)를 선택합니다.

   IAM은 `AWSRevokeOlderSessions`라는 정책을 즉시 해당 역할에 연결합니다. 이 정책은 Revoke active sessions(활성 세션 취소)를 선택한 순간 이전에 해당 역할을 수임한 사용자의 모든 액세스 권한을 거부합니다. Revoke active sessions(활성 세션 취소)를 선택한 이후에 역할을 수임한 사용자에게는 적용되지 않습니다.

사용자나 리소스에 새 정책을 적용할 때 정책 업데이트가 효력이 생기는 데 몇 분이 걸릴 수 있습니다.

Note

정책 삭제에 대해서는 걱정하지 마십시오. 세션을 취소한 이후에 역할을 수임한 사용자에게는 이 정책이 적용되지 않습니다. 나중에 Revoke Sessions(세션 취소)를 다시 선택하는 경우, 정책의 날짜/시간 스탬프가 새로 고쳐지면서 새로 지정된 시간 이전에 역할을 수임한 모든 사용자의 모든 권한을 거부하게 됩니다.

이러한 식으로 세션이 취소된 유효한 사용자는 작업을 계속하려면 새 세션을 위한 임시 자격 증명을 가져와야 합니다. AWS CLI는 자격 증명이 만료될 때까지 이를 캐시합니다. CLI가 더 이상 유효하지 않은 캐시된 자격 증명을 강제로 삭제하고 새로 고치게 하려면 다음 명령 중 하나를 실행합니다.

Linux, macOS 또는 Unix

```
$ rm -r ~/.aws/cli/cache
```

Windows

```
C:\> del /s /q %UserProfile%\.aws\cli\cache
```

자세한 내용은 임시 보안 자격 증명에 대한 권한 비활성화 (p. 322) 단원을 참조하십시오.

IAM 역할 관리

때때로 생성한 역할을 수정 또는 삭제해야 할 때가 있습니다. 역할을 변경하려면 다음 중 하나를 수행할 수 있습니다.

- 역할과 연결된 정책을 수정합니다.
- 역할에 액세스할 수 있는 사람을 변경합니다.
- 사용자에게 역할을 부여하는 권한을 편집합니다.
- AWS CLI 또는 API를 사용하여 수임한 역할에 대한 최대 세션 기간 설정을 변경합니다.

또한 더 이상 필요 없는 역할을 삭제할 수 있습니다. AWS Management 콘솔, AWS CLI 및 API에서 역할을 관리할 수 있습니다.

주제

역할 변경

AWS Management 콘솔, AWS CLI 또는 IAM API를 사용하여 역할을 변경할 수 있습니다.

주제

역할 액세스 보기

역할에 대한 권한을 변경하기 전에 최근 서비스 수준 활동을 검토해야 합니다. 이 기능은 사용 중인 보안 주체(사람 또는 애플리케이션)의 액세스 권한을 제거하지 않으려는 경우 중요합니다. 서비스에서 마지막으로 액세스한 데이터 보기에 대한 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

역할 수정(콘솔)

AWS Management 콘솔을 사용하여 역할을 변경할 수 있습니다. 역할의 태그 세트를 변경하려면 IAM 엔터티에 대한 태그 관리(콘솔) (p. 293) 단원을 참조하십시오.

주제

- 역할 신뢰 정책 수정(콘솔) (p. 275)
- 역할 권한 정책 수정(콘솔) (p. 276)
- 역할 설명 수정(콘솔) (p. 277)
- 역할 최대 세션 기간 수정(콘솔) (p. 277)
- 역할 권한 경계 수정(콘솔) (p. 278)

역할 신뢰 정책 수정(콘솔)

역할을 맡을 수 있는 주체를 바꾸려면 역할의 신뢰 정책을 변경해야 합니다. 서비스 연결 역할 (p. 175)에 대한 신뢰 정책을 수정할 수 없습니다.

> **Note**
>
> 사용자가 역할 신뢰 정책에 보안 주체로 나열되지만 역할을 수임할 수 없는 경우 사용자의 권한 경계 (p. 363)를 확인하십시오. 사용자에 대한 권한 경계가 설정된 경우 권한 경계에서 `sts:AssumeRole` 작업이 허용되어야 합니다.

역할 신뢰 정책을 수정하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다.
3. 계정의 역할 목록에서 변경할 역할의 이름을 선택합니다.
4. 신뢰 관계 탭을 선택한 후 Edit trust relationship(신뢰 관계 편집)을 선택합니다.
5. 필요에 따라 신뢰 정책을 편집합니다. 역할을 위임할 수 있는 보안 주체를 추가하려면 `Principal` 요소에 해당 보안 주체를 지정하십시오. 예를 들어 다음 정책 조각은 `Principal` 요소에서 AWS 계정 2개를 참조하는 방법을 나타냅니다.

```
"Principal": {
  "AWS": [
    "arn:aws:iam::111122223333:root",
    "arn:aws:iam::444455556666:root"
  ]
},
```

다른 계정에서 보안 주체를 지정할 경우 역할의 신뢰 정책에 계정을 추가하는 것은 신뢰 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 기본적으로 신뢰 계정의 어떠한 사용자도 역할을 위임할 수 없습니다. 새로이 신뢰받는 계정에 대한 관리자는 사용자가 역할을 수임할 수 있는 권한을 허용해야 합니다. 이를 위해 관리자는 사용자와 연결된 정책을 생성 또는 편집하여 `sts:AssumeRole` 작업에 대한 사용자 액세스를 허용합니다. 자세한 정보는 다음 절차 또는 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

다음 정책 조각은 `Principal` 요소에서 두 가지 AWS 서비스를 참조하는 방법을 나타냅니다.

```
"Principal": {
  "Service": [
    "opsworks.amazonaws.com",
    "ec2.amazonaws.com"
  ]
},
```

6. 신뢰 정책 편집을 마쳤으면 Update Trust Policy(신뢰 정책 업데이트)를 선택하여 변경 사항을 저장합니다.

   정책 구조 및 구문에 대한 자세한 정보는 정책 및 권한 (p. 349) 단원과 IAM JSON 정책 요소 참조 (p. 586) 단원을 참조하십시오.

신뢰할 수 있는 외부 계정의 사용자가 역할을 사용할 수 있도록 허용하려면(콘솔 사용)

자세한 정보와 이 절차에 대한 세부 정보는 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

1. 신뢰할 수 있는 외부 AWS 계정에 로그인합니다.
2. 사용자 또는 그룹 중 권한을 어디에 추가할지 결정합니다. 결정에 따라 IAM 콘솔의 탐색 창에서 사용자 또는 그룹을 선택합니다.
3. 액세스 권한을 부여하려는 사용자나 그룹의 이름을 선택한 후 권한 탭을 선택합니다.
4. 다음 중 하나를 수행하십시오.
   - 고객 관리형 정책을 편집하려면 정책 이름을 선택하고 정책 편집을 선택한 다음 JSON 탭을 선택합니다. AWS 관리형 정책은 편집할 수 없습니다. AWS 관리형 정책은 AWS 아이콘()으로 나타납니다. AWS 관리형 정책과 고객 관리형 정책의 차이점에 대한 자세한 정보는 관리형 정책과 인라인 정책 (p. 357) 단원을 참조하십시오.
   - 인라인 정책을 편집하려면 정책 이름 옆에 있는 화살표를 선택하고 정책 편집을 선택합니다.
5. 정책 편집기에서 새로운 `Statement` 요소를 추가하여 다음과 같이 지정합니다.

```
{
  "Effect": "Allow",
  "Action": "sts:AssumeRole",
  "Resource": "arn:aws:iam::ACCOUNT-ID:role/ROLE-NAME"
}
```

   설명문의 ARN을 사용자가 수임할 수 있는 역할의 ARN으로 바꿉니다.
6. 화면의 메시지에 따라 정책 편집을 마칩니다.

역할 권한 정책 수정(콘솔)

역할이 허용하는 권한을 변경하려면, 역할의 권한 정책을 수정합니다. IAM의 서비스 연결 역할 (p. 175)에 대한 권한 정책을 수정할 수 없습니다. 역할에 따른 서비스 내 권한 정책을 수정할 수 있는 가능성이 있습니다. 서비스에서 이 기능을 지원하는지 여부를 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [Yes] 링크를 선택합니다.

역할이 허용하는 권한을 변경하려면(콘솔 사용)

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.

2. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다.
3. 수정하려는 역할의 이름을 선택한 후 권한 탭을 선택합니다.
4. 다음 중 하나를 수행하십시오.

   - 기존의 고객 관리형 정책을 편집하려면 정책 이름을 선택한 후 정책 편집을 선택합니다.

     Note

     AWS 관리형 정책은 편집할 수 없습니다. AWS 관리형 정책은 AWS 아이콘()으로 나타납니다. AWS 관리형 정책과 고객 관리형 정책의 차이점에 대한 자세한 정보는 관리형 정책과 인라인 정책 (p. 357) 단원을 참조하십시오.
   - 기존의 관리형 정책을 역할에 연결하려면 Add permissions(권한 추가)를 선택합니다.
   - 기존의 인라인 정책을 편집하려면 정책 이름 옆에 있는 화살표를 선택하고 정책 편집을 선택합니다.
   - 새로운 인라인 정책을 포함시키려면 Add inline policy(인라인 정책 추가)를 선택합니다.

역할 설명 수정(콘솔)

역할의 설명을 변경하려면 설명 텍스트를 수정합니다.

역할의 설명을 변경하려면(콘솔 사용)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다.
3. 변경할 역할 이름을 선택합니다.
4. Role description(역할 설명) 옆의 맨 오른쪽에서 편집을 선택합니다.
5. 상자에 새 설명을 입력하고 [Save]를 선택합니다.

역할 최대 세션 기간 수정(콘솔)

AWS CLI 또는 API를 사용하여 수임한 역할에 대한 최대 세션 기간 설정을 지정하려면 최대 세션 기간 설정의 값을 수정합니다. 이 설정에는 1~12시간의 값을 지정할 수 있습니다. 값을 지정하지 않으면 기본 최댓값인 1시간이 적용됩니다. 이 설정은 AWS 서비스에서 수임하는 세션을 제한하지 않습니다.

Note

AWS CLI 또는 API에서 역할을 수임한 사람은 누구나 `duration-seconds` CLI 파라미터 또는 `DurationSeconds` API 파라미터를 사용해 더 긴 세션을 요청할 수 있습니다. `MaxSessionDuration` 설정은 `DurationSeconds` 파라미터를 사용해 요청할 수 있는 역할 세션에 대한 최대 기간을 결정합니다. 사용자가 `DurationSeconds` 파라미터의 값을 지정하지 않으면 보안 자격 증명이 한 시간 동안 유효하게 됩니다.

AWS CLI 또는 API를 사용하여 수임한 역할에 대한 최대 세션 기간 설정을 변경하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 [Roles]를 선택합니다.
3. 변경할 역할 이름을 선택합니다.
4. Maximum CLI/API session duration(최대 CLI/API 세션 기간) 옆에서 값을 선택합니다. 또는 Custom duration(사용자 지정 기간)을 선택하고 값(초)을 입력합니다.
5. Save를 선택합니다.

   다음에 다른 사람이 이 역할을 수임할 때까지 변경 사항은 적용되지 않습니다. 이 역할에 대한 기존 세션을 취소하는 방법을 알아보려면 IAM 역할의 임시 보안 자격 증명 취소 (p. 273) 단원을 참조하십시오.

역할 권한 경계 수정(콘솔)

역할이 허용하는 최대 권한을 변경하려면, 역할의 권한 경계 (p. 363)를 수정합니다.

역할에 대한 권한 경계 설정에 사용된 정책을 변경하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택합니다.
3. 권한 경계 (p. 363)를 변경하려는 역할의 이름을 선택합니다.
4. Permissions 탭을 선택합니다. 필요하다면 Permissions boundary(권한 경계) 섹션을 열고 Change boundary(경계 변경)을 선택합니다.
5. 정책을 선택하여 원하는 권한 경계를 사용하십시오.
6. Change boundary(경계 변경)을 선택합니다.

   다음에 다른 사람이 이 역할을 수임할 때까지 변경 사항은 적용되지 않습니다.

역할 변경(AWS CLI)

AWS Command Line Interface를 사용하여 역할을 변경할 수 있습니다. 역할의 태그 세트를 변경하려면 IAM 엔터티에 대한 태그 관리(콘솔) (p. 293) 단원을 참조하십시오.

주제

- 역할 신뢰 정책 수정(AWS CLI) (p. 278)
- 역할 권한 정책 수정(AWS CLI) (p. 280)
- 역할 설명 수정(AWS CLI) (p. 280)
- 역할 최대 세션 기간 수정(AWS CLI) (p. 280)
- 역할 권한 경계 수정(AWS CLI) (p. 281)

역할 신뢰 정책 수정(AWS CLI)

역할을 맡을 수 있는 주체를 바꾸려면 역할의 신뢰 정책을 변경해야 합니다. 서비스 연결 역할 (p. 175)에 대한 신뢰 정책을 수정할 수 없습니다.

> **Note**
>
> 사용자가 역할 신뢰 정책에 보안 주체로 나열되지만 역할을 수임할 수 없는 경우 사용자의 권한 경계 (p. 363)를 확인하십시오. 사용자에 대한 권한 경계가 설정된 경우 권한 경계에서 `sts:AssumeRole` 작업이 허용되어야 합니다.

역할 신뢰 정책을 수정하려면(AWS CLI)

1. (선택 사항) 수정할 역할의 이름을 모르는 경우 다음 명령을 실행하여 계정의 역할을 나열합니다.
   - aws iam list-roles
2. (옵션) 현재 역할의 신뢰 정책을 확인하려면 다음 명령을 실행합니다.
   - aws iam get-role
3. 역할에 액세스할 수 있는 신뢰할 수 있는 보안 주체를 변경하려면 업데이트된 신뢰 정책을 추가하여 텍스트 파일을 생성합니다. 정책 구조를 작성할 때는 어떤 텍스트 편집기든 사용할 수 있습니다.

   예를 들어 다음 신뢰 정책 조각은 `Principal` 요소에서 AWS 계정 2개를 참조하는 방법을 나타냅니다. 사용자가 개별 AWS 계정 2개를 사용하도록 허용하여 이 역할을 수임하도록 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {"AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root"
        ]},
        "Action": "sts:AssumeRole"
    }
}
```

다른 계정에서 보안 주체를 지정할 경우 역할의 신뢰 정책에 계정을 추가하는 것은 신뢰 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 기본적으로 신뢰 계정의 어떠한 사용자도 역할을 위임할 수 없습니다. 새로이 신뢰받는 계정에 대한 관리자는 사용자가 역할을 수임할 수 있는 권한을 허용해야 합니다. 이를 위해 관리자는 사용자와 연결된 정책을 생성 또는 편집하여 `sts:AssumeRole` 작업에 대한 사용자 액세스를 허용합니다. 자세한 정보는 다음 절차 또는 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

4. 방금 생성한 파일을 사용하여 신뢰 정책을 업데이트하려면 다음 명령을 실행합니다.

   - aws iam update-assume-role-policy

신뢰할 수 있는 외부 계정 사용자에게 역할 사용을 허용하려면(AWS CLI)

자세한 정보와 이 절차에 대한 세부 정보는 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

1. 역할에 대한 권한 정책을 포함하는 JSON 파일을 생성하여 역할을 수임할 수 있는 권한을 허용합니다. 예를 들어 다음 정책에는 필요한 최소 권한이 포함되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-ID-THAT-CONTAINS-ROLE:role/ROLE-NAME"
  }
}
```

   설명문의 ARN을 사용자가 수임할 수 있는 역할의 ARN으로 바꿉니다.

2. 다음 명령을 실행하여 신뢰 정책이 IAM에 포함하는 JSON 파일을 업로드합니다.

   - aws iam create-policy

   이 명령의 출력 화면에는 정책의 ARN이 포함됩니다. 이후 단계에서 사용해야 하므로 이 ARN을 기록해 두십시오.

3. 정책을 연결할 사용자 또는 그룹을 결정합니다. 원하는 사용자 또는 그룹의 이름을 모르는 경우에는 다음 명령 중 하나를 사용하여 계정에 속한 사용자 또는 그룹 목록을 조회합니다.

   - aws iam list-users
   - aws iam list-groups

4. 다음 명령 중 한 가지를 사용하여 이전 단계에서 생성한 정책을 사용자 또는 그룹에게 추가합니다.

   - aws iam attach-user-policy
   - aws iam attach-group-policy

역할 권한 정책 수정(AWS CLI)

역할이 허용하는 권한을 변경하려면, 역할의 권한 정책을 수정합니다. IAM의 서비스 연결 역할 (p. 175)에 대한 권한 정책을 수정할 수 없습니다. 역할에 따른 서비스 내 권한 정책을 수정할 수 있는 가능성이 있습니다. 서비스에서 이 기능을 지원하는지 여부를 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [Yes] 링크를 선택합니다.

역할에서 허용되는 권한을 변경하려면(AWS CLI)

1. (옵션) 현재 역할과 연동되어 있는 권한을 확인하려면 다음 명령을 실행합니다.

   1. 인라인 정책을 나열하기 위한 aws iam list-role-policies
   2. 관리형 정책을 나열하기 위한 aws iam list-attached-role-policies
2. 역할 권한의 업데이트 명령은 관리형 정책을 업데이트할 때와 인라인 정책을 업데이트할 때 서로 다릅니다.

   관리형 정책을 업데이트하려면 다음 명령을 실행하여 새로운 버전의 관리형 정책을 생성합니다.

   - aws iam create-policy-version

   인라인 정책을 업데이트하려면 다음 명령을 실행합니다.

   - aws iam put-role-policy

역할 설명 수정(AWS CLI)

역할의 설명을 변경하려면 설명 텍스트를 수정합니다.

역할의 설명을 변경하려면(AWS CLI)

1. (옵션) 역할의 현재 설명을 보려면 다음 명령을 실행합니다.

   - aws iam get-role
2. 역할의 설명을 업데이트하려면 설명 파라미터와 함께 다음 명령을 실행합니다.

   - aws iam update-role

역할 최대 세션 기간 수정(AWS CLI)

AWS CLI 또는 API를 사용하여 수임한 역할에 대한 최대 세션 기간 설정을 지정하려면 최대 세션 기간 설정의 값을 수정합니다. 이 설정에는 1~12시간의 값을 지정할 수 있습니다. 값을 지정하지 않으면 기본 최댓값인 1시간이 적용됩니다. 이 설정은 AWS 서비스에서 수임하는 세션을 제한하지 않습니다.

> **Note**
>
> AWS CLI 또는 API에서 역할을 수임한 사람은 누구나 `duration-seconds` CLI 파라미터 또는 `DurationSeconds` API 파라미터를 사용해 더 긴 세션을 요청할 수 있습니다. `MaxSessionDuration` 설정은 `DurationSeconds` 파라미터를 사용해 요청할 수 있는 역할 세션에 대한 최대 기간을 결정합니다. 사용자가 `DurationSeconds` 파라미터의 값을 지정하지 않으면 보안 자격 증명이 한 시간 동안 유효하게 됩니다.

AWS CLI를 사용하여 수임한 역할에 대한 최대 세션 기간 설정을 변경하려면(AWS CLI)

1. (옵션) 역할에 대한 현재 최대 세션 기간 설정을 확인하려면 다음 명령을 실행합니다.

   - aws iam get-role

2. 역할의 최대 세션 기간 설정을 업데이트하려면 `max-sessionduration` CLI 파라미터 또는 `MaxSessionDuration` API 파라미터와 함께 다음 명령을 실행합니다.

   - aws iam update-role

   다음에 다른 사람이 이 역할을 수임할 때까지 변경 사항은 적용되지 않습니다. 이 역할에 대한 기존 세션을 취소하는 방법을 알아보려면 IAM 역할의 임시 보안 자격 증명 취소 (p. 273) 단원을 참조하십시오.

역할 권한 경계 수정(AWS CLI)

역할이 허용하는 최대 권한을 변경하려면, 역할의 권한 경계 (p. 363)를 수정합니다.

역할(AWS CLI)에 대한 권한 경계 설정에 사용된 관리형 정책을 변경하려면

1. (선택 사항) 역할의 현재 권한 경계 (p. 363)를 확인하려면 다음 명령을 실행합니다.

   - aws iam get-role

2. 다른 관리형 정책을 사용하여 역할에 대한 권한 경계를 업데이트하려면 다음 명령 중 하나를 실행합니다.

   - aws iam put-role-permissions-boundary

   역할은 권한 경계로서 하나의 관리형 정책만 가질 수 있습니다. 권한 경계를 변경하면 역할이 허용하는 최대 권한을 변경합니다.

역할 변경(AWS API)

AWS API를 사용하여 역할을 변경할 수 있습니다. 역할의 태그 세트를 변경하려면 IAM 엔터티에 대한 태그 관리(콘솔) (p. 293) 단원을 참조하십시오.

주제

- 역할 신뢰 정책 수정(AWS API) (p. 281)
- 역할 권한 정책 수정(AWS API) (p. 283)
- 역할 설명 수정(AWS API) (p. 283)
- 역할 최대 세션 기간 수정(AWS API) (p. 283)
- 역할 권한 경계 수정(AWS API) (p. 284)

역할 신뢰 정책 수정(AWS API)

역할을 맡을 수 있는 주체를 바꾸려면 역할의 신뢰 정책을 변경해야 합니다. 서비스 연결 역할 (p. 175)에 대한 신뢰 정책을 수정할 수 없습니다.

> **Note**
>
> 사용자가 역할 신뢰 정책에 보안 주체로 나열되지만 역할을 수임할 수 없는 경우 사용자의 권한 경계 (p. 363)를 확인하십시오. 사용자에 대한 권한 경계가 설정된 경우 권한 경계에서 `sts:AssumeRole` 작업이 허용되어야 합니다.

역할 신뢰 정책을 수정하려면(AWS API)

1. (선택 사항) 변경할 역할의 이름을 모르는 경우 다음 연산을 호출하여 계정의 역할을 나열합니다.

   - ListRoles

2. (옵션) 현재 역할의 신뢰 정책을 확인하려면 다음 연산을 호출합니다.

   - GetRole

3. 역할에 액세스할 수 있는 신뢰할 수 있는 보안 주체를 변경하려면 업데이트된 신뢰 정책을 추가하여 텍스트 파일을 생성합니다. 정책 구조를 작성할 때는 어떤 텍스트 편집기든 사용할 수 있습니다.

   예를 들어 다음 신뢰 정책 조각은 `Principal` 요소에서 AWS 계정 2개를 참조하는 방법을 나타냅니다. 사용자가 개별 AWS 계정 2개를 사용하도록 허용하여 이 역할을 수임하도록 합니다.

   ```
   {
       "Version": "2012-10-17",
       "Statement": {
           "Effect": "Allow",
           "Principal": {"AWS": [
               "arn:aws:iam::111122223333:root",
               "arn:aws:iam::444455556666:root"
           ]},
           "Action": "sts:AssumeRole"
       }
   }
   ```

   다른 계정에서 보안 주체를 지정할 경우 역할의 신뢰 정책에 계정을 추가하는 것은 신뢰 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 기본적으로 신뢰 계정의 어떠한 사용자도 역할을 위임할 수 없습니다. 새로이 신뢰받는 계정에 대한 관리자는 사용자가 역할을 수임할 수 있는 권한을 허용해야 합니다. 이를 위해 관리자는 사용자와 연결된 정책을 생성 또는 편집하여 `sts:AssumeRole` 작업에 대한 사용자 액세스를 허용합니다. 자세한 정보는 다음 절차 또는 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

4. 방금 생성한 파일을 사용하여 신뢰 정책을 업데이트하려면 다음 작업을 호출합니다.

   - UpdateAssumeRolePolicy

신뢰할 수 있는 외부 계정 사용자에게 역할 사용을 허용하려면(AWS API)

자세한 정보와 이 절차에 대한 세부 정보는 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

1. 역할에 대한 권한 정책을 포함하는 JSON 파일을 생성하여 역할을 수임할 수 있는 권한을 허용합니다. 예를 들어 다음 정책에는 필요한 최소 권한이 포함되어 있습니다.

   ```
   {
     "Version": "2012-10-17",
     "Statement": {
       "Effect": "Allow",
       "Action": "sts:AssumeRole",
       "Resource": "arn:aws:iam::ACCOUNT-ID-THAT-CONTAINS-ROLE:role/ROLE-NAME"
     }
   }
   ```

   설명문의 ARN을 사용자가 수임할 수 있는 역할의 ARN으로 바꿉니다.

2. 다음 작업을 호출하여 신뢰 정책이 IAM에 포함하는 JSON 파일을 업로드합니다.

   - CreatePolicy

   이 연산의 출력 화면에는 정책의 ARN이 포함됩니다. 이후 단계에서 사용해야 하므로 이 ARN을 기록해 두십시오.

3. 정책을 연결할 사용자 또는 그룹을 결정합니다. 원하는 사용자 또는 그룹의 이름을 모르는 경우에는 다음 작업 중 하나를 호출하여 계정에 속한 사용자 또는 그룹 목록을 조회합니다.

- ListUsers
- ListGroups

4. 다음 연산 중 하나를 호출하여 이전 단계에서 생성한 정책을 사용자 또는 그룹에게 추가합니다.

   - API: AttachUserPolicy
   - AttachGroupPolicy

역할 권한 정책 수정(AWS API)

역할이 허용하는 권한을 변경하려면, 역할의 권한 정책을 수정합니다. IAM의 서비스 연결 역할 (p. 175)에 대한 권한 정책을 수정할 수 없습니다. 역할에 따른 서비스 내 권한 정책을 수정할 수 있는 가능성이 있습니다. 서비스에서 이 기능을 지원하는지 여부를 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [Yes] 링크를 선택합니다.

역할에서 허용되는 권한을 변경하려면(AWS API)

1. (옵션) 현재 역할과 연동되어 있는 권한을 확인하려면 다음 연산을 호출합니다.

   1. 인라인 정책을 나열하기 위한 ListRolePolicies
   2. 관리형 정책을 나열하기 위한 ListAttachedRolePolicies

2. 역할 권한의 업데이트 작업은 관리형 정책을 업데이트할 때와 인라인 정책을 업데이트할 때 서로 다릅니다.

   관리형 정책을 업데이트하려면 다음 연산을 호출하여 새로운 버전의 관리형 정책을 생성합니다.

   - CreatePolicyVersion

   인라인 정책을 업데이트하려면 다음 연산을 호출합니다.

   - PutRolePolicy

역할 설명 수정(AWS API)

역할의 설명을 변경하려면 설명 텍스트를 수정합니다.

역할의 설명을 변경하려면(AWS API)

1. (옵션) 현재 역할의 설명을 확인하려면 다음 연산을 호출합니다.

   - GetRole

2. 역할의 설명을 업데이트하려면 설명 파라미터와 함께 다음 연산을 호출합니다.

   - UpdateRole

역할 최대 세션 기간 수정(AWS API)

AWS CLI 또는 API를 사용하여 수임한 역할에 대한 최대 세션 기간 설정을 지정하려면 최대 세션 기간 설정의 값을 수정합니다. 이 설정에는 1~12시간의 값을 지정할 수 있습니다. 값을 지정하지 않으면 기본 최댓값인 1시간이 적용됩니다. 이 설정은 AWS 서비스에서 수임하는 세션을 제한하지 않습니다.

> **Note**
>
> AWS CLI 또는 API에서 역할을 수임한 사람은 누구나 `duration-seconds` CLI 파라미터 또는 `DurationSeconds` API 파라미터를 사용해 더 긴 세션을 요청할 수 있습니다.

`MaxSessionDuration` 설정은 `DurationSeconds` 파라미터를 사용해 요청할 수 있는 역할 세션에 대한 최대 기간을 결정합니다. 사용자가 `DurationSeconds` 파라미터의 값을 지정하지 않으면 보안 자격 증명이 한 시간 동안 유효하게 됩니다.

API를 사용하여 수임한 역할에 대한 최대 세션 기간 설정을 변경하려면(AWS API)

1. (옵션) 역할에 대한 현재 최대 세션 기간 설정을 확인하려면 다음 연산을 호출합니다.
   - GetRole
2. 역할의 최대 세션 기간 설정을 업데이트하려면 `max-sessionduration` CLI 파라미터 또는 `MaxSessionDuration` API 파라미터와 함께 다음 연산을 호출합니다.
   - UpdateRole

   다음에 다른 사람이 이 역할을 수임할 때까지 변경 사항은 적용되지 않습니다. 이 역할에 대한 기존 세션을 취소하는 방법을 알아보려면 IAM 역할의 임시 보안 자격 증명 취소 (p. 273) 단원을 참조하십시오.

역할 권한 경계 수정(AWS API)

역할이 허용하는 최대 권한을 변경하려면, 역할의 권한 경계 (p. 363)를 수정합니다.

역할(AWS API)에 대한 권한 경계 설정에 사용된 관리형 정책을 변경하려면

1. (선택 사항) 역할의 현재 권한 경계 (p. 363)를 확인하려면 다음 작업을 호출합니다.
   - GetRole
2. 다른 관리형 정책을 사용하여 역할에 대한 권한 경계를 업데이트하려면 다음 작업 중 하나를 호출합니다.
   - PutRolePermissionsBoundary

   역할은 권한 경계로서 하나의 관리형 정책만 가질 수 있습니다. 권한 경계를 변경하면 역할이 허용하는 최대 권한을 변경합니다.

역할 또는 인스턴스 프로파일 삭제

역할이 더 이상 필요하지 않은 경우 역할 및 연결된 권한을 삭제하는 것이 좋습니다. 이렇게 하면 적극적으로 모니터링하거나 유지 관리하지 않은 미사용 엔터티가 없습니다.

역할이 EC2 인스턴스와 연결된 경우 인스턴스 프로파일에서 해당 역할을 제거한 다음 인스턴스 프로파일을 삭제할 수도 있습니다.

> Warning
>
> 삭제 예정인 역할 또는 인스턴스 프로필로 실행 중인 Amazon EC2 인스턴스가 없어야 합니다. 실행 중인 인스턴스와 관련된 역할 또는 인스턴스 프로필을 삭제하면 인스턴스에서 실행 중인 애플리케이션이 중단됩니다.

역할을 영구적으로 삭제하지 않으려면 역할을 비활성화하면 됩니다. 이렇게 하려면 역할의 정책을 변경한 다음 현재 세션을 모두 취소하십시오. 예를 들어 모든 AWS에 대한 액세스를 거부한 정책을 역할에 추가할 수 있습니다. 역할을 수임하려는 모든 사용자에 대한 액세스를 거부하도록 신뢰 정책을 편집할 수도 있습니다. 세션 취소에 대한 자세한 내용은 IAM 역할의 임시 보안 자격 증명 취소 (p. 273) 단원을 참조하십시오.

주제

- 역할 액세스 보기 (p. 285)

역할 액세스 보기

역할을 삭제하기 전에 역할이 마지막으로 사용된 시기를 검토하는 것이 좋습니다. AWS Management 콘솔, AWS CLI 또는 AWS API를 사용하여 이 작업을 수행할 수 있습니다. 이 정보를 사용하는 사람의 액세스 권한을 제거하지 않으려는 경우 이 정보를 보는 것이 중요합니다.

역할의 마지막 활동 날짜가 Access Advisor(Access Advisor) 탭에 보고된 마지막 날짜와 일치하지 않을 수 있습니다. Access Advisor(Access Advisor) (p. 472) 탭은 역할의 권한 정책에서 허용하는 서비스에 대한 활동만 보고합니다. 역할의 마지막 활동 날짜에는 AWS의 서비스에 액세스하려는 마지막 시도가 포함됩니다.

> **Note**
>
> 역할의 마지막 활동 및 Access Advisor 데이터에 대한 추적 기간은 이후 400일입니다. 해당 리전이 이러한 기능 지원을 시작한 날짜가 작년이었다면 이 기간이 더 짧아질 수 있습니다. 이 역할이 400일 전에 사용되었을 수 있습니다. 추적 기간에 대한 자세한 내용은 데이터가 추적되는 리전 (p. 471) 단원을 참조하십시오.

역할이 마지막으로 사용된 시기를 보려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Roles를 선택합니다.
3. 활동을 보려는 역할의 행을 찾습니다. 검색 필드를 사용하여 결과를 좁힐 수 있습니다. 마지막 활동 열에서 역할이 마지막으로 사용된 이후 일 수를 확인합니다. 역할이 추적 기간 내에 사용되지 않은 경우 테이블에 없음이 표시됩니다.
4. 자세한 정보를 볼 역할의 이름을 선택합니다. 역할의 요약 페이지에는 해당 역할이 마지막으로 사용된 날짜를 표시하는 마지막 활동도 포함되어 있습니다. 역할이 지난 400일 이내에 사용되지 않은 경우 마지막 활동에 Not accessed in the tracking period(추적 기간 동안 액세스되지 않음)가 표시됩니다.

역할이 마지막으로 사용된 시기를 보려면(AWS CLI)

`aws iam get-role` - `RoleLastUsed` 객체를 포함하여 역할에 대한 정보를 반환하려면 이 명령을 실행합니다. 이 객체에는 역할이 마지막으로 사용된 `LastUsedDate` 및 `Region`이 있습니다. `RoleLastUsed`가 있지만 값을 포함하지 않는 경우 추적 기간 내에 해당 역할이 사용되지 않은 것입니다.

역할이 마지막으로 사용된 시기를 보려면(AWS API)

`GetRole` - `RoleLastUsed` 객체를 포함하여 역할에 대한 정보를 반환하려면 이 작업을 호출합니다. 이 객체에는 역할이 마지막으로 사용된 `LastUsedDate` 및 `Region`이 있습니다. `RoleLastUsed`가 있지만 값을 포함하지 않는 경우 추적 기간 내에 해당 역할이 사용되지 않은 것입니다.

서비스 연결 역할 삭제

역할이 서비스 연결 역할 (p. 175)인 경우, 연결된 서비스의 설명서를 참조하여 역할을 삭제하는 방법을 알아보십시오. 콘솔의 IAM 역할 페이지에서 계정의 서비스 연결 역할을 볼 수 있습니다. 서비스 연결 역할은 테이블의 Trusted entities(신뢰할 수 있는 개체) 열에 (Service-linked role)((서비스 연결 역할))로 표시됩니다. 역할의 요약 페이지 배너에도 해당 역할이 서비스 역할임이 표시됩니다.

서비스에 서비스 연결 역할 삭제에 대한 설명서가 없는 경우 IAM 콘솔, AWS CLI 또는 API를 사용하여 역할을 삭제할 수 있습니다. 자세한 내용은 서비스 연결 역할 삭제 (p. 223) 단원을 참조하십시오.

IAM 역할 삭제(콘솔)

AWS Management 콘솔를 사용하여 역할을 삭제하는 경우, IAM 또한 자동으로 해당 역할과 연결된 정책을 삭제합니다. 해당 역할이 포함된 Amazon EC2 인스턴스 프로파일도 삭제됩니다.

> **Important**
>
> 경우에 따라 역할이 Amazon EC2 인스턴스 프로파일과 연결될 수 있으며, 역할과 인스턴스 프로파일의 이름이 같을 수 있습니다. 이 경우 AWS Management 콘솔을 사용하여 역할 및 인스턴스 프로파일을 삭제할 수 있습니다. 이 연결은 콘솔에서 생성한 인스턴스 프로파일과 역할에서 자동으로 발생합니다. AWS CLI, Windows PowerShell용 도구또는 AWS API에서 역할을 생성한 경우 역할과 인스턴스 프로파일의 이름이 서로 다를 수 있습니다. 이 경우 콘솔을 사용하여 역할과 인스턴스 프로파일을 삭제할 수 없습니다. 그 대신 AWS CLI, Windows PowerShell용 도구 또는 AWS API를 사용하여 먼저 인스턴스 프로파일에서 역할을 제거해야 합니다. 그런 다음 별도의 단계로 역할을 삭제해야 합니다.

역할을 삭제하려면(콘솔 사용)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택한 다음 삭제할 역할 이름 옆에 있는 확인란을 선택합니다.
3. 페이지 상단에서 Delete role(역할 삭제)을 선택합니다.
4. 확인 대화 상자가 나타나면 서비스 마지막 액세스 데이터를 검토합니다. 이 데이터는 선택한 각 역할이 AWS 서비스를 마지막으로 액세스한 일시를 보여 줍니다. 이를 통해 역할이 현재 활동 중인지 여부를 확인할 수 있습니다. 계속하려면 예, 삭제를 선택합니다. 확신한다면, 서비스 마지막 액세스 데이터가 로드되고 있을 때에도 삭제를 진행할 수 있습니다.

> **Note**
>
> 인스턴스 프로파일이 역할과 이름이 동일한 경우를 제외하고는 콘솔을 사용하여 인스턴스 프로파일을 삭제할 수 없습니다. 또한 이전 절차에서 설명한 바와 같이 역할 삭제 과정의 일부로 인스턴스 프로파일을 삭제해야 합니다. 역할까지 삭제하지 않고 인스턴스 프로파일을 삭제하려면 AWS CLI 또는 AWS API를 사용해야 합니다. 자세한 내용은 다음 단원을 참조하십시오.

IAM 역할 삭제(AWS CLI)

AWS CLI를 사용하여 역할을 삭제하는 경우 먼저 해당 역할과 연결된 정책을 삭제해야 합니다. 또한 해당 역할이 들어 있는 연결된 인스턴스 프로파일은 별도로 삭제해야 합니다.

역할을 삭제하려면(AWS CLI)

1. 삭제할 역할의 이름을 모르는 경우 다음 명령을 입력하여 계정의 역할을 나열합니다.

   ```
   $ aws iam list-roles
   ```

   목록에는 각 역할의 Amazon 리소스 이름(ARN)이 포함되어 있습니다. CLI 명령에서 역할을 참조하려면 ARN이 아니라 역할 이름을 사용해야 합니다. 예를 들어, 어떤 역할의 ARN이 `arn:aws:iam::123456789012:role/myrole`인 경우 참조할 역할은 **`myrole`**입니다.
2. 역할이 속해 있는 모든 인스턴스 프로파일에서 역할을 제거합니다.

   a. 역할이 연결된 모든 인스턴스 프로파일을 나열하려면 다음 명령을 입력합니다.

   ```
   $ aws iam list-instance-profiles-for-role --role-name role-name
   ```

b. 인스턴스 프로파일에서 역할을 제거하려면 각 인스턴스 프로파일에 대해 다음 명령을 입력합니다.

```
$ aws iam remove-role-from-instance-profile --instance-profile-name instance-profile-name --role-name role-name
```

3. 역할과 연결된 모든 정책을 삭제합니다.

   a. 해당 역할에 있는 모든 정책을 나열하려면 다음 명령을 입력합니다.

   ```
   $ aws iam list-role-policies --role-name role-name
   ```

   b. 역할에서 각 정책을 삭제하려면 각 정책에 대해 다음 명령을 입력합니다.

   ```
   $ aws iam delete-role-policy --role-name role-name --policy-name policy-name
   ```

4. 다음 명령을 입력하여 역할을 삭제합니다.

```
$ aws iam delete-role --role-name role-name
```

5. 역할과 연결된 인스턴스 프로파일을 다시 사용할 계획이 없는 경우 다음 명령을 입력하여 삭제할 수 있습니다.

```
$ aws iam delete-instance-profile --instance-profile-name instance-profile-name
```

IAM 역할 삭제(AWS API)

IAM API를 사용하여 역할을 삭제하려면 먼저 해당 역할과 연결된 정책을 삭제해야 합니다. 또한 해당 역할이 들어 있는 연결된 인스턴스 프로파일은 별도로 삭제해야 합니다.

역할을 삭제하려면(AWS API)

1. 역할이 속해 있는 모든 인스턴스 프로파일을 나열하려면 ListInstanceProfilesForRole을 호출하십시오.

   역할이 속해 있는 모든 인스턴스 프로파일에서 해당 역할을 제거하려면 RemoveRoleFromInstanceProfile을 호출하십시오. 역할 이름과 인스턴스 프로파일 이름을 전달해야 합니다.

   역할과 연결된 인스턴스 프로파일을 다시 사용하지 않을 경우 DeleteInstanceProfile을 호출하여 삭제할 수 있습니다.
2. 역할에 대한 모든 정책을 나열하려면 ListRolePolicies를 호출하십시오.

   역할과 연결된 모든 정책을 삭제하려면 DeleteRolePolicy를 호출하십시오. 역할 이름과 정책 이름을 전달해야 합니다.
3. DeleteRole을 호출하여 역할을 삭제하십시오.

관련 정보

인스턴스 프로파일에 대한 일반적인 정보는 인스턴스 프로파일 사용 (p. 271) 단원을 참조하십시오.

서비스 연결 역할에 대한 일반적인 내용은 서비스 연결 역할 사용 (p. 218) 단원을 참조하십시오.

IAM 역할과 리소스 기반 정책의 차이

일부 AWS 서비스에 대해서는 리소스에 대한 교차 계정 액세스 권한을 부여할 수 있습니다. 이렇게 하려면 역할을 프록시로 사용하는 대신 공유하고자 하는 리소스에 정책을 직접 연결하면 됩니다. 공유하려는 리소스

는 반드시 리소스 기반 정책 (p. 372)을 지원해야 합니다. ID 기반 정책과 달리 리소스 기반 정책은 해당 리소스에 액세스할 수 있는 사용자(보안 주체)를 지정합니다.

> Note
>
> IAM 역할 및 리소스 기반 정책은 단일 파티션 내에서만 계정 간에 액세스 권한을 위임합니다. 예를 들어 표준 `aws` 파티션의 미국 서부(캘리포니아 북부 지역)에 계정이 있다고 가정합니다. `aws-cn` 파티션의 중국(베이징)에도 계정이 있습니다. 중국(베이징)의 계정에서 Amazon S3 리소스 기반 정책을 사용하여 표준 `aws` 계정의 사용자에 대한 액세스를 허용할 수 없습니다.

리소스 기반 정책을 사용한 교차 계정 액세스는 역할을 사용한 교차 계정 액세스에 비해 몇 가지 이점이 있습니다. 리소스 기반 정책을 통해 액세스한 리소스로 인해 보안 주체는 여전히 신뢰할 수 있는 계정에서 작업을 할 수 있고, 역할 권한을 수신하기 위해 자신의 권한을 포기할 필요가 없습니다. 즉, 보안 주체는 신뢰하는 계정의 리소스에 액세스하는 동시에 신뢰할 수 있는 계정의 리소스에 계속 액세스할 수 있습니다. 다른 계정의 공유 리소스로 정보를 복사하거나 공유 리소스의 정보를 복사하는 등의 작업에서 이는 특히 유용합니다.해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

리소스 기반 정책에서 지정할 수 있는 보안 주체에는 계정, IAM 사용자, 연동 사용자, IAM 역할, 위임된 역할 세션 또는 AWS 서비스가 포함됩니다. 자세한 내용은 보안 주체 지정 (p. 589) 단원을 참조하십시오.

다음 목록에는 리소스 기반 정책을 지원하는 일부 AWS 서비스가 나와 있습니다. 보안 주체 대신 리소스에 권한 정책을 연결할 수 있도록 지원하는 AWS 서비스는 늘어나고 있습니다. 해당 서비스의 전체 목록은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하고 리소스 기반 열의 값이 예인 서비스를 찾아보십시오.

- Amazon S3 버킷 – 정책은 버킷과 연결되지만, 버킷과 그 안에 포함된 객체에 대한 액세스를 모두 제어합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 액세스 제어 단원을 참조하십시오.

  일부의 경우, 교차 계정의 Amazon S3 액세스 권한에 대한 역할을 사용하는 것이 최선일 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 연습 예제를 참조하십시오.
- Amazon Simple Notification Service(Amazon SNS) 주제 – 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 주제에 대한 액세스 관리 단원을 참조하십시오.
- Amazon Simple Queue Service(Amazon SQS) 대기열 – 자세한 내용은 Amazon Simple Queue Service 개발자 안내서의 부록: 액세스 정책 언어를 참조하십시오.

리소스 기반 정책에서 AWS 권한 위임에 대하여

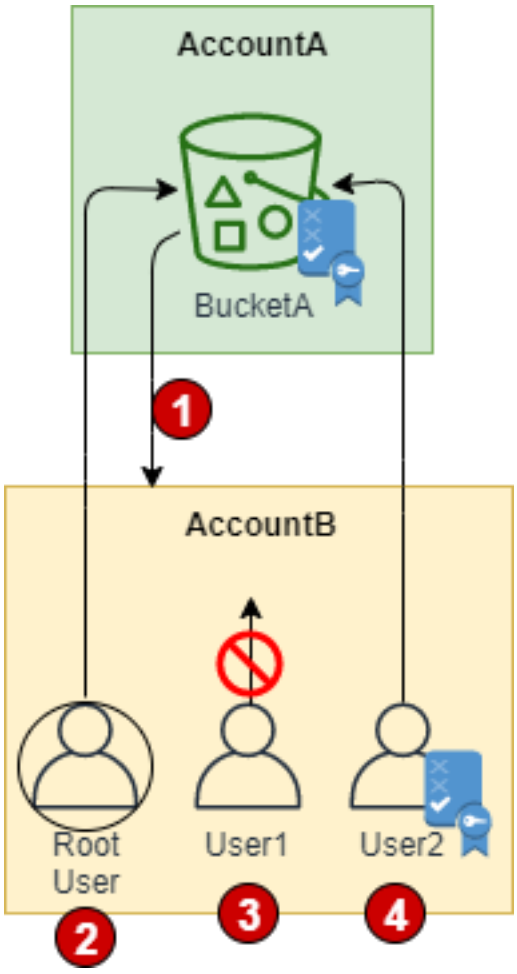
리소스가 계정의 보안 주체에 권한을 부여하는 경우 이러한 권한을 특정 IAM 자격 증명에 위임할 수 있습니다. 자격 증명은 사용자, 사용자 그룹 또는 계정의 역할입니다. 자격 증명에 정책을 연결하여 권한을 위임합니다. 리소스 소유 계정에서 허용하는 최대 권한을 부여할 수 있습니다.

리소스 기반 정책에서는 계정의 모든 보안 주체에게 리소스에 대한 전체 관리 액세스 권한을 허용한다고 가정합니다. 이제 AWS 계정의 보안 주체에게 전체 액세스 권한, 읽기 전용 액세스 권한 또는 기타 부분적 액세스 권한을 위임할 수 있습니다. 또는 리소스 기반 정책에서 목록 액세스 권한만 허용하는 경우에는 목록 액세스 권한만 위임할 수 있습니다. 계정에 부여된 것보다 더 많은 권한을 위임하려고 해도 보안 주체는 목록 액세스 권한만 갖게 됩니다. IAM 자격 증명에 정책을 연결하는 방법에 대한 자세한 내용은 IAM 정책 관리 (p. 435) 단원을 참조하십시오 .

> Note
>
> IAM 역할 및 리소스 기반 정책은 단일 파티션 내에서만 계정 간에 액세스 권한을 위임합니다. 예를 들어 표준 `aws` 파티션의 계정과 `aws-cn` 파티션의 계정 간에 교차 계정 액세스를 추가할 수 없습니다.

예를 들어 `AccountA` 및 `AccountB`를 관리한다고 가정합니다. `AccountA`에는 `BucketA`라는 이름의 Amazon S3 버킷이 있습니다. 모든 `AccountB` 보안 주체에게 버킷의 객체에 대한 전체 액세스 권한을 허용하는 `BucketA`에 리소스 기반 정책을 연결합니다. 해당 버킷의 모든 객체를 생성, 읽기 또는 삭제할 수 있습니다. `AccountB`에서는 `User2`이라는 IAM 사용자에게 정책을 연결합니다. 이 정책은 사용자에게

BucketA의 객체에 대한 읽기 전용 액세스를 허용합니다. 즉, User2에서는 객체를 볼 수 있지만 객체를 생성, 편집 또는 삭제할 수는 없습니다.



1. AccountA은 리소스 기반 정책에서 보안 주체로서 AccountB를 명명하여 AccountB에게 BucketA에 대한 전체 액세스 권한을 제공합니다. 따라서 AccountB에 BucketA에서 작업을 수행할 수 있는 권한이 부여되고 AccountB 관리자는 AccountB의 사용자에게 액세스 권한을 위임할 수 있습니다.
2. AccountB 루트 사용자는 계정에 부여된 모든 권한을 가집니다. 따라서 루트 사용자은 BucketA에 대한 전체 액세스 권한을 가집니다.
3. AccountB 관리자는 User1에 대한 액세스 권한을 부여하지 않습니다. 기본적으로 사용자에게는 명시적으로 부여된 권한을 제외한 어떤 권한도 없습니다. 따라서 User1에는 BucketA에 대한 액세스 권한이 없습니다 .
4. AccountB 관리자는 User2에게 BucketA에 대한 읽기 전용 액세스 권한을 부여합니다. User2에서 버킷의 객체를 볼 수 있습니다. AccountB가 위임할 수 있는 최대 액세스 수준은 계정에 부여된 액세스 수준입니다. 이 경우 리소스 기반 정책에서는 AccountB에 대한 전체 액세스 권한을 부여하지만 User2에는 읽기 전용 액세스 권한만 부여됩니다.

IAM은 보안 주체가 요청을 할 때 보안 주체의 권한을 평가합니다. 따라서 와일드카드(*)를 사용하여 사용자에게 리소스에 대한 전체 액세스 권한을 부여하면 보안 주체는 AWS 계정이 액세스 권한을 가지고 있는 모든 리소스에 액세스할 수 있습니다. 사용자 정책을 생성한 이후에 추가하거나 액세스 권한을 획득한 리소스의 경우에도 마찬가지입니다.

앞의 예에서 AccountB이 모든 계정의 모든 리소스에 대한 전체 액세스 권한을 허용하는 User2에 정책을 연결했다면 User2은 AccountB에 액세스 권한이 있는 모든 리소스에 자동으로 액세스할 수 있었을 것입니

다. 여기에는 `BucketA` 액세스 권한과 `AccountA`의 리소스 기반 정책에서 부여한 다른 리소스에 대한 액세스 권한이 포함됩니다 .

> Important
>
> 신뢰 관계가 설정된 엔터티에만 액세스 권한을 부여하고 필요한 최소 수준의 액세스 권한만 부여합니다. 신뢰받는 엔터티가 다른 AWS 계정인 경우 언제든지 해당 계정은 IAM 계정에 속한 어떤 사용자에게도 다시 액세스 권한을 위임할 수 있습니다. 신뢰하는 AWS 계정은 권한이 부여된 액세스 범위 내에서만 권한을 위임할 수 있으며, 계정에 부여된 권한보다 더 많은 액세스 권한을 위임할 수 없습니다.

권한, 정책 및 정책 작성에 사용하는 권한 정책 언어에 대한 자세한 내용은 액세스 관리 (p. 348) 단원을 참조하십시오.

IAM 사용자 및 역할 태그 지정

IAM 태그를 사용하여 키–값 페어 태그를 사용하여 IAM 엔터티(사용자 또는 역할)에 사용자 지정 속성을 추가할 수 있습니다. 예를 들어 사용자에게 위치 정보를 추가하려면 태그 키 **`location`** 및 태그 값 **`us_wa_seattle`**을 추가할 수 있습니다. 또는 세 개의 개별 위치 태그 키–값 페어 **`loc-country = us`**, **`loc-state = wa`** 및 **`loc-city = seattle`**을 사용할 수도 있습니다. 태그를 사용하여 리소스에 대한 엔터티의 액세스를 제어하거나 엔터티에 연결할 수 있는 태그를 제어할 수 있습니다. 태그를 사용하여 액세스를 제어하는 방법에 대한 자세한 내용은 IAM 리소스 태그를 사용하여 IAM 사용자 및 역할에 대한 액세스 제어 (p. 382) 단원을 참조하십시오.

역할을 수임하거나 사용자를 연동할 때 AWS STS에서 태그를 사용하여 사용자 지정 속성을 추가할 수도 있습니다. 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

AWS 태그 이름 지정 규칙 선택

IAM 사용자 및 역할에 태그 연결을 시작할 때 태그 이름 지정 규칙을 신중하게 선택합니다. 모든 AWS 태그에 동일한 규칙을 적용합니다. 정책에서 태그를 사용하여 AWS 리소스에 대한 액세스를 제어하는 경우 특히 중요합니다. AWS에서 태그를 이미 사용하고 있다면 이름 지정 규칙을 검토하고 적절하게 조정하십시오. 태그 지정 범주 및 전략에 대한 자세한 내용은 AWS General Reference 안내서의 AWS 리소스 AWS 태그 지정을 참조하십시오. 태그 지정 사용 사례 및 모범 사례를 보려면 태그 지정 모범 사례 백서를 다운로드하십시오.

IAM 및 AWS STS의 태그 지정 규칙

IAM 및 AWS STS에서 태그의 생성과 적용을 관리하는 규칙은 여러 가지가 있습니다.

태그 이름 지정

IAM 사용자, IAM 역할, AWS STS 역할 맡기 세션 및 AWS STS 연동 사용자 세션에 대한 태그 이름 지정 규칙을 공식화하는 경우 다음 규칙을 준수합니다.

- 태그 키 및 값은 문자, 숫자, 공백 및 _ . : / = + - @ . 기호를 포함할 수 있습니다.
- 태그 키–값 페어는 대소문자를 구분하지 않지만 대소문자는 유지됩니다. 즉, 별도의 **`Department`** 및 **`department`** 태그 키를 가질 수 없음을 의미합니다. **`Department=foo`** 태그로 사용자 태그를 지정하고 **`department=bar`** 태그를 추가하면 첫 번째 태그가 바뀝니다. 두 번째 태그는 추가되지 않습니다.
- **`aws:`**로 시작하는 태그 키 또는 값을 생성할 수 없습니다. 이 태그 접두사는 AWS 내부 전용으로 예약되어 있습니다.
- **`phoneNumber =`** 와 같이 값이 비어 있는 태그를 만들 수 있습니다. 빈 태그 키는 생성할 수 없습니다.
- 단일 태그에 여러 값을 지정할 수 없지만 단일 값으로 사용자 지정 다중 값 구조를 생성할 수 있습니다. 예를 들어 사용자 Zhang이 엔지니어링 팀과 QA 팀에서 근무한다고 가정합니다. **`team = Engineering`** 태

그를 연결하고 **team = QA** 태그를 연결한 경우 태그 값을 **Engineering**에서 **QA**로 변경합니다 . 대신 사용자 지정 구분자를 사용하여 단일 태그에 여러 값을 포함할 수 있습니다. 이 예에서는 Zhang에게 **team = Engineering:QA** 태그를 연결할 수 있습니다.

> Note
>
> 이 예제에서 **team** 태그를 사용하여 엔지니어에 대한 액세스를 제어하려면 **Engineering:QA**를 포함하여 **Engineering**을 포함할 수 있는 모든 구성을 허용하는 정책을 만들어야 합니다. 정책에서의 태그 사용에 대한 자세한 내용은 IAM 리소스 태그를 사용하여 IAM 사용자 및 역할에 대한 액세스 제어 (p. 382) 단원을 참조하십시오.

태그 적용 및 편집

태그를 IAM 엔터티(사용자 및 역할)에 연결할 때 다음 규칙을 준수하십시오.

- 그룹이나 정책이 아닌 사용자나 역할에 태그를 지정할 수 있습니다.
- Tag Editor를 사용하여 IAM 엔터티에 태그를 지정할 수 없습니다. Tag Editor는 IAM 태그를 지원하지 않습니다. Tag Editor를 다른 서비스와 함께 사용하는 방법에 대한 내용은 AWS Management 콘솔 사용 설명서의 Tag Editor 작업 단원을 참조하십시오.
- IAM 엔터티에 태그를 지정하려면 특정 권한이 있어야 합니다. 역할과 사용자에 태그를 지정하거나 태그를 해제하려면 태그를 나열할 수 있는 권한이 있어야 합니다. 자세한 내용은 IAM 엔터티 태그 지정에 필요한 권한 (p. 291) 단원을 참조하십시오.
- 라우팅 테이블에 추가할 수 있는 경로의 수에는 제한이 있습니다. 자세한 정보는 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.
- 여러 개의 IAM 엔터티에 동일한 태그를 적용할 수 있습니다. 예를 들어, 12명의 멤버가 있는 AWS_Development 부서가 있다고 가정합니다. 태그 키 **department** 및 값 **awsDevelopment**(**department = awsDevelopment**)를 가진 12명의 사용자와 역할이 있을 수 있습니다. 태그 지정을 지원하는 다른 서비스 (p. 573)의 리소스에도 동일한 태그를 사용할 수 있습니다.
- IAM 엔터티는 동일한 태그 키의 여러 인스턴스를 가질 수 없습니다. 예를 들어 태그 키–값 페어 **costCenter = 1234**가 지정된 사용자가 있는 경우 태그 키–값 페어 **costCenter = 5678**을 연결할 수 있습니다. IAM은 **costCenter** 태그의 값을 **5678**로 업데이트합니다.
- IAM 사용자 또는 역할에 연결된 태그를 편집하려면 새 값으로 태그를 연결하여 기존 태그를 덮어씁니다. 예를 들어, 태그 키–값 페어 **department = Engineering**을 가진 사용자가 있다고 가정합니다. 사용자를 QA 부서로 이동해야 하는 경우 **department = QA** 태그 키–값 쌍을 사용자에게 연결할 수 있습니다. 결과적으로 **department** 태그 키의 **Engineering** 값이 **QA** 값으로 대체됩니다.

IAM 엔터티 태그 지정에 필요한 권한

IAM 엔터티(사용자 또는 역할)이 다른 엔터티에 태그를 지정할 수 있도록 권한을 구성해야 합니다. IAM 정책에서 다음 IAM 태그 작업 중 하나 또는 모두를 지정할 수 있습니다.

- `iam:ListRoleTags`
- `iam:ListUserTags`
- `iam:TagRole`
- `iam:TagUser`
- `iam:UntagRole`
- `iam:UntagUser`

특정 사용자의 태그를 추가, 나열 또는 제거하도록 IAM 엔터티를 허용하려면

태그를 관리해야 하는 IAM 엔터티의 권한 정책에 다음 명령문을 추가합니다. 계정 번호를 사용하여 *<username>*을 관리해야 할 사용자 이름으로 바꿉니다. 이 예제 JSON 정책 문서를 사용하여 정책을 생성하

는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:ListUserTags",
        "iam:TagUser",
        "iam:UntagUser"
    ],
    "Resource": "arn:aws:iam:*:<account-number>:user/<username>"
}
```

IAM 사용자가 태그를 자체 관리할 수 있게 하려면

사용자가 자신의 태그를 관리할 수 있도록 권한 정책에 다음 명령문을 추가합니다. 이 예제 JSON 정책 문서를 사용하여 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:ListUserTags",
        "iam:TagUser",
        "iam:UntagUser"
    ],
    "Resource": "arn:aws:iam:*:user/${aws:username}"
}
```

IAM 엔터티를 사용하여 특정 사용자에게 태그를 추가하려면

특정 사용자의 태그를 추가하기만 하고 제거하지는 않으려면 IAM 엔터티의 권한 정책에 다음 명령문을 추가합니다.

> **Note**
>
> `iam:AddRoleTags` 및 `iam:AddUserTags` 작업을 수행하려면 `iam:ListRoleTags` 및 `iam:ListUserTags` 작업도 포함해야 합니다.

이 정책을 사용하려면 *<username>*을 관리해야 할 사용자 이름으로 바꿉니다. 이 예제 JSON 정책 문서를 사용하여 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:ListUserTags",
        "iam:TagUser"
    ],
    "Resource": "arn:aws:iam:*:<account-number>:user/<username>"
}
```

특정 역할의 태그를 추가, 나열 또는 제거하도록 IAM 엔터티를 허용하려면

태그를 관리해야 하는 IAM 엔터티의 권한 정책에 다음 명령문을 추가합니다. *<rolename>*을 관리해야 하는 역할의 이름으로 바꿉니다. 이 예제 JSON 정책 문서를 사용하여 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

```
{
```

```
    "Effect": "Allow",
    "Action": [
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:UntagRole"
    ],
    "Resource": "arn:aws:iam:*:<account-number>:role/<rolename>"
}
```

또는 IAMFullAccess 등의 AWS 관리형 정책을 사용하여 IAM에 모든 액세스 권한을 제공할 수 있습니다.

IAM 엔터티에 대한 태그 관리(콘솔)

AWS Management 콘솔에서 IAM 사용자 또는 역할에 대한 태그를 관리할 수 있습니다.

사용자 또는 역할에 대한 태그를 관리하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 콘솔의 탐색 창에서 역할 또는 사용자를 선택한 다음 편집할 엔터티의 이름을 선택합니다.
3. 태그 탭을 선택하고 다음 작업 중 하나를 완료하십시오.
   - 엔터티에 아직 태그가 없는 경우 태그 추가를 선택합니다.
   - 기존 태그 세트를 관리하려면 태그 편집을 선택합니다.
4. 태그를 추가하거나 제거하여 태그 세트를 완성합니다. 변경 사항 저장을 선택합니다.

IAM 엔터티에 대한 태그 관리(AWS CLI 또는 AWS API)

IAM 사용자 및 역할에 대한 태그를 나열, 연결 또는 제거할 수 있습니다. AWS CLI 또는 AWS API를 사용하여 IAM 사용자 및 역할에 대한 태그를 관리할 수 있습니다.

IAM 역할에 현재 연결된 태그를 나열하려면(AWS CLI 또는 AWS API)

- AWS CLI: aws iam list-role-tags
- AWS API: ListRoleTags

IAM 사용자에 현재 연결된 태그를 나열하려면(AWS CLI 또는 AWS API)

- AWS CLI: aws iam list-user-tags
- AWS API: ListUserTags

IAM 역할에 태그를 연결하려면(AWS CLI 또는 AWS API)

- AWS CLI: aws iam tag-role
- AWS API: TagRole

IAM 사용자에 태그를 연결하려면(AWS CLI 또는 AWS API)

- AWS CLI: aws iam tag-user
- AWS API: TagUser

IAM 역할에서 태그를 제거하려면(AWS CLI 또는 AWS API)

- AWS CLI: aws iam untag-role
- AWS API: UntagRole

IAM 사용자의 태그를 제거하려면(AWS CLI 또는 AWS API)

- AWS CLI: aws iam untag-user
- AWS API: UntagUser

다른 AWS 서비스의 리소스에 대한 태그 연결 정보는 해당 서비스의 설명서를 참조하십시오.

태그를 사용하여 IAM 권한 정책으로 보다 세부적인 권한을 설정하는 방법에 대한 자세한 내용은 IAM 정책 요소: 변수 및 태그 (p. 615) 단원을 참조하십시오.

AWS STS에서 세션 태그 전달

세션 태그는 IAM 역할을 맡거나 AWS STS에서 사용자를 연동할 때 전달하는 키-값 페어 속성입니다. STS 또는 자격 증명 공급자(IdP)를 통해 AWS CLI 또는 AWS API를 요청하면 됩니다. AWS STS를 사용하여 임시 보안 자격 증명을 요청하면 세션이 생성됩니다. 세션은 만료되고 액세스 키 페어 및 세션 토큰과 같은 자격 증명을 갖습니다. 세션 자격 증명을 사용하여 후속 요청을 하면 요청 컨텍스트 (p. 599)에 `aws:PrincipalTag (p. 657)` 컨텍스트 키가 포함됩니다. 정책의 `Condition` 요소에서 `aws:PrincipalTag` 키를 사용하여 해당 태그를 기반으로 액세스를 허용하거나 거부할 수 있습니다.

임시 자격 증명을 사용하여 요청하면 보안 주체에 태그 세트가 포함될 수 있습니다. 이러한 태그는 다음 소스에서 가져옵니다.

1. 세션 태그 – 이 태그는 역할을 맡거나 AWS CLI 또는 AWS API를 사용하여 사용자를 연동할 때 전달됩니다. 이러한 작업에 대한 자세한 내용은 아래 세션 태그 지정 작업 (p. 294) 단원을 참조하십시오.
2. 수신 전이적 세션 태그 – 이 태그는 역할 체인의 이전 세션에서 상속됩니다. 자세한 내용은 이 주제의 후반부에서 세션 태그를 사용하는 역할 체인 (p. 300) 단원을 참조하십시오.
3. IAM 태그 – 이 태그는 사용자가 맡은 IAM 역할에 연결되어 있습니다.

주제

세션 태그 지정 작업

AWS STS에서 다음 AWS CLI 또는 AWS API 작업을 사용하여 세션 태그를 전달할 수 있습니다. AWS Management 콘솔 역할 전환 (p. 256) 기능을 사용하여 세션 태그를 전달할 수 없습니다.

세션 태그를 전이적으로 설정할 수도 있습니다. 전이적 태그는 역할 체인 동안 지속됩니다. 자세한 내용은 세션 태그를 사용하는 역할 체인 (p. 300) 단원을 참조하십시오.

세션 태그 전달 방법 비교

방법	역할을 맡을 수 있는 사용자	태그를 전달하는 방법	전이적 태그를 설정하는 방법
`assume-role` CLI 또는 `AssumeRole` API 작업	IAM 사용자 또는 세션	`Tags` API 파라미터 또는 `--tags` CLI 옵션	`TransitiveTagKeys` API 파라미터 또는 `--transitive-tag-keys` CLI 옵션
`assume-role-with-saml` CLI 또는 `AssumeRoleWithSAML` API 작업	SAML 자격 증명 공급자를 사용하여 인증된 모든 사용자	`PrincipalTag` SAML 속성	`TransitiveTagKeys` SAML 속성
`assume-role-with-web-identity` CLI 또는 `AssumeRoleWithWebIdentity` API 작업	웹 자격 증명 공급자를 사용하여 인증된 모든 사용자	`PrincipalTag` 웹 자격 증명 토큰	`TransitiveTagKeys` 웹 자격 증명 토큰
`get-federation-token` CLI 또는 `GetFederationToken` API 작업	IAM 사용자 또는 루트 사용자	`Tags` API 파라미터 또는 `--tags` CLI 옵션	지원되지 않음

다음 조건 중 하나에 해당하는 경우 세션 태그 지정을 지원하는 작업이 실패할 수 있습니다.

- 50개 이상의 세션 태그를 전달하는 경우
- 세션 태그 키의 일반 텍스트가 128자를 초과하는 경우
- 세션 태그 값의 일반 텍스트가 256자를 초과하는 경우
- 세션 정책의 일반 텍스트의 총 크기가 2048자를 초과하는 경우
- 결합된 세션 정책 및 세션 태그의 총 압축 크기가 너무 큰 경우 작업이 실패할 경우 오류 메시지는 결합된 정책과 태그가 최대 크기 제한에 얼마나 가까운지를 백분율로 나타냅니다.

세션 태그에 대해 알아야 할 사항

세션 태그를 사용하기 전에 세션 및 태그에 대한 다음 세부 정보를 검토하십시오.

- 세션 태그는 세션을 요청하는 동안 지정하는 보안 주체 태그입니다. 태그는 세션의 자격 증명을 사용하여 생성한 요청에 적용됩니다.
- 세션 태그는 키-값 페어입니다. 예를 들어, 세션에 연락처 정보를 추가하려면 세션 태그 키 `email` 및 태그 값 `johndoe@example.com`을 추가할 수 있습니다.
- 세션 태그는 IAM 및 AWS STS의 태그 이름 지정 규칙 (p. 290)을 따라야 합니다. 이 주제에는 세션 태그에 적용되는 대/소문자 구분 및 제한된 접두사에 대한 정보가 포함되어 있습니다.
- 새 세션 태그는 대/소문자에 관계없이 동일한 태그 키의 기존에 맡은 역할 또는 연동 사용자 태그를 재정의합니다.
- AWS Management 콘솔을 사용하여 세션 태그를 전달할 수는 없습니다.
- 세션 태그는 현재 세션에서만 유효합니다.

- 세션 태그는 역할 체인 (p. 176)을 지원합니다. 기본적으로 태그는 후속 역할 세션에 전달되지 않습니다. 그러나 세션 태그를 전이적으로 설정할 수 있습니다. 전이적 태그는 역할 체인 동안 지속됩니다. 자세한 내용은 세션 태그를 사용하는 역할 체인 (p. 300) 단원을 참조하십시오.
- 세션 태그를 사용하여 리소스에 대한 액세스를 제어하거나 후속 세션에 전달할 수 있는 태그를 제어할 수 있습니다. 자세한 내용은 ABAC에 SAML 세션 태그 사용 (p. 53) 단원을 참조하십시오.
- AWS CloudTrail 로그에서 세션 태그를 포함하여 세션의 보안 주체 태그를 볼 수 있습니다. 자세한 내용은 CloudTrail에서 세션 태그 보기 (p. 301) 단원을 참조하십시오.
- 각 세션 태그에 대해 단일 값을 전달해야 합니다. 다중 값 세션 태그는 지원되지 않습니다.
- 최대 50개의 세션 태그를 전달할 수 있습니다. 이러한 제한 및 기타 제한에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.
- AWS 변환은 전달된 세션 정책과 세션 태그를 별도의 제한이 있는 압축된 이진 형식으로 압축합니다. 이 제한을 초과할 경우 AWS CLI 또는 AWS API 오류 메시지는 결합된 정책과 태그가 최대 크기 제한에 얼마나 가까운지를 백분율로 나타냅니다.

세션 태그를 추가하는 데 필요한 권한

API 작업과 일치하는 작업 외에도 정책에는 다음과 같은 권한 전용 작업이 있어야 합니다.

```
sts:TagSession
```

이 작업은 다음 조건 키와 함께 사용할 수 있습니다.

- `aws:PrincipalTag (p. 657)` – 이 키를 사용하여 요청을 하는 보안 주체에 연결된 태그를 정책에서 지정한 태그와 비교합니다. 예를 들어, 요청을 하는 보안 주체에 지정된 태그가 있는 경우에만 보안 주체가 세션 태그를 전달하도록 허용할 수 있습니다.
- `aws:RequestTag (p. 659)` – 이 키를 사용하여 요청에서 전달된 태그 키-값 페어를 정책에서 지정한 태그 페어와 비교합니다. 예를 들어, 보안 주체가 지정된 세션 태그를 전달할 수는 있지만, 지정된 값만 사용하도록 허용할 수 있습니다.
- `aws:ResourceTag (p. 659)` – 이 키를 사용하여 정책에서 지정한 태그 키-값 페어를 리소스에 연결된 키-값 페어와 비교합니다. 예를 들어, 보안 주체가 맡고 있는 역할에 지정된 태그가 포함된 경우에만 보안 주체가 세션 태그를 전달하도록 허용할 수 있습니다.
- `aws:TagKeys (p. 662)` – 이 키를 사용하여 요청의 태그 키를 정책에서 지정한 키와 비교합니다. 예를 들어, 보안 주체가 지정된 태그 키를 가진 세션 태그만 전달하도록 허용할 수 있습니다. 이 조건 키는 전달할 수 있는 최대 세션 태그 세트를 제한합니다.
- `sts:TransitiveTagKeys (p. 673)` - 이 키를 사용하여 요청의 전이적 세션 태그 키와 정책에 지정된 전이적 세션 태그 키를 비교합니다. 예를 들어, 보안 주체가 특정 태그만 전이적으로 설정하도록 허용하는 정책을 작성할 수 있습니다. 전이적 태그는 역할 체인 동안 지속됩니다. 자세한 내용은 세션 태그를 사용하는 역할 체인 (p. 300) 단원을 참조하십시오.

예를 들어, 다음 역할 신뢰 정책 (p. 177)은 `test-session-tags` 사용자가 정책이 연결된 역할을 맡을 수 있도록 허용합니다. 해당 사용자가 역할을 맡는 경우 AWS CLI 또는 AWS API를 사용하여 세 개의 필수 세션 태그와 필수 외부 ID (p. 229)를 전달해야 합니다. 또한 사용자는 `Project` 및 `Department` 태그를 전이적으로 설정하도록 선택할 수 있습니다.

Example 세션 태그에 대한 역할 신뢰 정책

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

```
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {"AWS": "arn:aws:iam::123456789012:user/test-session-tags"},
            "Condition": {
              "StringLike": {
                    "aws:RequestTag/Project": "*",
                    "aws:RequestTag/CostCenter": "*",
                    "aws:RequestTag/Department": "*"
                },
                "StringEquals": {"sts:ExternalId": "Example987"}
            }
        },
        {
            "Sid": "AllowPassSessionTagsAndTransitive",
            "Effect": "Allow",
            "Action": "sts:TagSession",
            "Principal": {"AWS": "arn:aws:iam::123456789012:user/test-session-tags"},
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/Project": "*",
                    "aws:RequestTag/CostCenter": "*"
                },
                "StringEquals": {
                    "aws:RequestTag/Department": [
                        "Engineering",
                        "Marketing"
                    ]
                },
                "ForAllValues:StringEquals": {
                    "sts:TransitiveTagKeys": [
                        "Project",
                        "Department"
                    ]
                }
            }
        }
    ]
}
```

이 정책이 하는 일은 무엇입니까?

- `AllowIamUserAssumeRole` 문은 `test-session-tags` 사용자가 정책이 연결된 역할을 맡을 수 있도록 허용합니다. 해당 사용자가 역할을 맡을 때는 필수 세션 태그 및 외부 ID (p. 229)를 전달해야 합니다.
  - 이 문의 첫 번째 조건 블록의 경우 사용자가 `Project`, `CostCenter` 및 `Department` 세션 태그를 전달해야 합니다. 이 문에서 태그 값은 중요하지 않으므로 태그 값에 와일드카드(*)를 사용했습니다. 이 블록의 경우 사용자가 적어도 이 세 개의 세션 태그를 전달해야 하며, 그렇지 않으면 작업이 실패합니다. 사용자는 추가 태그를 전달할 수 있습니다.
  - 두 번째 조건 블록의 경우 사용자가 `Example987` 값의 외부 ID (p. 229)를 전달해야 합니다.
- `AllowPassSessionTagsAndTransitive` 문은 `sts:TagSession` 권한 전용 작업을 허용합니다. 이 작업을 허용해야 사용자가 세션 태그를 전달할 수 있습니다. 정책에 두 번째 문은 없고 첫 번째 문만 포함되어 있는 경우 사용자는 역할을 맡을 수 없습니다.
  - 이 문의 첫 번째 조건 블록은 사용자가 `CostCenter` 및 `Project` 세션 태그에 대한 값을 전달하도록 허용합니다. 정책의 태그 값에 와일드카드(*)를 사용하여 이 작업을 수행하려면 StringLike (p. 602) 조건 연산자를 사용해야 합니다.
  - 두 번째 조건 블록은 사용자가 `Department` 세션 태그의 `Engineering` 또는 `Marketing` 값만 전달하도록 허용합니다.
  - 세 번째 조건 블록은 전이적으로 설정할 수 있는 최대 태그 세트를 나열합니다. 사용자는 하위 세트를 설정하거나 태그를 전이적으로 설정하지 않도록 선택할 수 있습니다. 그러나 추가 태그를 전이적으로 설정할 수는 없습니다. `"Null":{"sts:TransitiveTagKeys":"false"}`를 포함하는 다른 조건 블록을 추가하여 태그 중 하나 이상을 전이적으로 설정하도록 요구할 수 있습니다.

AssumeRole을 사용하여 세션 태그 전달

`AssumeRole` 작업은 AWS 리소스에 액세스하는 데 사용할 수 있는 임시 자격 증명 세트를 반환합니다. IAM 사용자 또는 역할 자격 증명을 사용하여 `AssumeRole`을 호출할 수 있습니다. 역할을 맡는 동안 세션 태그를 전달하려면 `--tags` AWS CLI 옵션 또는 `Tags` AWS API 파라미터를 사용합니다.

태그를 전이적으로 설정하려면 `--transitive-tag-keys` AWS CLI 옵션 또는 `TransitiveTagKeys` AWS API 파라미터를 사용합니다. 전이적 태그는 역할 체인 동안 지속됩니다. 자세한 내용은 세션 태그를 사용하는 역할 체인 (p. 300) 단원을 참조하십시오.

다음 예제에서는 `AssumeRole`을 사용하는 샘플 요청을 보여 줍니다. 이 예제에서는 `my-role-example` 역할을 맡을 때 `my-session`이라는 세션을 생성합니다. 세션 태그 키-값 페어 `Project = Automation`, `CostCenter = 12345` 및 `Department = Engineering`을 추가합니다. 또한 해당 키를 지정하여 `Project` 및 `Department` 태그를 전이적으로 설정합니다.

Example AssumeRole CLI 요청

```
aws sts assume-role \
--role-arn arn:aws:iam::123456789012:role/my-role-example \
--role-session-name my-session \
--tags Key=Project,Value=Automation Key=CostCenter,Value=12345
 Key=Department,Value=Engineering \
--transitive-tag-keys Project Department \
--external-id Example987
```

AssumeRoleWithSAML을 사용하여 세션 태그 전달

`AssumeRoleWithSAML` 작업은 SAML 기반 연동을 사용하여 인증됩니다. 이 작업은 AWS 리소스에 액세스하는 데 사용할 수 있는 임시 자격 증명 세트를 반환합니다. AWS Management 콘솔 액세스를 위해 SAML 기반 연동을 사용하는 방법에 대한 자세한 내용은 SAML 2.0 연동 사용자가 AWS Management 콘솔에 액세스할 수 있게 하기 (p. 208) 단원을 참조하십시오. AWS CLI 또는 AWS API 액세스에 대한 자세한 내용은 SAML 2.0 기반 연동에 대하여 (p. 188) 단원을 참조하십시오. Active Directory 사용자를 위한 SAML 연동을 설정하는 방법에 대한 자습서는AWS 보안 블로그의 ADFS(Active Directory 연동 서비스)를 사용한 AWS 연동 인증을 참조하십시오.

관리자는 회사 디렉터리의 멤버가 AWS STS `AssumeRoleWithSAML` 작업을 사용하여 AWS로 연동하도록 허용할 수 있습니다. 이렇게 하려면 다음 작업을 완료해야 합니다.

1. AWS에 대한 SAML 공급자로 네트워크 구성 (p. 201)
2. IAM에서 SAML 공급자 생성 (p. 198)
3. 연동 사용자를 위해 AWS에서 역할 및 해당 권한 구성 (p. 244)
4. SAML IdP 구성을 완료하고 SAML 인증 응답에 대한 어설션 생성하기 (p. 203)

AWS에는 자격 증명 솔루션으로 세션 태그에 대한 엔드 투 엔드 환경을 인증한 파트너가 포함되어 있습니다. 이러한 자격 증명 공급자를 사용하여 세션 태그를 구성하는 방법은 타사 SAML 솔루션 공급자를 AWS와 통합 (p. 201) 단원을 참조하십시오.

SAML 속성을 세션 태그로 전달하려면 `Name` 속성이 `https://aws.amazon.com/SAML/Attributes/PrincipalTag:`*`{TagKey}`*로 설정된 `Attribute` 요소를 포함합니다. `AttributeValue` 요소를 사용하여 태그 값을 지정합니다. 각 세션 태그마다 별도의 `Attribute` 요소를 포함합니다.

예를 들어, 다음 자격 증명 속성을 세션 태그로 전달한다고 가정합니다.

- `Project:Automation`
- `CostCenter:12345`
- `Department:Engineering`

이러한 속성을 전달하려면 SAML 어설션에 다음 요소를 포함합니다.

Example SAML 어설션의 코드 조각

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:Project">
  <AttributeValue>Automation</AttributeValue>
</Attribute>
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:CostCenter">
  <AttributeValue>12345</AttributeValue>
</Attribute>
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:Department">
  <AttributeValue>Engineering</AttributeValue>
</Attribute>
```

위의 태그를 전이적으로 설정하려면 `Name` 속성이 `https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys`로 설정된 다른 `Attribute` 요소를 포함합니다. 전이적 태그는 역할 체인 동안 지속됩니다. 자세한 내용은 세션 태그를 사용하는 역할 체인 (p. 300) 단원을 참조하십시오.

`Project` 및 `Department` 태그를 전이적으로 설정하려면 다음과 같은 다중 값 속성을 사용합니다.

Example SAML 어설션의 코드 조각

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>Project</AttributeValue>
  <AttributeValue>Department</AttributeValue>
</Attribute>
```

AssumeRoleWithWebIdentity를 사용하여 세션 태그 전달

`AssumeRoleWithWebIdentity` 작업은 OIDC(OpenID Connect) 호환 웹 자격 증명 연동을 사용하여 인증됩니다. 이 작업은 AWS 리소스에 액세스하는 데 사용할 수 있는 임시 자격 증명 세트를 반환합니다. AWS Management 콘솔 액세스를 위해 웹 자격 증명 연동을 사용하는 방법에 대한 자세한 내용은 웹 자격 증명 연동에 대하여 (p. 183) 단원을 참조하십시오.

OIDC(OpenID Connect)에서 세션 태그를 전달하려면 JWT(JSON 웹 토큰)에 세션 태그를 포함해야 합니다. `AssumeRoleWithWebIdentity` 요청을 제출할 때 토큰의 `https://aws.amazon.com/tags` 네임스페이스에 세션 태그를 포함합니다. OIDC 토큰 및 클레임에 대한 자세한 내용은 Amazon Cognito 개발자 안내서의 사용자 풀과 함께 토큰 사용을 참조하십시오.

예를 들어, 다음의 디코딩된 JWT는 `Project`, `CostCenter` 및 `Department` 세션 태그를 사용하여 `AssumeRoleWithWebIdentity`를 호출하는 데 사용되는 토큰입니다. 또한 토큰은 `Project` 및 `CostCenter` 태그를 전이적으로 설정합니다. 전이적 태그는 역할 체인 동안 지속됩니다. 자세한 내용은 세션 태그를 사용하는 역할 체인 (p. 300) 단원을 참조하십시오.

Example 디코딩된 JSON 웹 토큰

```
{
    "sub": "johndoe",
    "aud": "ac_oic_client",
    "jti": "ZYUCeRMQVtqHypVPWAN3VB",
    "iss": "https://xyz.com",
    "iat": 1566583294,
    "exp": 1566583354,
    "auth_time": 1566583292,
    "https://aws.amazon.com/tags": {
        "principal_tags": {
            "Project": ["Automation"],
            "CostCenter": ["987654"],
            "Department": ["Engineering"]
        },
```

```
        "transitive_tag_keys": [
            "Project",
            "CostCenter"
        ]
    }
}
```

GetFederationToken을 사용하여 세션 태그 전달

`GetFederationToken`을 사용하면 사용자를 연동할 수 있습니다. 이 작업은 AWS 리소스에 액세스하는 데 사용할 수 있는 임시 자격 증명 세트를 반환합니다. 연동 사용자 세션에 태그를 추가하려면 `--tags` AWS CLI 옵션 또는 `Tags` AWS API 파라미터를 사용합니다. `GetFederationToken`을 사용할 경우 세션 태그를 전이적으로 설정할 수 없습니다. 이는 임시 자격 증명을 사용하여 역할을 맡을 수 없기 때문입니다. 즉, 역할 체인이 불가능합니다.

다음 예제에서는 `GetFederationToken`을 사용하는 샘플 요청을 보여 줍니다. 이 예제에서는 토큰을 요청할 때 `my-fed-user`라는 세션을 생성합니다. 세션 태그 키-값 페어 `Project = Automation` 및 `Department = Engineering`을 추가합니다.

Example GetFederationToken CLI 요청

```
aws sts get-federation-token \
--name my-fed-user \
--tags key=Project,value=Automation key=Department,value=Engineering
```

`GetFederationToken` 작업에서 반환되는 임시 자격 증명을 사용하는 경우 세션의 보안 주체 태그에 사용자의 태그와 전달된 세션 태그가 포함됩니다.

세션 태그를 사용하는 역할 체인

한 역할을 맡은 다음 임시 자격 증명을 사용하여 다른 역할을 맡을 수 있습니다. 이러한 작업을 세션 간에 계속할 수 있습니다. 이를 역할 체인 (p. 176)이라고 합니다. 역할을 맡는 동안 세션 태그를 전달하면 키를 전이적으로 설정할 수 있습니다. 이렇게 하면 해당 세션 태그가 역할 체인의 후속 세션에 전달됩니다. 역할 태그를 전이적으로 설정할 수 없습니다. 이러한 태그를 후속 세션에 전달하려면 세션 태그로 지정합니다.

다음 예제를 통해 세션 태그, 전이적 태그 및 역할 태그가 역할 체인의 후속 세션에 전달되는 방식을 이해할 수 있습니다.

다음 역할 체인 시나리오 예제에서는 AWS CLI에서 IAM 사용자의 액세스 키를 사용하여 `Role1`이라는 역할을 맡습니다. 그런 다음 결과 세션 자격 증명을 사용하여 `Role2`라는 두 번째 역할을 맡습니다. 그런 다음 두 번째 세션 자격 증명을 사용하여 `Role3`라는 세 번째 역할을 맡을 수 있습니다. 이러한 요청은 세 가지 개별 작업으로 발생합니다. IAM에서는 각 역할에 이미 태그가 지정되어 있습니다. 그리고 각 요청 중에 추가 세션 태그를 전달합니다.

역할을 체인할 때 이전 세션의 태그가 이후 세션에서도 유지되도록 할 수 있습니다. `assume-role` CLI 명령을 사용하여 이 작업을 수행하려면 태그를 세션 태그로 전달하고 태그를 전이적으로 설정해야 합니다. 태그 `Star = 1`을 세션 태그로 전달합니다. 태그 `Heart = 1`은 역할에 연결되어 있으며 세션을 사용할 때 보안 주체 태그로 적용됩니다. 그러나 `Heart = 1` 태그가 두 번째 또는 세 번째 세션에 자동으로 전달되도록 할 수도 있습니다. 이를 수행하려면 수동으로 세션 태그로 포함합니다. 그렇게 하면 결과 세션의 보안 주체 태그가 이 두 태그를 포함하며 전이적으로 설정됩니다.

다음 AWS CLI 명령을 사용하여 이 요청을 수행합니다.

Example AssumeRole CLI 요청

```
aws sts assume-role \
--role-arn arn:aws:iam::123456789012:role/Role1 \
--role-session-name Session1 \
--tags Key=Star,Value=1 Key=Heart,Value=1 \
```

```
--transitive-tag-keys Star Heart
```

그런 다음 해당 세션에 대한 자격 증명을 사용하여 `Role2`를 맡습니다. 태그 `Sun = 2`는 두 번째 역할에 연결되며 두 번째 세션을 사용할 때 보안 주체 태그로 적용됩니다. `Heart` 및 `Star` 태그는 첫 번째 세션의 전이적 세션 태그에서 상속됩니다. 두 번째 세션의 결과 보안 주체 태그는 `Heart = 1`, `Star = 1` 및 `Sun = 2`입니다. `Heart` 및 `Star`는 계속 전이적으로 유지됩니다. `Role2`에 연결된 `Sun` 태그는 세션 태그가 아니므로 전이적으로 표시되지 않습니다. 이 태그는 향후 세션에 상속되지 않습니다.

다음 AWS CLI 명령을 사용하여 이 두 번째 요청을 수행합니다.

Example AssumeRole CLI 요청

```
aws sts assume-role \
--role-arn arn:aws:iam::123456789012:role/Role2 \
--role-session-name Session2
```

그런 다음 두 번째 세션 자격 증명을 사용하여 `Role3`를 맡습니다. 세 번째 세션의 보안 주체 태그는 새 세션 태그, 상속된 전이적 세션 태그 및 역할 태그에서 가져옵니다. 두 번째 세션의 `Heart = 1` 및 `Star = 1` 태그는 첫 번째 세션의 전이적 세션 태그에서 상속되었습니다. `Heart = 3` 세션 태그를 전달하려고 하면 작업이 실패합니다. 상속된 `Star = 1` 세션 태그는 역할의 `Star = 3` 태그를 재정의합니다. 역할의 `Lightning` 태그는 세 번째 세션에도 적용되며 전이적으로 설정되지 않습니다.

다음 AWS CLI 명령을 사용하여 세 번째 요청을 수행합니다.

Example AssumeRole CLI 요청

```
aws sts assume-role \
--role-arn arn:aws:iam::123456789012:role/Role3 \
--role-session-name Session3
```

ABAC에 세션 태그 사용

ABAC(속성 기반 액세스 제어)는 태그 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다.

회사에서 회사 사용자 자격 증명에 대해 SAML 기반 자격 증명 공급자(IdP)를 사용하는 경우 세션 태그를 AWS에 전달하도록 SAML 어설션을 구성할 수 있습니다. 직원이 AWS에 연동되면 해당 속성이 AWS의 결과 보안 주체에 적용됩니다. 그런 다음 ABAC를 사용하여 이러한 속성에 따라 권한을 허용하거나 거부할 수 있습니다. 세부 정보는 ABAC에 SAML 세션 태그 사용 (p. 53) 단원을 참조하십시오.

CloudTrail에서 세션 태그 보기

AWS CloudTrail를 사용하여 역할을 맡거나 사용자를 연동하기 위한 요청을 볼 수 있습니다. CloudTrail 로그 파일에는 맡은 역할 또는 연동 사용자 세션의 보안 주체 태그에 대한 정보가 포함됩니다. 자세한 내용은 AWS CloudTrail을 사용하여 IAM 및 AWS STS API 호출 로깅 (p. 334) 단원을 참조하십시오.

예를 들어, AWS STS `AssumeRoleWithSAML` 요청을 하고 세션 태그를 전달하고 해당 태그를 전이적으로 설정한다고 가정합니다. CloudTrail 로그에서 다음 정보를 찾을 수 있습니다.

Example AssumeRoleWithSAML CloudTrail 로그

```
    "requestParameters": {
        "sAMLAssertionID": "_c0046cEXAMPLEb9d4b8eEXAMPLE2619aEXAMPLE",
        "roleSessionName": "MyRoleSessionName",
        "principalTags": {
            "CostCenter": "987654",
            "Project": "Unicorn"
        },
        "transitiveTagKeys": [
            "CostCenter",
```

```
            "Project"
        ],
        "durationSeconds": 3600,
        "roleArn": "arn:aws:iam::123456789012:role/SAMLTestRoleShibboleth",
        "principalArn": "arn:aws:iam::123456789012:saml-provider/Shibboleth"
    },
```

다음 CloudTrail 로그 예제에서 세션 태그를 사용하는 이벤트를 볼 수 있습니다.

- CloudTrail 로그 파일의 AWS STS 역할 체인 API 이벤트 예제 (p. 341)
- CloudTrail 로그 파일의 SAML AWS STS API 이벤트 예제 (p. 343)
- CloudTrail 로그 파일의 웹 자격 증명 AWS STS API 이벤트 예제 (p. 344)

임시 보안 자격 증명

AWS Security Token Service(AWS STS)를 사용하면 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 자격 증명을 생성하여 신뢰받는 사용자에게 제공할 수 있습니다. 임시 보안 자격 증명은 다음과 같은 차이점을 제외하고는 IAM 사용자가 사용할 수 있는 장기 액세스 키 자격 증명과 거의 동일한 효력을 지닙니다.

- 임시 보안 자격 증명은 그 이름이 암시하듯 단기적입니다. 이 자격 증명은 몇 분에서 몇 시간까지 지속되도록 구성할 수 있습니다. 자격 증명이 만료된 후 AWS는 더는 그 자격 증명을 인식하지 못하거나 그 자격 증명을 사용한 API 요청으로부터 이루어지는 어떤 종류의 액세스도 허용하지 않습니다.
- 임시 보안 자격 증명은 사용자와 함께 저장되지 않지만 동적으로 생성되어 요청시 사용자에게 제공됩니다. 임시 보안 자격 증명이 만료되었을 때(심지어는 만료 전이라도) 사용자는 새 자격 증명을 요청할 수 있습니다. 단, 자격 증명을 요청하는 해당 사용자에게 그렇게 할 수 있는 권한이 있어야 합니다.

이러한 차이점은 다음과 같은 임시 자격 증명 사용의 이점을 발생시킬 수 있습니다.

- 애플리케이션으로 장기 AWS 보안 자격 증명을 배포 또는 포함할 필요가 없습니다.
- 사용자에 대한 AWS 자격 증명을 정의하지 않고도 AWS 리소스에 대한 액세스 권한을 사용자에게 제공할 수 있습니다. 임시 자격 증명은 역할 및 자격 증명 연동 (p. 174)을 위한 기초입니다.
- 임시 보안 자격 증명은 수명이 제한되어 있어서, 더 이상 필요하지 않을 때 교체하거나 명시적으로 취소할 필요가 없습니다. 임시 보안 자격 증명이 만료된 후에는 다시 사용할 수 없습니다. 그 자격 증명에 대해 유효 기간을 최대 한계까지 지정할 수 있습니다.

AWS STS 및 AWS 리전

임시 보안 자격 증명은 AWS STS에 의해 생성됩니다. 기본적으로 AWS STS는 `https://sts.amazonaws.com`에 단일 엔드포인트가 있는 전역적 서비스입니다. 그러나 지원되는 기타 다른 리전에서 엔드포인트에 대한 AWS STS API 호출을 할 수도 있습니다. 이렇게 지리적으로 더 가까운 리전에 있는 서버로 요청을 전송함으로써 지연 시간(서버 랙)을 단축할 수 있습니다. 자격 증명은 어떤 리전에서 오는지 상관없이 전역적으로 유효합니다. 자세한 내용은 AWS 리전에서 AWS STS 관리 (p. 326) 단원을 참조하십시오.

임시 자격 증명과 관련된 일반적인 시나리오

임시 자격 증명은 자격 증명 연동, 위임, 교차 계정 액세스, IAM 역할 등의 시나리오에서 유용합니다.

ID 페더레이션

AWS 밖의 외부 시스템에서 사용자 자격 증명을 관리할 수 있고 그 시스템으로부터 로그인하는 사용자에게 액세스 권한을 부여하여 AWS 작업을 수행하고 AWS 리소스에 액세스하도록 할 수 있습니다. IAM은 두 가지 유형의 자격 증명 연동을 지원합니다. 두 경우 모두 자격 증명은 AWS 외부에 저장됩니다. 차이는 외부 시스

템이 상주하는 곳이 어디인가 즉, 데이터센터인가 아니면 웹 상의 외부 타사인가 하는 데 있습니다. 외부 자격 증명 공급자에 대한 자세한 내용은 자격 증명 공급자 및 연동 (p. 183) 단원을 참조하십시오.

- 엔터프라이즈 자격 증명 연동 – 조직의 네트워크에서 사용자를 인증한 다음, 해당 사용자에 대한 새로운 AWS 자격 증명을 생성하지 않고 또한, 사용자에게 별도의 사용자 이름 및 암호로 로그인하도록 요구하지 않고도 AWS에 대한 액세스 권한을 사용자에게 제공할 수 있습니다. 이는 임시 액세스 권한에 대한 SSO(Single Sign-On) 접근 방식으로 알려져 있습니다. AWS STS는 SAML 2.0(Security Assertion Markup Language 2.0)과 같은 개방형 표준을 지원합니다. 이를 통해 Microsoft AD FS를 사용해 Microsoft Active Directory를 최대한 활용할 수 있습니다. 또한, SAML 2.0을 사용해 사용자 자격 증명 연동을 위한 자신만의 솔루션을 관리할 수 있습니다. 자세한 내용은 SAML 2.0 기반 연동에 대하여 (p. 188)을 참조하십시오.
  - 사용자 지정 연동 브로커 – 조직의 인증 시스템을 사용해 AWS 리소스에 대한 액세스 권한을 부여할 수 있습니다. 시나리오 예시는 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.
  - SAML 2.0을 사용한 연동 – 조직의 인증 시스템과 SAML을 사용해 AWS 리소스에 대한 액세스를 허용할 수 있습니다. 자세한 내용과 시나리오 예시는 SAML 2.0 기반 연동에 대하여 (p. 188) 단원을 참조하십시오.
- 웹 자격 증명 연동 – Login with Amazon, Facebook, Google 또는 OpenID Connect(OIDC) 2.0 호환 공급자와 같은 유명한 타사 자격 증명 공급자를 사용해 사용자가 로그인할 수 있습니다. 그 공급자로부터 얻은 자격 증명을 AWS 계정 리소스 사용 권한과 교환할 수 있습니다. 이는 임시 액세스 권한에 대한 웹 자격 증명 연동 접근 방식으로 알려져 있습니다. 모바일 또는 웹 애플리케이션을 위해 웹 자격 증명 연동을 사용하면 사용자 지정 로그인 코드를 생성하거나 자신의 사용자 자격 증명을 관리할 필요가 없습니다. 웹 자격 증명 연동을 사용하면 AWS 계정을 안전하게 보호할 수 있다는 이점이 있습니다. 애플리케이션으로 IAM 사용자 액세스 키 같은 장기 보안 자격 증명을 배포할 필요가 없기 때문입니다. 자세한 내용은 웹 자격 증명 연동에 대하여 (p. 183)을 참조하십시오.

  AWS STS 웹 자격 증명 연동은 Login with Amazon, Facebook, Google 및 모든 OpenID Connect(OIDC) 호환 자격 증명 공급자를 지원합니다.

  > **Note**
  >
  > 모바일 애플리케이션의 경우 Amazon Cognito 사용을 권장합니다. 이 서비스와 함께 AWS iOS용 Mobile SDK, AWS Android 및 Fire OS용 Mobile SDK를 사용하여 사용자 고유 자격 증명을 만들고 AWS 리소스에 대한 보안 액세스를 인증할 수 있습니다. Amazon Cognito는 AWS STS와 동일한 자격 증명 제공자를 지원하며 인증되지 않은(게스트) 액세스도 지원하고 로그인하면 사용자 데이터를 마이그레이션할 수 있습니다. Amazon Cognito는 디바이스를 바꿔 가며 이용해도 데이터를 보존하도록 사용자 데이터 동기화를 위한 API 작업도 제공합니다. 자세한 내용은 다음 자료를 참조하십시오.
  >
  > - AWS iOS용 Mobile SDK 개발자 안내서의 Amazon Cognito 자격 증명
  > - AWS Android용 Mobile SDK 개발자 안내서의 Amazon Cognito 자격 증명

교차 계정 액세스를 위한 역할

많은 조직이 1개 이상의 AWS 계정을 유지합니다. 역할 및 교차 계정 액세스를 사용하면 하나의 계정에서 사용자 자격 증명을 정의하고 그 자격 증명을 사용해 조직에 속한 다른 계정의 AWS 리소스에 액세스할 수 있습니다. 이는 임시 액세스 권한에 대한 위임 접근 방식으로 알려져 있습니다. 교차 계정 역할 생성에 대한 자세한 내용은 역할을 만들어 IAM 사용자에게 권한 위임 (p. 226) 단원을 참조하십시오. 해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

Amazon EC2의 역할

Amazon EC2 인스턴스에서 애플리케이션을 실행할 때 그 애플리케이션이 AWS 리소스에 대한 액세스 권한이 필요한 경우 인스턴스 시작 시 인스턴스에 대한 임시 보안 자격 증명을 제공할 수 있습니다. 이 임시 보안 자격 증명은 인스턴스에서 실행되는 모든 애플리케이션에서 사용 가능하므로 그 인스턴스에 어떤 장기 자격 증명도 저장할 필요가 없습니다. 자세한 내용은 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265)를 참조하십시오.

기타 AWS 서비스

임시 보안 자격 증명을 사용해 대부분의 AWS 서비스에 액세스할 수 있습니다. 임시 보안 자격 증명을 수락하는 서비스의 목록은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

임시 보안 자격 증명 요청하기

임시 보안 자격 증명을 요청하려면 AWS API에서 AWS Security Token Service(AWS STS) 작업을 사용할 수 있습니다. 이러한 작업에는 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 자격 증명을 생성하여 신뢰할 수 있는 사용자에게 제공할 수 있습니다. AWS STS에 대한 자세한 내용은 임시 보안 자격 증명 (p. 302) 단원을 참조하십시오. 역할을 수임해 임시 보안 자격 증명을 요청하는 데 사용할 수 있는 여러 방법을 알아보려면 IAM 역할 사용 (p. 250) 단원을 참조하십시오.

API 작업을 호출하려면 AWS SDK 중 하나를 사용할 수 있습니다. SDK는 Java, .NET, Python, Ruby, Android 및 iOS 등 다양한 프로그래밍 언어 및 환경에서 사용할 수 있습니다. SDK는 요청에 암호화 방식으로 서명, 필요한 경우 요청 재시도, 오류 응답 처리와 같은 작업들을 다룹니다. AWS Security Token Service API Reference에 기술된 AWS STS 쿼리 API를 사용할 수도 있습니다. 끝으로 AWS Command Line Interface 및 Windows PowerShell용 AWS 도구라는 두 가지 명령줄 도구가 AWS STS 명령을 지원합니다.

AWS STS API 작업은 액세스 키 페어 및 세션 토큰을 포함하는 임시 보안 자격 증명을 사용하여 새 세션을 생성합니다. 액세스 키 페어는 액세스 키 ID와 보안 키로 구성되어 있습니다. 사용자(또는 사용자가 실행하는 애플리케이션)는 이 자격 증명을 사용해 리소스에 액세스할 수 있습니다. AWS STS API 작업을 사용하여 프로그래밍 방식으로 역할 세션을 생성하고 세션 정책 및 세션 태그를 전달할 수 있습니다. 결과적으로 얻는 세션의 권한은 역할의 자격 증명 기반 정책의 교차와 세션 정책입니다. 세션 정책에 대한 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오. 세션 태그에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

> **Note**
>
> AWS STS API 작업이 반환하는 보안 토큰의 크기는 고정적이지 않습니다. 따라서 최대 크기를 가정하지 않는 것이 좋습니다. 일반적인 토큰 크기는 4096바이트 미만이나 경우에 따라 다를 수 있습니다.

AWS 리전에서 AWS STS 사용하기

전역 엔드포인트 또는 리전 엔드포인트 중 하나에 AWS STS API 호출을 전송할 수 있습니다. 더 가까이 있는 엔드포인트를 선택하면 지연 시간을 단축해 API 호출의 성능을 향상시킬 수 있습니다. 또한 원래 엔드포인트와 더 이상 통신하지 할 수 없는 경우 대체 리전 엔드포인트에 호출을 직접 보내는 방법을 선택할 수 있습니다. 다양한 AWS SDK 중 하나를 사용하고 있다면 API 호출 전에 그 SDK의 메서드를 사용해 리전을 선택하십시오. HTTP API 요청을 수동으로 구축하는 경우 그 요청을 정확한 엔드포인트에 직접 전송해야 합니다. 자세한 정보는 리전 및 엔드포인트의 AWS STS 섹션 및 AWS 리전에서 AWS STS 관리 (p. 326) 단원을 참조하십시오.

다음은 AWS 환경 및 애플리케이션에서 사용할 임시 자격 증명을 획득하는 데 사용할 수 있는 API 작업입니다.

AssumeRole—사용자 지정 자격 증명 브로커를 통한 교차 계정 위임과 연동

`AssumeRole` API 작업은 기존 IAM 사용자가 아직 액세스 권한이 없는 AWS 리소스에 액세스할 수 있도록 허용하는 데 유용합니다. 예를 들어 사용자가 다른 AWS 계정의 리소스에 액세스해야 할 수 있습니다. 또한, 기존 사용자에게는 임시로 액세스 특권을 얻는 수단으로서 유용합니다. 예를 들면 멀티 팩터 인증(MFA)을 제공할 수 있습니다. 기존 IAM 사용자 자격 증명을 사용해 이 API를 호출해야 합니다. 자세한 정보는 역할을 만들어 IAM 사용자에게 권한 위임 (p. 226) 및 MFA 보호 API 액세스 구성 (p. 146)을(를) 참조하십시오.

이 호출에는 반드시 유효한 AWS 보안 자격 증명을 사용해야 합니다. 이 호출을 할 때 다음과 같은 정보를 전달하게 됩니다.

- 앱이 수임해야 하는 역할의 Amazon 리소스 이름(ARN)
- (선택 사항) 기간. 임시 보안 자격 증명의 기간을 지정합니다. `DurationSeconds` 파라미터를 사용하여 역할 세션 기간을 900초(15초)에서 해당 역할에 대한 최대 세션 기간 설정까지 지정합니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오. 이 파라미터를 전달하지 않으면 임시 자격 증명이 한 시간 내에 만료됩니다. 이 API의 `DurationSeconds` 파라미터는 콘솔 세션의 기간을 지정하는 데 사용하는 `SessionDuration` HTTP 파라미터와 다릅니다. 콘솔 로그인 토큰의 연동 엔드포인트에 대한 요청에는 `SessionDuration` HTTP 파라미터를 사용하십시오. 자세한 정보는 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.
- (선택 사항) 역할 세션 이름. 세션을 식별하는 데 사용할 수 있는 문자열 값입니다. 이 값은 CloudTrail가 캡처하고 로깅하여, 감사하는 동안 역할 사용자들을 구분하는 데 도움이 될 수 있습니다.
- (선택 사항) 인라인 또는 관리형 세션 정책. 이러한 정책은 역할 세션에 할당된 역할 자격 증명 기반 정책의 권한을 제한합니다. 결과적으로 얻는 세션의 권한은 역할의 자격 증명 기반 정책의 교차와 세션 정책입니다. 세션 정책을 사용하여 수임된 역할의 자격 증명 기반 정책에서 허용되는 것보다 더 많은 권한을 부여할 수는 없습니다. 역할 세션 권한에 대한 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오.
- (선택 사항) 세션 태그. 역할을 맡은 다음 임시 자격 증명을 사용하여 요청할 수 있습니다. 이렇게 하면 세션의 보안 주체 태그에 역할의 태그와 전달된 세션 태그가 포함됩니다. 임시 자격 증명을 사용하여 이렇게 호출하는 경우 새 세션은 호출 세션의 전이적 세션 태그도 상속합니다. 세션 태그에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.
- (선택 사항) MFA 정보. MFA(멀티 팩터 인증)를 사용하도록 구성한 경우, MFA 디바이스의 식별자와 해당 디바이스에서 제공한 일회용 코드를 포함시켜야 합니다.
- (선택 사항) 계정에 대한 액세스 권한을 타사에 위임할 때 사용할 수 있는 `ExternalId` 값입니다. 이 값은 지정된 타사만 역할에 액세스할 수 있도록 하는 데 도움이 됩니다. 자세한 내용은 AWS 리소스에 대한 액세스를 타사에 부여할 때 외부 ID를 사용하는 방법 (p. 229) 단원을 참조하십시오.

다음 예제에서는 `AssumeRole`을 사용한 샘플 요청 및 응답을 보여줍니다. 이 요청 예제에서는 포함된 세션 정책 (p. 351), 세션 태그 (p. 294) 및 외부 ID (p. 229)를 사용하여 지정된 기간 동안 `demo` 역할을 맡습니다. 결과 세션의 이름이 `John-session`으로 지정됩니다.

Example 요청

```
https://sts.amazonaws.com/
?Version=2011-06-15
&Action=AssumeRole
&RoleSessionName=John-session
&RoleArn=arn:aws::iam::123456789012:role/demo
&Policy=%7B%22Version%22%3A%222012-10-17%22%2C%22Statement%22%3A%5B%7B%22Sid%22%3A
%20%22Stmt1%22%2C%22Effect%22%3A%20%22Allow%22%2C%22Action%22%3A%20%22s3%3A*%22%2C
%22Resource%22%3A%20%22*%22%7D%5D%7D
&DurationSeconds=1800
&Tags.member.1.Key=Project
&Tags.member.1.Value=Pegasus
&Tags.member.2.Key=Cost-Center
&Tags.member.2.Value=12345
&ExternalId=123ABC
&AUTHPARAMS
```

이전 예제의 정책 값은 다음 정책을 URL로 인코딩한 버전입니다.

```
{"Version":"2012-10-17","Statement":
[{"Sid":"Stmt1","Effect":"Allow","Action":"s3:*","Resource":"*"}]}
```

예시의 `AUTHPARAMS` 파라미터는 서명에 대한 자리 표시자입니다. 서명은 AWS HTTP API 요청에 포함해야 하는 인증 정보입니다. AWS SDK를 사용하여 API 요청을 생성하는 것이 좋습니다. 이렇게 하면 SDK가 요청 서명을 대신 처리한다는 장점이 있습니다. API 요청을 직접 생성하여 서명해야 할 경우 Amazon Web Services 일반 참조의 서명 버전 4를 사용하여 AWS 요청에 서명에서 요청에 서명하는 방법 단원을 참조하십시오.

그 응답에는 임시 보안 자격 증명뿐만 아니라 연동 사용자 및 자격 증명 만료 시간에 대한 Amazon 리소스 이름(ARN)이 포함되어 있습니다.

Example 응답

```
<AssumeRoleResponse xmlns="https://sts.amazonaws.com/doc/2011-06-15/">
<AssumeRoleResult>
<Credentials>
  <SessionToken>
   AQoDYXdzEPT//////////wEXAMPLEtc764bNrC9SAPBSM22wDOk4x4HIZ8j4FZTwdQW
   LWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7mSEI/qkPpKPi/kMcGd
   QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
   9HFvlRd8Tx6q6fE8YQcHNVXAkiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
   +scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCR/oLxBA==
  </SessionToken>
  <SecretAccessKey>
   wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY
  </SecretAccessKey>
  <Expiration>2019-07-15T23:28:33.359Z</Expiration>
  <AccessKeyId>AKIAIOSFODNN7EXAMPLE</AccessKeyId>
</Credentials>
<AssumedRoleUser>
  <Arn>arn:aws:sts::123456789012:assumed-role/demo/John</Arn>
  <AssumedRoleId>ARO123EXAMPLE123:John</AssumedRoleId>
</AssumedRoleUser>
<PackedPolicySize>8</PackedPolicySize>
</AssumeRoleResult>
<ResponseMetadata>
<RequestId>c6104cbe-af31-11e0-8154-cbc7ccf896c7</RequestId>
</ResponseMetadata>
</AssumeRoleResponse>
```

> **Note**
>
> AWS 변환은 전달된 세션 정책과 세션 태그를 별도의 제한이 있는 압축된 이진 형식으로 압축합니다. 일반 텍스트가 다른 요구 사항을 충족하는 경우에도 이 제한으로 인해 요청이 실패할 수 있습니다. `PackedPolicySize` 응답 요소는 요청에 대한 정책 및 태그가 상위 크기 제한과 얼마나 가까운지를 백분율로 나타냅니다.

AssumeRoleWithWebIdentity—웹 기반 자격 증명 공급자를 통한 연동

`AssumeRoleWithWebIdentity` API 작업은 퍼블릭 자격 증명 공급자를 통해 인증된 연합된 사용자의 임시 보안 자격 증명 세트를 반환합니다. 퍼블릭 자격 증명 공급자의 예에는 Login with Amazon, Facebook, Google 또는 OpenID Connect(OIDC) 호환 자격 증명 공급자 등이 있습니다. 이 작업은 AWS에 대한 액세스가 필요한 모바일 애플리케이션 또는 클라이언트 기반 애플리케이션을 생성하는 데 유용합니다. 이 작업을 사용하는 경우 사용자가 자체 AWS 또는 IAM 자격 증명을 필요로 하지 않습니다. 자세한 정보는 웹 자격 증명 연동에 대하여 (p. 183) 단원을 참조하십시오.

`AssumeRoleWithWebIdentity`를 직접 호출하는 대신 모바일 개발을 위한 AWS SDK에서 Amazon Cognito 및 Amazon Cognito 자격 증명 공급자를 사용할 것을 권장합니다. 자세한 내용은 다음 자료를 참조하십시오.

- Android용 AWS Mobile SDK Developer Guide의 Amazon Cognito 자격 증명
- AWS Mobile SDK for iOS Developer Guide의 Amazon Cognito 자격 증명

Amazon Cognito를 사용하고 있지 않다면 AWS STS의 `AssumeRoleWithWebIdentity` 작업을 호출합니다. 이것은 서명되지 않은 호출로서 앱이 이 호출을 하기 위해 어떤 AWS 보안 자격 증명에도 액세스할 필요가 없음을 뜻합니다. 이 호출을 할 때 다음과 같은 정보를 전달하게 됩니다.

- 앱이 수임해야 하는 역할의 Amazon 리소스 이름(ARN) 앱이 사용자가 로그인하는 여러 가지 방식을 지원하는 경우 다양한 역할, 즉 자격 증명 공급자당 하나의 역할을 정의해야 합니다. `AssumeRoleWithWebIdentity`에 대한 호출에는 사용자가 로그인할 때 사용한 공급자에 특정된 역할의 ARN이 포함되어야 합니다.
- 앱이 사용자를 인증한 후에 IdP로부터 얻는 토큰
- 속성을 토큰에 세션 태그 (p. 294)로 전달하도록 IdP를 구성할 수 있습니다.
- (선택 사항) 기간. 임시 보안 자격 증명의 기간을 지정합니다. `DurationSeconds` 파라미터를 사용하여 역할 세션 기간을 900초(15초)에서 해당 역할에 대한 최대 세션 기간 설정까지 지정합니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오. 이 파라미터를 전달하지 않으면 임시 자격 증명이 한 시간 내에 만료됩니다. 이 API의 `DurationSeconds` 파라미터는 콘솔 세션의 기간을 지정하는 데 사용하는 `SessionDuration` HTTP 파라미터와 다릅니다. 콘솔 로그인 토큰의 연동 엔드포인트에 대한 요청에는 `SessionDuration` HTTP 파라미터를 사용하십시오. 자세한 정보는 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.
- (선택 사항) 역할 세션 이름. 세션을 식별하는 데 사용할 수 있는 문자열 값입니다. 이 값은 CloudTrail가 캡처하고 로깅하여, 감사하는 동안 역할 사용자들을 구분하는 데 도움이 될 수 있습니다.
- (선택 사항) 인라인 또는 관리형 세션 정책. 이러한 정책은 역할 세션에 할당된 역할 자격 증명 기반 정책의 권한을 제한합니다. 결과적으로 얻는 세션의 권한은 역할의 자격 증명 기반 정책의 교차와 세션 정책입니다. 세션 정책을 사용하여 수임된 역할의 자격 증명 기반 정책에서 허용되는 것보다 더 많은 권한을 부여할 수는 없습니다. 역할 세션 권한에 대한 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오.

  Note

  `AssumeRoleWithWebIdentity`에 대한 호출이 서명(암호화)되지 않았습니다. 따라서 요청이 신뢰할 수 있는 중개자를 통해 전송된 경우에만 선택적 세션 정책을 포함해야 합니다. 이러한 경우 누군가가 정책을 변경해 제한을 제거할 수 있습니다.

`AssumeRoleWithWebIdentity`를 호출하면 AWS가 토큰의 신뢰성을 확인합니다. 예를 들어 공급자에 따라 AWS는 해당 공급자를 호출해 앱이 전달한 토큰을 포함할 수 있습니다. 자격 증명 공급자가 토큰을 확인한다고 가정하면, AWS는 다음 정보를 반환합니다.

- 일련의 임시 보안 자격 증명 이러한 임시 보안 자격 증명은 액세스 키 ID, 보안 액세스 키 및 세션 토큰으로 이루어져 있습니다.
- 위임된 역할의 역할 ID 및 ARN
- 고유한 사용자 ID를 포함하는 `SubjectFromWebIdentityToken` 값

임시 보안 자격 증명이 있으면 AWS API 호출에 사용할 수 있습니다. 이는 장기 보안 자격 증명을 사용한 AWS API 호출과 동일한 프로세스입니다. 차이점은 AWS에서 임시 보안 자격 증명이 유효한지 확인하도록 하는 세션 토큰을 포함해야 한다는 점입니다.

앱은 자격 증명을 캐싱해야 합니다. 언급한 바와 같이, 자격 증명은 한 시간 후에 만료되도록 기본 설정되어 있습니다. AWS SDK의 AmazonSTSCredentialsProvider 작업을 사용하지 않은 경우 `AssumeRoleWithWebIdentity`를 직접 다시 호출해야 합니다. 이전 자격 증명이 만료되기 전에 이 작업을 호출하여 임시 보안 자격 증명 세트를 새로 받으십시오.

AssumeRoleWithSAML—SAML 2.0과 호환되는 엔터프라이즈 자격 증명 공급자를 통한 연동

`AssumeRoleWithSAML` API 작업은 조직의 기존 자격 증명 시스템을 통해 인증된 연합된 사용자의 임시 보안 자격 증명 세트를 반환합니다. 또한 사용자는 SAML 2.0(Security Assertion Markup Language)을 사용하여 AWS에 인증 및 권한 부여 정보를 전달해야 합니다. 이 API 작업은 자격 증명 시스템(예: Windows Active Directory 또는 OpenLDAP)을 SAML 어설션을 생성할 수 있는 소프트웨어와 통합한 조직에 유용합니다. 이러한 통합은 사용자 자격 증명 및 권한에 대한 정보를 제공합니다(예: Active Directory Federation Services 또는 Shibboleth). 자세한 정보는 SAML 2.0 기반 연동에 대하여 (p. 188) 단원을 참조하십시오.

이것은 서명되지 않은 호출로서 앱이 이 호출을 하기 위해 어떤 AWS 보안 자격 증명에도 액세스할 필요가 없음을 뜻합니다. 이 호출을 할 때 다음과 같은 정보를 전달하게 됩니다.

- 앱이 수임해야 하는 역할의 Amazon 리소스 이름(ARN)
- 자격 증명 공급자에 대해 기술하는 IAM에서 만든 SAML 자격 증명 공급자의 ARN
- 앱의 로그인 요청에 대한 인증 응답 시 SAML 자격 증명 공급자가 제공한 base-64 인코딩 SAML 어설션
- 속성을 SAML 어설션에 세션 태그 (p. 294)로 전달하도록 IdP를 구성할 수 있습니다.
- (선택 사항) 기간. 임시 보안 자격 증명의 기간을 지정합니다. `DurationSeconds` 파라미터를 사용하여 역할 세션 기간을 900초(15초)에서 해당 역할에 대한 최대 세션 기간 설정까지 지정합니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오. 이 파라미터를 전달하지 않으면 임시 자격 증명이 한 시간 내에 만료됩니다. 이 API의 `DurationSeconds` 파라미터는 콘솔 세션의 기간을 지정하는 데 사용하는 `SessionDuration` HTTP 파라미터와 다릅니다. 콘솔 로그인 토큰의 연동 엔드포인트에 대한 요청에는 `SessionDuration` HTTP 파라미터를 사용하십시오. 자세한 정보는 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.
- (선택 사항) 인라인 또는 관리형 세션 정책. 이러한 정책은 역할 세션에 할당된 역할 자격 증명 기반 정책의 권한을 제한합니다. 결과적으로 얻는 세션의 권한은 역할의 자격 증명 기반 정책의 교차와 세션 정책입니다. 세션 정책을 사용하여 수임된 역할의 자격 증명 기반 정책에서 허용되는 것보다 더 많은 권한을 부여할 수는 없습니다. 역할 세션 권한에 대한 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오.

`AssumeRoleWithSAML`을 호출하면 AWS가 SAML 어설션의 신뢰성을 확인합니다. 자격 증명 공급자가 어설션을 확인한다고 가정하면, AWS는 다음 정보를 반환합니다.

- 일련의 임시 보안 자격 증명 이러한 임시 보안 자격 증명은 액세스 키 ID, 보안 액세스 키 및 세션 토큰으로 이루어져 있습니다.
- 위임된 역할의 역할 ID 및 ARN
- SAML 어설션의 `Audience` 요소의 `Recipient` 속성 값을 포함하는 `SubjectConfirmationData` 값
- SAML 어설션의 `Issuer` 요소 값을 포함하는 `Issuer` 값
- `Issuer` 값, AWS 계정 ID, SAML 공급자의 표시 이름으로 구축된 해시 값을 포함하는 `NameQualifier` 요소 `Subject` 요소와 결합되면 연동 사용자를 고유한 이름으로 식별할 수 있습니다.
- SAML 어설션의 `Subject` 요소에 있는 `NameID` 요소의 값을 포함하는 `Subject` 요소
- `SubjectType` 요소의 형식을 나타내는 `Subject` 요소 그 값은 `persistent`, `transient`, 또는 SAML 어설션에서 사용되는 `Format` 및 `Subject` 요소의 전체 `NameID` URI일 수 있습니다. `NameID` 요소의 `Format` 속성에 대한 자세한 정보는 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오.

임시 보안 자격 증명이 있으면 AWS API 호출에 사용할 수 있습니다. 이는 장기 보안 자격 증명을 사용한 AWS API 호출과 동일한 프로세스입니다. 차이점은 AWS에서 임시 보안 자격 증명이 유효한지 확인하도록 하는 세션 토큰을 포함해야 한다는 점입니다.

앱은 자격 증명을 캐싱해야 합니다. 자격 증명은 한 시간 후에 만료되도록 기본 설정되어 있습니다. AWS SDK의 AmazonSTSCredentialsProvider 작업을 사용하지 않을 경우, `AssumeRoleWithSAML`를 직접 다시 호출해야 합니다. 이전 자격 증명이 만료되기 전에 이 작업을 호출하여 임시 보안 자격 증명 세트를 새로 받으십시오.

GetFederationToken—사용자 지정 자격 증명 브로커를 통한 연동

`GetFederationToken` API 작업은 연동 사용자에게 일련의 임시 보안 자격 증명을 반환합니다. 이 API는 기본 만료 기간이 상당히 길다는 점이(1시간이 아니라12시간) `AssumeRole`과 다릅니다. 또한 `DurationSeconds` 파라미터를 사용하여 임시 보안 자격 증명이 유효하게 남아 있을 기간을 지정할 수 있습니다. 결과물로 얻은 자격 증명은 900초(15분)~129,600초(36시간)로 지정된 기간 동안 유효합니다. 만료 기간이 더 길어지면 새 자격 증명을 자주 얻을 필요가 없기 때문에 AWS에 대한 호출 횟수가 줄어들 수 있습니다. 자세한 정보는 임시 보안 자격 증명 요청하기 (p. 304) 단원을 참조하십시오.

이 요청을 할 때 특정 IAM 사용자의 자격 증명을 사용합니다. 임시 보안 자격 증명에 대한 권한은 `GetFederationToken`을 호출할 때 전달하는 세션 정책에 의해 결정됩니다. 결과적으로 얻는 세션의 권한은 IAM 사용자 정책 또는 전달한 정책의 교집합입니다. 세션 정책을 사용하여 연동을 요청하는 IAM 사용자의 자격 증명 기반 정책에서 허용되는 권한을 부여할 수는 없습니다. 역할 세션 권한에 대한 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오.

`GetFederationToken` 작업에서 반환되는 임시 자격 증명을 사용하는 경우 세션의 보안 주체 태그에 사용자의 태그와 전달된 세션 태그가 포함됩니다. 세션 태그에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

`GetFederationToken` 호출은 보안 토큰, 액세스 키, 보안 키, 만료로 구성된 임시 보안 자격 증명을 반환합니다. 조직 내에서 권한을 관리하고 싶다면 `GetFederationToken`을 사용할 수 있습니다(예: 프록시 애플리케이션을 사용할 권한 할당). `GetFederationToken`을 사용하는 샘플 애플리케이션을 보려면 AWS 샘플 코드 및 라이브러리의 Active Directory 사용 시 자격 증명 연동 샘플 애플리케이션 단원을 참조하십시오.

다음 예에서는 `GetFederationToken`을 사용한 샘플 요청 및 응답을 보여줍니다. 이 요청 예제에서는 지정된 기간 동안 호출 사용자를 세션 정책 (p. 351) ARN 및 세션 태그 (p. 294)와 연동합니다. 결과 세션의 이름이 `Jane-session`으로 지정됩니다.

Example 요청

```
https://sts.amazonaws.com/
?Version=2011-06-15
&Action=GetFederationToken
&Name=Jane-session
&PolicyArns.member.1.arn==arn%3Aaws%3Aiam%3A%3A123456789012%3Apolicy%2FRole1policy
&DurationSeconds=1800
&Tags.member.1.Key=Project
&Tags.member.1.Value=Pegasus
&Tags.member.2.Key=Cost-Center
&Tags.member.2.Value=12345
&AUTHPARAMS
```

앞의 예시에서 표시된 정책 ARN에는 다음과 같은 URL 인코딩 ARN이 포함되어 있습니다.

```
arn:aws:iam::123456789012:policy/Role1policy
```

또한 이 예제의 `&AUTHPARAMS` 파라미터는 인증 정보의 자리 표시자로 사용됩니다. 이는 서명이며 AWS HTTP API 요청과 함께 포함되어야 합니다. AWS SDK를 사용하여 API 요청을 생성하는 것이 좋습니다. 이렇게 하면 SDK가 요청 서명을 대신 처리한다는 장점이 있습니다. API 요청을 직접 생성하여 서명해야 할 경우 Amazon Web Services 일반 참조의 서명 버전 4를 사용하여 AWS 요청에 서명에서 요청에 서명하는 방법 단원을 참조하십시오.

그 응답에는 임시 보안 자격 증명뿐만 아니라 연동 사용자 및 자격 증명 만료 시간에 대한 Amazon 리소스 이름(ARN)이 포함되어 있습니다.

Example 응답

```
<GetFederationTokenResponse xmlns="https://sts.amazonaws.com/doc/2011-06-15/">
<GetFederationTokenResult>
<Credentials>
  <SessionToken>
   AQoDYXdzEPT//////////wEXAMPLEtc764bNrC9SAPBSM22wDOk4x4HIZ8j4FZTwdQW
   LWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7mSEI/qkPpKPi/kMcGd
   QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
   9HFvlRd8Tx6q6fE8YQcHNVXAkiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
   +scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCEXAMPLE==
  </SessionToken>
  <SecretAccessKey>
```

```
  wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY
  </SecretAccessKey>
  <Expiration>2019-04-15T23:28:33.359Z</Expiration>
  <AccessKeyId>AKIAIOSFODNN7EXAMPLE;</AccessKeyId>
</Credentials>
<FederatedUser>
  <Arn>arn:aws:sts::123456789012:federated-user/Jean</Arn>
  <FederatedUserId>123456789012:Jean</FederatedUserId>
</FederatedUser>
<PackedPolicySize>4</PackedPolicySize>
</GetFederationTokenResult>
<ResponseMetadata>
<RequestId>c6104cbe-af31-11e0-8154-cbc7ccf896c7</RequestId>
</ResponseMetadata>
</GetFederationTokenResponse>
```

> **Note**
>
> AWS 변환은 전달된 세션 정책과 세션 태그를 별도의 제한이 있는 압축된 이진 형식으로 압축합니다. 일반 텍스트가 다른 요구 사항을 충족하는 경우에도 이 제한으로 인해 요청이 실패할 수 있습니다. `PackedPolicySize` 응답 요소는 요청에 대한 정책 및 태그가 상위 크기 제한과 얼마나 가까운지를 백분율로 나타냅니다.

AWS는 리소스 수준에서 권한을 부여할 것을 권장합니다(예: Amazon S3 버킷에 리소스 기반 정책 연결). `Policy` 파라미터는 생략할 수 있습니다. 그러나 연동 사용자에 대한 정책을 포함하지 않으면, 임시 보안 자격 증명은 어떤 권한도 부여하지 않을 것입니다. 이 경우 반드시 리소스 정책을 사용해 연동 사용자에게 AWS 리소스에 대한 액세스 권한을 부여해야 합니다.

예를 들어, 나의AWS 계정 번호가 1111222233333이고 Susan이 액세스하도록 허용하려는 Amazon S3 버킷을 내가 가지고 있다고 가정해 보겠습니다. Susan의 임시 보안 자격 증명에는 버킷에 대한 정책은 포함되어 있지 않습니다. 이러한 경우 버킷에 Susan의 ARN과 일치하는 ARN과 관련된 정책이 있는지 확인해야 합니다(예: `arn:aws:sts::111122223333:federated-user/Susan`).

GetSessionToken—신뢰할 수 없는 환경에 있는 사용자를 위한 임시 자격 증명

`GetSessionToken` API 작업은 기존 IAM 사용자에게 일련의 임시 보안 자격 증명을 반환합니다. 예를 들어 MFA가 IAM 사용자에 대해 활성화된 경우에만 AWS 요청을 허용하면 보안을 강화하는 데 유용합니다. 자격 증명은 일시적이므로 덜 안전한 환경을 통해 리소스에 액세스하는 IAM 사용자가 있을 때 보안을 강화하는 역할을 합니다. 덜 안전한 환경의 예시로는 모바일 디바이스 또는 웹 브라우저가 있습니다. 자세한 정보는 임시 보안 자격 증명 요청하기 (p. 304) 단원 또는 AWS Security Token Service API Reference의 GetSessionToken 단원을 참조하십시오.

기본적으로 IAM 사용자에 대한 임시 보안 자격 증명은 최대 12시간 동안 유효합니다. 그러나 `DurationSeconds` 파라미터를 사용하여 이 기간을 15분만큼 짧게 또는 36시간만큼 길게 요청할 수 있습니다. 보안상의 이유로 AWS 계정 루트 사용자의 토큰은 1시간의 유효 기간으로 제한됩니다.

`GetSessionToken`은 보안 토큰, 액세스 키 ID 및 보안 액세스 키로 구성된 임시 보안 자격 증명을 반환합니다. 다음 예제에서는 `GetSessionToken`을 사용한 샘플 요청 및 응답을 보여줍니다. 응답에는 임시 보안 자격 증명의 만료 시간도 포함되어 있습니다.

Example 요청

```
https://sts.amazonaws.com/
?Version=2011-06-15
&Action=GetSessionToken
&DurationSeconds=1800
```

```
&AUTHPARAMS
```

예시의 AUTHPARAMS 파라미터는 서명에 대한 자리 표시자입니다. 서명은 AWS HTTP API 요청에 포함해야 하는 인증 정보입니다. AWS SDK를 사용하여 API 요청을 생성하는 것이 좋습니다. 이렇게 하면 SDK가 요청 서명을 대신 처리한다는 장점이 있습니다. API 요청을 직접 생성하여 서명해야 할 경우 Amazon Web Services 일반 참조의 서명 버전 4를 사용하여 AWS 요청에 서명에서 요청에 서명하는 방법 단원을 참조하십시오.

Example 응답

```
<GetSessionTokenResponse xmlns="https://sts.amazonaws.com/doc/2011-06-15/">
<GetSessionTokenResult>
<Credentials>
  <SessionToken>
   AQoEXAMPLEH4aoAH0gNCAPyJxz4BlCFFxWNE1OPTgk5TthT+FvwqnKwRcOIfrRh3c/L
   To6UDdyJwOOvEVPvLXCrrrUtdnniCEXAMPLE/IvU1dYUg2RVAJBanLiHb4IgRmpRV3z
   rkuWJOgQs8IZZaIv2BXIa2R4OlgkBN9bkUDNCJiBeb/AXlzBBko7b15fjrBs2+cTQtp
   Z3CYWFXG8C5zqx37wnOE49mRl/+OtkIKGO7fAE
  </SessionToken>
  <SecretAccessKey>
  wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY
  </SecretAccessKey>
  <Expiration>2011-07-11T19:55:29.611Z</Expiration>
  <AccessKeyId>AKIAIOSFODNN7EXAMPLE</AccessKeyId>
</Credentials>
</GetSessionTokenResult>
<ResponseMetadata>
<RequestId>58c5dbae-abef-11e0-8cfe-09039844ac7d</RequestId>
</ResponseMetadata>
</GetSessionTokenResponse>
```

선택 사항으로 GetSessionToken 요청은 AWS 멀티 팩터 인증(MFA) 확인에 대한 SerialNumber 및 TokenCode 값을 포함할 수 있습니다. 제공한 값이 유효하면 AWS STS에서는 MFA 인증 상태가 포함된 임시 보안 자격 증명을 제공합니다. 그런 다음 임시 보안 자격 증명은 MFA 인증이 유효한 동안 MFA로 보호되는 API 작업 또는 AWS 웹 사이트에 액세스하는 데 사용할 수 있습니다.

다음 예는 MFA 확인 코드 및 디바이스 일련 번호를 포함하는 GetSessionToken 요청을 보여줍니다.

```
https://sts.amazonaws.com/
?Version=2011-06-15
&Action=GetSessionToken
&DurationSeconds=7200
&SerialNumber=YourMFADeviceSerialNumber
&TokenCode=123456
&AUTHPARAMS
```

> **Note**
>
> AWS STS에 대한 호출은 전역 엔드포인트 또는 AWS 계정이 활성화된 리전 엔드포인트 어느 곳으로도 이루어질 수 있습니다. 자세한 정보는 리전 및 엔드포인트의 AWS STS 단원을 참조하십시오. 예시의 AUTHPARAMS 파라미터는 서명에 대한 자리 표시자입니다. 서명은 AWS HTTP API 요청에 포함해야 하는 인증 정보입니다. AWS SDK를 사용하여 API 요청을 생성하는 것이 좋습니다. 이렇게 하면 SDK가 요청 서명을 대신 처리한다는 장점이 있습니다. API 요청을 직접 생성하여 서명해야 할 경우 Amazon Web Services 일반 참조의 서명 버전 4를 사용하여 AWS 요청에 서명에서 요청에 서명하는 방법 단원을 참조하십시오.

AWS STS API 작업 비교

다음 표는 임시 보안 자격 증명을 반환하는 AWS STS의 API 작업이 수행하는 기능을 비교해 보여줍니다. 역할을 수임해 임시 보안 자격 증명을 요청하는 데 사용할 수 있는 여러 방법을 알아보려면 IAM 역할 사

용 (p. 250) 단원을 참조하십시오. 세션 태그를 전달할 수 있는 다양한 AWS STS API 작업에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

API 옵션 비교

AWS STS API	호출할 수 있는 사용자	자격 증명의 수명 (최소 | 최대 | 기본)	MFA 지원[1]	세션 정책 지원[2]	결과 임시 자격 증명에 대한 제한
AssumeRole	IAM 사용자 또는 기존 임시 보안 자격 증명이 있는 IAM 역할	15분 | 최대 세션 기간 설정[3] | 1시간	예	예	`GetFederationToken` 또는 `GetSessionToken` 호출 불가
AssumeRoleWithSAML	어떤 사용자나 호출자도 잘 알려진 자격 증명 공급자의 인증을 나타내는 SAML 인증 응답을 반드시 전달해야 합니다.	15분 | 최대 세션 기간 설정[3] | 1시간	아니요	예	`GetFederationToken` 또는 `GetSessionToken` 호출 불가
AssumeRoleWithWebIdentity	어떤 사용자나 호출자도 잘 알려진 자격 증명 공급자의 인증을 나타내는 웹 자격 인증 토큰을 반드시 전달해야 합니다.	15분 | 최대 세션 기간 설정[3] | 1시간	아니요	예	`GetFederationToken` 또는 `GetSessionToken` 호출 불가
GetFederationToken	IAM 사용자 또는 AWS 계정 루트 사용자	IAM 사용자: 15분 | 36시간 | 12시간 루트 사용자: 15분 | 1시간 | 1시간	아니요	예	AWS CLI 또는 AWS API를 사용하여 IAM 작업을 호출할 수 없습니다. `GetCallerIdentity`를 제외한 AWS STS 작업을 호출할 수 없습니다.[4] 콘솔로의 SSO가 허용됩니다.[5]
GetSessionToken	IAM 사용자 또는 AWS 계정 루트 사용자	IAM 사용자: 15분 | 36시간 | 12시간 루트 사용자: 15분 | 1시간 | 1시간	예	아니요	요청으로 MFA 정보가 포함되지 않으면 IAM API 작업 호출 불가 `AssumeRole` 또는 `GetCallerIdentity`를 제외한 AWS STS API 작업 호출 불가 콘솔로의 SSO는 허용되지 않습니다.[6]

[1] MFA 지원. AssumeRole 및 GetSessionToken API 작업을 호출할 때 멀티 팩터 인증(MFA)에 대한 정보를 포함시킬 수 있습니다. 이는 API 호출의 결과물인 임시 보안 자격 증명을 MFA 디바이스로 인증된 사용자들만 사용할 수 있게 해줍니다. 자세한 정보는 MFA 보호 API 액세스 구성 (p. 146) 단원을 참조하십시오.

[2] 세션 정책 지원. 세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 정책입니다. 이 정책은 세션에 할당된 역할/사용자 자격 증명 기반 정책의 권한을 제한합니다. 결과적으로 얻는 세션의 권한은 엔터티의 자격 증명 기반 정책과 세션 정책의 교집합입니다 세션 정책을 사용하여 수임된 역할의 자격 증명 기반 정책에서 허용되는 것보다 더 많은 권한을 부여할 수는 없습니다. 역할 세션 권한에 대한 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오.

[3] 최대 세션 기간 설정. `DurationSeconds` 파라미터를 사용하여 역할 세션 기간을 900초(15초)에서 해당 역할에 대한 최대 세션 기간 설정까지 지정합니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오.

[4] GetCallerIdentity. 이 작업을 실행하는 데 따로 권한이 필요하지 않습니다. 관리자가 `sts:GetCallerIdentity` 작업에 대한 액세스를 명시적으로 거부하는 정책을 IAM 사용자 또는 역할에게 추가하더라도 이 작업을 계속해서 실행할 수 있습니다. 권한이 필요하지 않은 이유는 IAM 사용자 또는 역할의 액세스가 거부되어도 반환되는 정보는 동일하기 때문입니다. 응답 예제를 보려면 iam:DeleteVirtualMFADevice를 수행할 권한이 없음 (p. 536) 단원을 참조하십시오.

[5] 콘솔로 SSO(Single Sign-On)하기 SSO를 지원하기 위해 AWS는 페더레이션 엔드포인트(`https://signin.aws.amazon.com/federation`)를 호출해 임시 보안 자격 증명을 전달할 수 있게 해줍니다. 엔드포인트는 암호 없이도 사용자를 콘솔에 바로 로그인시켜주는 URL을 구성하는 데 사용 가능한 토큰을 반환합니다. 자세한 정보는 AWS 보안 블로그의 SAML 2.0 연동 사용자가 AWS Management 콘솔에 액세스할 수 있게 하기 (p. 208) 및 AWS Management Console에 대한 교차 계정 액세스를 가능하게 하는 방법 단원을 참조하십시오.

[6] 임시 자격 증명을 검색한 이후에 연동 SSO 엔드포인트로 자격 증명을 전달하여 AWS Management 콘솔에 액세스할 수 없습니다. 자세한 내용은 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.

AWS 리소스에서 임시 자격 증명 사용

임시 보안 자격 증명을 사용하여 AWS CLI 또는 AWS API(AWS SDK 사용)를 사용하여 AWS 리소스를 프로그래밍 방식으로 요청할 수 있습니다. 임시 자격 증명은 IAM 사용자 자격 증명과 같은 장기 보안 자격 증명을 사용하는 것과 동일한 권한을 제공합니다. 그러나 몇 가지 차이점이 있습니다.

- 임시 보안 자격 증명을 사용해 호출할 경우 그 호출에 반드시 세션 토큰이 포함되어야 하는데, 이 세션 토큰은 임시 자격 증명과 함께 반환됩니다. AWS는 세션 토큰을 사용해 임시 보안 자격 증명의 유효성을 검증합니다.
- 임시 자격 증명은 지정된 간격 후에 만료됩니다. 자격 증명이 만료된 후에는 그 자격 증명을 사용한 어떤 요청도 실패할 것이므로 일련의 새로운 자격 증명을 얻어야 합니다.
- 임시 자격 증명을 사용하여 요청하면 보안 주체에 태그 세트가 포함될 수 있습니다. 이러한 태그는 세션 태그와 사용자가 맡은 역할에 연결된 태그에서 가져옵니다. 세션 태그에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

AWS SDK, AWS Command Line Interface(AWS CLI) 또는 Windows PowerShell용 도구를 사용하는 경우 임시 보안 자격 증명을 가져오고 사용하는 방법은 컨텍스트에 따라 다릅니다. EC2 인스턴스 내부에서 코드, AWS CLI 또는 Windows PowerShell용 도구 명령을 실행 중이라면 Amazon EC2에 대한 역할을 이용할 수 있습니다. 그렇지 않은 경우 AWS STS API를 호출해 임시 자격 증명을 얻은 다음, 그 자격 증명을 사용해 AWS 서비스를 명시적으로 호출할 수 있습니다.

> **Note**
>
> AWS Security Token Service(AWS STS)를 사용하면 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 자격 증명을 생성하여 신뢰받는 사용자에게 제공할 수 있습니다. AWS STS에 대한 자세한 정보는 임시 보안 자격 증명 (p. 302) 단원을 참조하십시오. AWS STS는 `https://sts.amazonaws.com`에 기본 엔드포인트가 있는 전역적 서비스입니다. 이 엔드포인트는 미국 동부(오하이오) 리전에 있지만 이 엔드포인트 및 다른 엔드포인트에서 얻은 자격 증명은 전역적으로 유효합니다. 이러한 자격 증명은 모든 리전의 서비스 및 리소스에서 작동합니다. 지원되는 리전에서 엔드포인트에 대한 AWS STS API 호출을 할 수도 있습니다. 이렇게 지리적으로 더 가까운 리전에 있는 서버에서 요청함으로써 지연 시간을 단축할 수 있습니다. 자격 증명은 어떤 리전에서 오는지 상관없이 전역적으로 유효합니다. 자세한 내용은 AWS 리전에서 AWS STS 관리 (p. 326) 단원을 참조하십시오.

목차

Amazon EC2 인스턴스에서 임시 자격 증명 사용하기

EC2 인스턴스 내에서 AWS CLI 명령 또는 코드를 실행하고자 하는 경우 자격 증명을 얻는 바람직한 방법은 Amazon EC2에 대한 역할을 사용하는 것입니다. EC2 인스턴스 상에서 실행되는 애플리케이션에 부여하고 싶은 권한을 지정하는 IAM 역할을 생성합니다. 인스턴스를 시작할 때 그 역할을 인스턴스에 연결합니다.

인스턴스 상에서 실행되는 애플리케이션, AWS CLI 및 Windows PowerShell용 도구 명령은 인스턴스 메타데이터로부터 자동 임시 보안 자격 증명을 얻을 수 있습니다. 임시 보안 자격 증명을 명시적으로 가져올 필요는 없습니다. AWS SDK, AWS CLI 및 Windows PowerShell용 도구는 EC2 인스턴스 메타데이터 서비스에서 자격 증명을 자동으로 가져와서 사용합니다. 임시 자격 증명은 그 인스턴스에 연결된 역할에 대해 정의한 권한이 있습니다.

자세한 내용 및 예시는 다음을 참조하십시오.

- IAM 역할을 사용하여 Amazon Elastic Compute Cloud의 AWS 리소스에 대한 액세스 권한 부여 — AWS SDK for Java
- IAM 역할을 사용하여 액세스 권한 부여 — .NET용 AWS SDK
- 역할 생성 — Ruby용 AWS SDK

AWS SDK에서 임시 보안 자격 증명 사용하기

코드에서 임시 보안 자격 증명을 사용하려면 `AssumeRole`과 같이 AWS STS API를 프로그래밍 방식으로 호출하고 결과 자격 증명 및 세션 토큰을 추출합니다. 그런 다음 해당 값을 AWS에 대한 후속 호출을 위한 자격 증명으로 사용하면 됩니다. 다음 예는 AWS SDK를 사용할 경우 임시 보안 자격 증명을 사용하는 방법에 대한 유사 코드를 보여줍니다.

```
assumeRoleResult = AssumeRole(role-arn);
tempCredentials = new SessionAWSCredentials(
   assumeRoleResult.AccessKeyId,
   assumeRoleResult.SecretAccessKey,
   assumeRoleResult.SessionToken);
s3Request = CreateAmazonS3Client(tempCredentials);
```

Python으로 작성된 예제(AWS SDK for Python (Boto) 사용)는 IAM 역할(AWS API)로 전환하기 (p. 263) 단원을 참조하십시오. 이 예제에서는 `AssumeRole`을 호출하여 임시 보안 자격 증명을 가져온 다음 해당 자격 증명을 사용하여 Amazon S3를 호출하는 방법을 보여 줍니다.

`AssumeRole`, `GetFederationToken` 및 기타 API 작업을 호출하는 방법에 대한 자세한 내용은 AWS Security Token Service API Reference를 참조하십시오. 이러한 호출의 결과에서 임시 보안 자격 증명 및 세션 토큰을 얻는 방법에 대한 자세한 내용은 사용하고 있는 SDK의 설명서를 참조하십시오. SDK 및 도구 키트 섹션의 AWS 설명서 메인 페이지에서 모든 AWS SDK의 설명서를 검색할 수 있습니다.

이전 자격 증명이 만료되기 전에 반드시 새로운 일련의 자격 증명을 얻도록 해야 합니다. 일부 SDK에서는 자격 증명 갱신 프로세스를 관리해주는 공급자를 사용할 수 있습니다. 사용하고 있는 SDK의 설명서를 확인하십시오.

AWS CLI에서 임시 보안 자격 증명 사용하기

AWS CLI에서 임시 보안 자격 증명을 사용할 수 있습니다. 이 임시 보안 자격 증명은 정책을 테스트하는 데 유용합니다.

AWS CLI를 사용해 `AssumeRole` 또는 `GetFederationToken`과 같은 AWS STS API를 호출한 다음, 그 결과물로 얻은 출력을 캡처할 수 있습니다. 다음 예는 파일에 출력을 전송하는 `AssumeRole`에 대한 호출을 보여줍니다. 이 예제에서 `profile` 파라미터는 AWS CLI 구성 파일의 프로파일로 간주됩니다. 또한 역할을 맡을 권한이 있는 IAM 사용자의 자격 증명을 참조하는 것으로 간주됩니다.

```
$ aws sts assume-role --role-arn arn:aws:iam::123456789012:role/role-name --role-session-
name "RoleSession1" --profile IAM-user-name > assume-role-output.txt
```

명령이 끝나면 라우팅한 위치에서 액세스 키 ID, 보안 액세스 키 및 세션 토큰을 추출할 수 있습니다. 수동으로 또는 스크립트를 사용하여 이 작업을 수행할 수 있습니다. 그런 다음 이 값을 환경 변수에 할당할 수 있습니다.

AWS CLI 명령을 실행한다면 AWS CLI가 환경 변수를 먼저 검색하고 다음 순서로 자격 증명을 검색하는 특정 순서로 구성 파일을 검색합니다. 따라서 임시 자격 증명을 환경 변수에 넣은 후에 AWS CLI는 그 자격 증명을 기본 값으로 사용합니다. 명령에 `profile` 파라미터를 지정하면 AWS CLI에서 환경 변수를 건너뜁니다. 대신 AWS CLI에서 구성 파일을 확인하므로 사용자가 필요한 경우 환경 변수의 자격 증명을 재정의할 수 있습니다.

다음 예는 임시 보안 자격 증명에 대한 환경 변수를 설정한 다음, AWS CLI 명령을 호출하는 방법을 보여줍니다. `profile` 파라미터는 AWS CLI 명령에 포함되어 있지 않기 때문에 AWS CLI는 먼저 환경 변수에서 자격 증명을 검색하고, 따라서 임시 자격 증명을 사용합니다.

Linux

```
$ export AWS_ACCESS_KEY_ID=AKIAI44QH8DHBEXAMPLE
$ export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
$ export AWS_SESSION_TOKEN=AQoDYXdzEJr...<remainder of security token>
$ aws ec2 describe-instances --region us-west-1
```

Windows

```
C:\> SET AWS_ACCESS_KEY_ID=AKIAI44QH8DHBEXAMPLE
C:\> SET AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
C:\> SET AWS_SESSION_TOKEN=AQoDYXdzEJr...<remainder of token>
C:\> aws ec2 describe-instances --region us-west-1
```

API 작업을 통해 임시 보안 자격 증명 사용

AWS로 직접 HTTPS API 요청을 하는 경우, AWS Security Token Service(AWS STS)에서 가져오는 임시 보안 자격 증명으로 그러한 요청에 서명할 수 있습니다. 이렇게 하려면 AWS STS에서 받은 보안 액세스 키와 액세스 키 ID를 사용합니다. 장기 자격 증명을 사용하는 것과 동일한 방식으로 액세스 키 ID 및 보안 액세스 키를 사용하여 요청에 서명합니다. 또한 AWS STS로부터 받는 세션 토큰을 API 요청에 추가합니다. 그 세션 토큰을 HTTP 헤더 또는 `X-Amz-Security-Token`이라는 쿼리 문자열 파라미터에 추가합니다. 그 세션 토큰을 HTTP 헤더 또는 쿼리 문자열 파라미터에 추가하되, 하나에만 추가해야 합니다. HTTPS API 요청에 서명하는 방법에 대한 자세한 내용은 AWS General Reference의 AWS API 요청 서명을 참조하십시오.

추가 정보

다른 AWS 서비스와 함께 AWS STS를 사용하는 방법에 대한 자세한 내용은 다음 링크를 참조하십시오.

- Amazon S3. Amazon Simple Storage Service 개발자 가이드 의 IAM 사용자의 임시 자격 증명을 사용하여 요청 또는 연합된 사용자의 임시 자격 증명을 사용하여 요청하기을 참조하십시오.
- Amazon SNS. Amazon Simple Notification Service 개발자 안내서의 임시 보안 자격 증명 사용을 참조하십시오.
- Amazon SQS. Amazon Simple Queue Service 개발자 안내서의 임시 보안 자격 증명 사용을 참조하십시오.
- Amazon SimpleDB. Amazon SimpleDB 개발자 안내서의 임시 보안 자격 증명 사용을 참조하십시오.

사용자 임시 보안 자격 증명에 대한 권한 제어

AWS Security Token Service(AWS STS)를 사용하면 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 자격 증명을 생성하여 신뢰받는 사용자에게 제공할 수 있습니다. AWS STS에 대한 자세한 내용은 임시 보안 자격 증명 (p. 302) 단원을 참조하십시오. 임시 보안 자격 증명은 AWS STS가 발급한 후 만료 기간 동안 유효하며 취소될 수 없습니다. 그러나 임시 보안 자격 증명에 할당된 권한은 자격 증명을 사용해 요청이 이루어질 때마다 평가되기 때문에 자격 증명이 발급된 이후에라도 액세스 권한을 변경함으로써 자격 증명 취소 효과를 얻을 수 있습니다.

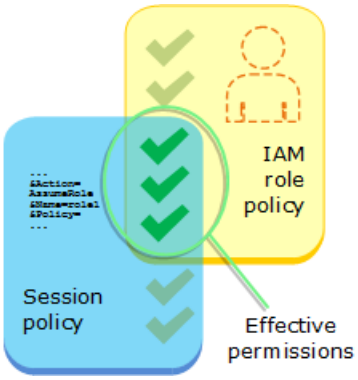
다음 주제는 독자가 AWS 권한 및 정책에 대한 유효한 지식이 있다고 가정합니다. 이 주제에 대한 자세한 내용은 액세스 관리 (p. 348) 단원을 참조하십시오.

주제

AssumeRole, AssumeRoleWithSAML 및 AssumeRoleWithWebIdentity에 대한 권한

수임된 역할에 대한 권한 정책은 `AssumeRole`, `AssumeRoleWithSAML` 및 `AssumeRoleWithWebIdentity`에 의해 반환되는 임시 보안 자격 증명에 대한 권한을 결정합니다. 역할을 생성 또는 업데이트할 때 이러한 권한을 정의합니다.

인라인 또는 관리형 세션 정책 (p. 351)을 `AssumeRole`, `AssumeRoleWithSAML` 또는 `AssumeRoleWithWebIdentity` API 작업의 파라미터로 전달할 수 있습니다. 세션 정책은 역할의 임시 자격 증명 세션에 대한 권한을 제한합니다. 결과적으로 얻는 세션의 권한은 역할의 자격 증명 기반 정책의 교차와 세션 정책입니다. 후속 AWS API 호출 시에도 역할의 임시 자격 증명을 사용하여 역할이 속한 계정의 리소스에 액세스할 수 있습니다. 세션 정책을 사용하여 수임된 역할의 자격 증명 기반 정책에서 허용되는 것보다 더 많은 권한을 부여할 수는 없습니다. 이 역할의 효과적인 권한을 AWS가 어떻게 결정하는지 자세히 알아보려면 정책 평가 로직 (p. 622) 단원을 참조하십시오.



'허용' 또는 '거부' 권한 부여 결정을 내릴 때 `AssumeRole`에 대한 원래 호출을 생성한 자격 증명에 연결된 정책은 AWS에서 평가하지 않습니다. 해당 사용자는 맡은 역할에 의해 할당된 권한을 위해 자신의 원래 권한을 일시적으로 포기합니다. `AssumeRoleWithSAML` 및 `AssumeRoleWithWebIdentity` API 작업의 경우 API 호출자가 AWS 자격 증명이 아니기 때문에 평가할 정책이 없습니다.

예: AssumeRole을 사용한 권한 할당

서로 다른 종류의 정책으로 `AssumeRole` API 작업을 사용할 수 있습니다. 여기 몇 가지 예가 있습니다.

역할 권한 정책

이 예에서는 선택 사항인 `Policy` 파라미터에 세션 정책을 지정하지 않고 `AssumeRole` API 작업을 호출합니다. 임시 자격 증명에 할당된 권한은 위임된 역할의 권한 정책에 따라 결정됩니다. 다음 예제 권한 정책은 S3 버킷 `productionapp`에 포함된 객체를 모두 나열하도록 역할 권한을 부여합니다. 또한 해당 역할이 이 버킷 내에서 객체를 가져오고, 배치하고, 삭제하도록 허용합니다.

Example 역할 권한 정책

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::productionapp"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::productionapp/*"
    }
  ]
}
```

파라미터로 전달되는 세션 정책

사용자에게 이전 예제와 동일한 역할을 수임하도록 허용하려 한다고 가정해 보겠습니다. 하지만 이 경우 역할 세션에 대해 `productionapp` S3 버킷에/에서 객체를 넣거나 가져오는 작업만을 허용하는 권한을 부여하고자 합니다. 객체를 삭제할 수 없도록 하고자 합니다. 이렇게 하기 위한 한 가지 방법은 새 역할을 만들어 그 역할의 권한 정책에 원하는 권한을 지정하는 것입니다. 또 다른 방법은 `AssumeRole` API를 호출하여 선택 사항인 `Policy` 파라미터의 세션 정책을 API 작업의 일부로 포함하는 것입니다. 결과적으로 얻는 세션의 권한은 역할의 자격 증명 기반 정책의 교차와 세션 정책입니다. 세션 정책을 사용하여 수임된 역할의 자격 증명 기반 정책에서 허용되는 것보다 더 많은 권한을 부여할 수는 없습니다. 역할 세션 권한에 대한 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오.

새 세션의 임시 자격 증명을 검색한 후 이를 권한을 부여하고자 하는 사용자에게 전달할 수 있습니다.

예를 들어 다음 정책이 API 호출의 파라미터로 전달된다고 가정합시다. 세션을 사용하는 사람에게는 다음 작업에 대한 수행 권한만 부여됩니다.

- `productionapp` 버킷에 있는 모든 객체의 목록을 조회합니다.
- 객체를 가져와 `productionapp` 버킷에 넣습니다.

다음 세션 정책에서는 `s3:DeleteObject` 권한이 필터링되어 위임된 세션에 `s3:DeleteObject` 권한이 부여되지 않습니다. 이 정책은 역할 세션에 대한 최대 권한을 설정하여 역할에 대한 기존 권한 정책을 재정의합니다.

Example **`AssumeRole`** API 호출로 전달된 세션 정책

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
```

```
      "Resource": "arn:aws:s3:::productionapp"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::productionapp/*"
    }
  ]
}
```

리소스 기반 정책

일부 AWS 리소스는 리소스 기반 정책을 지원하고 이 정책은 임시 보안 자격 증명에 영향을 미치는 권한을 정의하는 또 다른 메커니즘을 제공합니다. Amazon S3 버킷, Amazon SNS 주제, Amazon SQS 대기열 같은 몇몇 리소스만이 리소스 기반 정책을 지원합니다. 다음 예는 앞의 예들을 확장한 것으로서 `productionapp`이라는 S3 버킷을 사용합니다. 다음 정책은 버킷에 연결되어 있습니다.

다음 리소스 기반 정책을 `productionapp` 버킷에 연결할 때 모든 사용자들은 버킷에서 객체를 삭제할 권한을 거부당합니다. (정책의 `Principal` 요소에 유의하십시오.) 역할 권한 정책이 `DeleteObject` 권한을 부여한다 해도 여기에는 모든 수임된 역할 사용자들이 포함됩니다. 명시적인 `Deny` 문은 항상 `Allow` 문보다 우선 적용됩니다.

Example 버킷 정책

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Principal": {"AWS": "*"},
    "Effect": "Deny",
    "Action": "s3:DeleteObject",
    "Resource": "arn:aws:s3:::productionapp/*"
  }
}
```

다수의 정책 유형이 AWS에 의해 어떻게 결합되고 평가되는지에 대한 자세한 정보는 정책 평가 로직 (p. 622) 단원을 참조하십시오.

GetFederationToken에 대한 권한

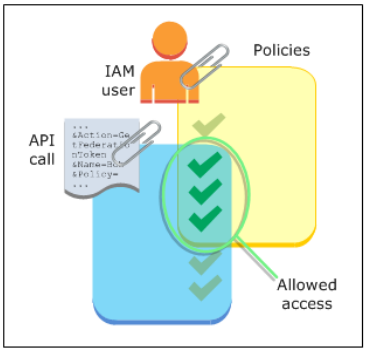
IAM 사용자가 `GetFederationToken` 작업을 호출하고 해당 사용자에 대한 임시 자격 증명을 반환합니다. 이 작업은 사용자를 연동합니다. 연동 사용자에게 할당된 권한은 둘 중 한 곳에 정의되어 있습니다.

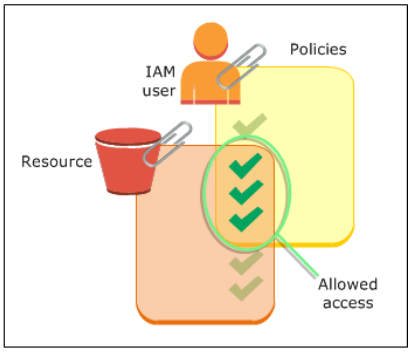
- `GetFederationToken` API 호출의 파라미터로 전달되는 세션 정책. (가장 일반적)
- 정책의 `Principal` 요소에서 연동 사용자를 명시적으로 호명하는 리소스 기반 정책. (일반적이지 않음)

세션 정책은 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 연동 사용자 세션을 생성하고 세션 정책을 전달할 때 결과적으로 얻는 세션의 권한은 IAM 사용자의 자격 증명 기반 정책의 교차와 세션 정책입니다. 세션 정책을 사용하여 연동된 사용자의 자격 증명 기반 정책에서 허용되는 권한을 부여할 수는 없습니다.

대부분의 경우 `GetFederationToken` API 호출로 정책을 전달하지 않으면 그 결과 얻게 되는 임시 보안 자격 증명은 아무 권한이 없습니다. 하지만 리소스 기반 정책은 세션에 대한 추가 권한을 제공할 수 있습니다. 세션을 허용된 보안 주체로 지정하는 리소스 기반 정책을 사용하여 리소스에 액세스할 수 있습니다.

다음 그림은 `GetFederationToken` 호출에 의해 반환되는 임시 보안 자격 증명에 대한 권한을 정책들이 어떻게 상호 작용하여 결정하는지를 시각적으로 재현한 것입니다.





예: GetFederationToken을 사용한 권한 할당

서로 다른 종류의 정책으로 `GetFederationToken` API 작업을 사용할 수 있습니다. 여기 몇 가지 예가 있습니다.

IAM 사용자에게 연결된 정책

이 예시에는 2개의 백엔드 웹 서비스에 의존하는 브라우저 기반 클라이언트 애플리케이션이 있습니다. 백엔드 서비스 중 하나는 자신만의 인증 서버로서 고유한 자격 증명 시스템을 사용해 클라이언트 애플리케이션을 인증합니다. 다른 백엔드 서비스는 AWS 서비스로, 클라이언트 애플리케이션의 기능 중 일부를 제공합니다. 이 클라이언트 애플리케이션은 서버에 의해 인증되고, 서버는 적절한 권한 정책을 생성하거나 가져옵니다. 서버는 이제 `GetFederationToken` API를 호출해 임시 보안 자격 증명을 얻은 다음, 그 자격 증명을 클라이언트 애플리케이션에 반환합니다. 이제 클라이언트 애플리케이션은 임시 보안 자격 증명을 사용해 AWS 서비스에 직접 요청할 수 있게 됩니다. 이 아키텍처는 클라이언트 애플리케이션이 장기 AWS 자격 증명을 포함하지 않고도 AWS 요청을 할 수 있도록 허용합니다.

인증 서버에서 이름이 `token-app`인 IAM 사용자의 장기 보안 자격 증명을 사용하여 `GetFederationToken` API를 호출합니다. 하지만 장기 IAM 사용자 자격 증명은 서버에 유지되고 클라이언트에 배포되지 않습니다. 다음 예시 정책은 `token-app` IAM 사용자에게 연결되어 연동 사용자(클라이언트)에게 필요한 가장 폭넓은 권한 집합을 정의합니다. `sts:GetFederationToken` 권한은 인증 서비스가 연동 사용자에 대한 임시 보안 자격 증명을 얻는 데 필요하다는 점에 유의하십시오.

> **Note**
>
> AWS는 샘플 Java 애플리케이션을 제공함으로써 이 목적에 기여하는데, Java 애플리케이션은 자격 증명 등록을 위한 토큰 벤딩 머신 - 샘플 Java 웹 애플리케이션에서 다운로드할 수 있습니다.

Example **`GetFederationToken`**을 호출하는 IAM 사용자 **`token-app`**에 연결된 정책

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:GetFederationToken",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "dynamodb:ListTables",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sqs:ReceiveMessage",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": "s3:ListBucket",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sns:ListSubscriptions",
      "Resource": "*"
    }
  ]
}
```

이전 정책은 IAM 사용자에게 여러 가지 권한을 부여합니다. 하지만 이 정책만으로는 연동된 사용자에게 권한을 부여하지 않습니다. IAM 사용자가 `GetFederationToken`을 호출하고 정책을 API 호출의 파라미터로 전달하지 않는다면, 그 결과로 얻은 연동 사용자에게는 유효한 권한이 없습니다.

파라미터로 전달되는 세션 정책

연동 사용자에게 적절한 권한이 할당되도록 하는 가장 일반적인 방법은 `GetFederationToken` API 호출의 세션 정책을 전달하는 것입니다. 앞의 예시를 확장해 IAM 사용자 `token-app`의 자격 증명을 사용하여 `GetFederationToken` 호출이 이루어진다고 가정합니다. 그런 다음 세션 정책이 API 호출의 파라미터로 전달된다고 가정합니다. 결과적으로 연동 사용자는 이름이 `productionapp`인 Amazon S3 버킷의 콘텐츠를 나열할 권한을 갖습니다. 사용자는 `productionapp` 버킷의 항목들에 대한 Amazon S3, `GetObject`, `PutObject` 및 `DeleteObject` 작업을 수행할 수 없습니다.

연동 사용자에게 이 권한이 할당되는 것은 권한이 IAM 사용자 정책과 전달한 세션 정책의 교차 지점이기 때문입니다.

연동 사용자는 Amazon SNS, Amazon SQS, Amazon DynamoDB 또는 S3 버킷(`productionapp` 제외)에서 작업을 수행할 수 없습니다. 이러한 작업은 관련 권한이 `GetFederationToken` 호출과 연결된 IAM 사용자에게 부여되었더라도 거부됩니다.

Example **`GetFederationToken`** API 호출의 파라미터로 전달되는 세션 정책

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::productionapp"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::productionapp/*"]
    }
  ]
}
```

리소스 기반 정책

일부 AWS 리소스는 리소스 기반 정책을 지원하고, 이 정책은 연동 사용자에게 직접 권한을 부여하는 또 다른 메커니즘을 제공합니다. 일부 AWS 서비스만이 리소스 기반 정책을 지원합니다. 예를 들어, Amazon S3의 경우 버킷, Amazon SNS의 경우 주제, Amazon SQS의 경우 대기열에 정책을 연결할 수 있습니다. 리소스 기반 정책을 지원하는 모든 서비스 목록은 IAM로 작업하는 AWS 서비스 (p. 573) 및 표의 "리소스 기반 정책" 열을 참조하십시오. 리소스 기반 정책을 사용하여 연동 사용자에게 직접 권할을 할당할 수 있습니다. 리소스 기반 정책의 `Principal` 요소에서 연동 사용자의 Amazon 리소스 이름(ARN)을 지정하면 됩니다. 다음 예에서는 이를 설명하고 이름이 `productionapp`인 S3 버킷을 사용하여 앞의 예시를 확장합니다.

다음 리소스 기반 정책은 버킷에 연결되어 있습니다. 이 버킷 정책은 Carol이라는 연합된 사용자가 버킷에 액세스할 수 있도록 허용합니다. 다음 리소스 기반 정책이 적용되고 앞서 기술된 예시 정책이 `token-app` IAM 사용자에 연결되어 있으면, Carol이라는 연합된 사용자는 `productionapp`이라는 버킷에 대해 `s3:GetObject`, `s3:PutObject` 및 `s3:DeleteObject` 작업을 수행할 수 있는 권한이 있습니다. 이는 `GetFederationToken` API 호출의 파라미터로 전달되는 세션 정책이 없을 때에도 해당됩니다. 왜냐하면 이 경우에 Carol이라는 연동 사용자는 다음 리소스 기반 정책에 의해 명시적으로 권한을 부여받았기 때문입니다.

그 권한이 IAM 사용자 및 연동 사용자 둘 다에게 명시적으로 부여될 때만 연동 사용자는 권한을 부여받는다는 것을 명심하십시오. `GetFederationToken` API 호출의 파라미터로 전달되는 세션 정책을 통해 연합된 사용자에게 권한을 부여할 수 있습니다. 다음 예제에서처럼 정책의 `Principal` 요소에서 연합된 사용자의 이름을 명시적으로 지정하는 리소스 기반 정책을 통해서도 권한을 부여할 수 있습니다.

Example 연동 사용자에 대한 액세스를 허용하는 버킷 정책

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Principal": {"AWS": "arn:aws:sts::ACCOUNT-ID-WITHOUT-HYPHENS:federated-user/Carol"},
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": ["arn:aws:s3:::productionapp/*"]
  }
}
```

GetSessionToken에 대한 권한

`GetSessionToken` API 작업 또는 `get-session-token` CLI 명령을 호출해야 하는 기본적인 경우는 사용자가 멀티 팩터 인증(MFA)으로 인증되어야 할 때입니다. MFA로 인증된 사용자가 요청하는 경우에 한해 특정 작업들을 허용하는 정책을 작성하는 것도 가능합니다. MFA 권한 부여 확인을 성공적으로 통과하려면 사용자는 먼저 `GetSessionToken`을 호출하여 선택 사항인 `SerialNumber` 및 `TokenCode` 파라미터를 포함해야 합니다. 사용자가 MFA 디바이스를 통해 인증을 받으면 `GetSessionToken` API 작업에서 반환하는 자격 증명에는 MFA 컨텍스트가 포함됩니다. 이 컨텍스트에서는 사용자가 MFA 디바이스를 통해 인증을 받았고 MFA 인증이 필요한 API 작업에 대한 권한이 있음을 표시합니다.

GetSessionToken에 필요한 권한

사용자는 권한이 없어도 세션 토큰을 얻을 수 있습니다. `GetSessionToken` 작업의 목적은 MFA를 사용하는 사용자를 인증하는 것입니다. 정책을 사용하여 인증 작업을 제어할 수는 없습니다.

대부분의 AWS 작업을 수행할 수 있는 권한을 부여하려면 이름이 같은 작업을 정책에 추가합니다. 예를 들어 사용자를 생성하려면 `CreateUser` API 작업, `create-user` CLI 명령 또는 AWS Management 콘솔을 사용해야 합니다. 이러한 작업을 수행하려면 `CreateUser` 작업에 액세스할 수 있게 허용하는 정책이 있어야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateUser",
            "Resource": "*"
        }
    ]
}
```

정책에 `GetSessionToken` 작업을 포함할 수 있지만, 사용자가 `GetSessionToken` 작업을 수행할 수 있는 권한에는 영향을 미치지 않습니다.

GetSessionToken에서 부여하는 권한

`GetSessionToken`이 IAM의 자격 증명으로 호출되면, 임시 보안 자격 증명은 IAM 사용자와 동일한 권한을 갖습니다. 마찬가지로 `GetSessionToken`이 AWS 계정 루트 사용자으로 호출되면, 임시 보안 자격 증명은 루트 사용자 권한을 갖습니다.

> **Note**
>
> 루트 사용자 자격 증명으로 `GetSessionToken`을 호출하지 않는 것이 좋습니다. 대신에 모범 사례 (p. 60)에 따라 필요한 권한을 지닌 IAM 사용자를 생성하십시오. 그런 다음 이러한 IAM 사용자를 AWS와의 일상적인 상호 작용에 사용하십시오.

`GetSessionToken`을 호출할 때 얻는 임시 자격 증명은 다음과 같은 기능과 한계를 지닙니다.

- `https://signin.aws.amazon.com/federation`에서 페더레이션 Single Sign-On 엔드포인트로 자격 증명을 전달하여 AWS Management 콘솔에 액세스할 수 있습니다. 자세한 내용은 사용자 지정 자격 증명 브로커가 AWS 콘솔에 액세스할 수 있도록 하기 (p. 210) 단원을 참조하십시오.
- 자격 증명을 사용해 IAM 또는 AWS STS API 작업을 호출할 수 없습니다. 자격 증명을 사용해 다른 AWS 서비스에 대한 API 작업을 호출할 수는 있습니다.

AWS STS API 작업 비교 (p. 311)에서 이 API 작업과 이 작업의 한계 및 기능을 임시 보안 자격 증명을 생성하는 다른 API와 비교해 보십시오.

`GetSessionToken`을 사용한 MFA 보호 API 액세스에 대한 자세한 내용은 MFA 보호 API 액세스 구성 (p. 146) 단원을 참조하십시오.

임시 보안 자격 증명에 대한 권한 비활성화

임시 보안 자격 증명은 만료될 때까지 유효하며 취소될 수 없습니다. 그러나 권한은 자격 증명을 사용해 AWS 요청이 이루어질 때마다 평가되기 때문에 자격 증명이 발급된 이후에라도 자격 증명에 대한 권한을 변경함으로써 자격 증명 취소 효과를 얻을 수 있습니다. 임시 보안 자격 증명에서 모든 권한을 제거하는 경우 그 자격 증명을 사용하는 후속 AWS 요청은 실패하게 됩니다. 임시 보안 자격 증명에 할당된 권한을 변경 또는 제거하는 메커니즘은 다음 섹션에 설명되어 있습니다.

> **Note**
>
> 기존 정책 권한을 업데이트할 때 또는 사용자나 리소스에 새 정책을 적용할 때 정책 업데이트가 효력이 생기는 데 몇 분이 걸릴 수 있습니다.

주제

- 임시 보안 자격 증명 생성자에 대한 액세스 거부 (p. 322)
- 이름을 사용한 임시 보안 자격 증명에 대한 액세스 거부 (p. 323)
- 특정 시각 이전에 발급된 임시 보안 자격 증명에 대한 액세스 거부 (p. 324)

임시 보안 자격 증명 생성자에 대한 액세스 거부

임시 보안 자격 증명에 할당된 권한을 비활성화 또는 제거하려면 자격 증명 생성자와 연결된 권한을 변경 또는 제거하면 됩니다. 자격 증명 생성자는 자격 증명 획득에 사용된 AWS STS API에 의해 결정됩니다. 이 생성자에 연결된 권한을 변경 또는 제거하는 메커니즘은 다음 섹션에 설명되어 있습니다.

AssumeRole, AssumeRoleWithSAML 또는 AssumeRoleWithWebIdentity에 의해 생성된 자격 증명에 대한 액세스 거부

`AssumeRole`, `AssumeRoleWithSAML`, 또는 `AssumeRoleWithWebIdentity` API 작업을 호출함으로써 획득한 임시 보안 자격 증명에 할당된 권한을 변경하거나 제거하려면 위임받은 역할에 대한 권한을 정의하는

역할 권한 정책을 편집 또는 삭제하면 됩니다. 역할을 수임함으로써 획득한 임시 보안 자격 증명은 수임된 역할에 대한 권한 정책에 정의된 것보다 더 많은 권한을 가질 수 없으며, 임시 보안 자격 증명에 할당된 권한은 AWS 호출에 사용될 때마다 평가됩니다. 역할의 권한 정책을 편집하거나 삭제하면 이러한 변경은 역할의 권한 정책을 변경하기 전에 발급된 자격 증명을 비롯해 해당 역할에 연결된 모든 임시 보안 자격 증명의 권한에 영향을 미칩니다. IAM 역할의 임시 보안 자격 증명 취소 (p. 273)의 단계를 따라 특정 세션에 대한 모든 권한을 즉시 취소할 수 있습니다.

역할 권한 정책 편집에 대한 자세한 정보는 역할 변경 (p. 274) 단원을 참조하십시오.

GetFederationToken 또는 GetSessionToken에 의해 생성된 자격 증명에 대한 액세스 거부

`GetFederationToken` 또는 `GetSessionToken` API 작업을 호출함으로써 획득한 임시 보안 자격 증명에 할당된 권한을 변경 또는 제거하려면 `GetFederationToken` 또는 `GetSessionToken`을 호출하는 데 사용된 자격 증명의 IAM 사용자에 연결된 정책을 편집 또는 삭제하면 됩니다. `GetFederationToken` 또는 `GetSessionToken`을 호출하여 획득한 임시 보안 자격 증명은 권한 획득을 위해 자신의 자격 증명을 사용한 IAM 사용자보다 많은 권한을 가질 수 없습니다. 뿐만 아니라 임시 보안 자격 증명에 할당된 권한은 AWS 요청을 위해 사용될 때마다 평가됩니다. IAM 사용자의 권한을 편집 또는 삭제하면 그 변경 사항이 사용자가 생성한 모든 임시 보안 자격 증명뿐만 아니라 IAM 사용자에게도 영향을 미친다는 것에 유의하십시오.

> **Important**
>
> AWS 계정 루트 사용자에 대한 권한은 변경할 수 없습니다. 따라서 루트 사용자로 로그인할 때 `GetFederationToken` 또는 `GetSessionToken`을 호출하여 생성된 임시 보안 자격 증명에 대한 권한도 변경할 수 없습니다. 이런 이유 때문에 루트 사용자로 `GetFederationToken` 또는 `GetSessionToken`을 호출하지 않는 것이 좋습니다.

`GetFederationToken` 또는 `GetSessionToken`을 호출하는 데 자격 증명이 사용된 IAM 사용자와 연결된 정책을 변경 또는 제거하는 방법에 대한 정보는 IAM 정책 관리 (p. 435) 단원을 참조하십시오.

이름을 사용한 임시 보안 자격 증명에 대한 액세스 거부

자격 증명을 생성한 IAM 사용자 또는 역할의 권한에 영향을 미치지 않고 임시 보안 자격 증명에 대한 액세스를 거부할 수 있습니다. 액세스를 거부하려면 리소스 기반 정책의 `Principal` 요소에서 임시 보안 자격 증명의 Amazon 리소스 이름(ARN)을 지정하면 됩니다. (일부 AWS 서비스만이 리소스 기반 정책을 지원합니다).

연동 사용자에 대한 액세스 거부

예를 들어 이름이 `token-app`인 IAM 사용자가 있고 그 사용자의 자격 증명이 `GetFederationToken`을 호출하는 데 사용된다고 가정합시다. `GetFederationToken` API 호출로 인해 Bob이라는 연동 사용자(연동 사용자의 이름은 API 호출의 `Name` 파라미터에서 가져옵니다)와 연결된 임시 보안 자격 증명이 생성되었습니다. 연동 사용자 Bob이 EXAMPLE-BUCKET이라는 S3 버킷에 액세스하는 것을 거부하려면 아래 예시된 버킷 정책을 EXAMPLE-BUCKET에 연결하면 됩니다. 이렇게 하면 연동 사용자의 Amazon S3 권한에만 영향을 미칠 뿐 연동 사용자에게 부여된 다른 권한들은 영향을 받지 않는 것에 유의하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Principal": {"AWS": "arn:aws:sts::ACCOUNT-ID-WITHOUT-HYPHENS:federated-user/Bob"},
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "arn:aws:s3:::EXAMPLE-BUCKET"
  }
}
```

연동 사용자를 지정하는 대신에 버킷 정책의 `Principal` 요소에 있는 `GetFederationToken`을 호출하는 데 자격 증명이 사용된 IAM 사용자의 ARN을 지정할 수 있습니다. 이 경우 이전 정책의 `Principal` 요소는 다음과 같을 것입니다.

```
"Principal": {"AWS": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:user/token-app"}
```

정책에서 IAM 사용자 `token-app`의 ARN을 지정하면 그 결과 Bob이라는 연동 사용자뿐만 아니라 `token-app`에 의해 생성된 모든 연동 사용자에 대한 액세스가 거부된다는 점에 유의하십시오.

수임된 역할 사용자에 대한 액세스 거부

역할 수임에 의해 생성된 임시 보안 자격 증명의 ARN을 지정할 수도 있습니다. 차이는 리소스 기반 정책의 `Principal` 요소에서 사용되는 구문에 있습니다. 예를 들어 사용자가 `Accounting-Role`이라는 역할을 수임하고 `RoleSessionName`의 `Mary`을 지정한다고 가정합시다(`RoleSessionName`은 `AssumeRole` API 호출의 파라미터입니다). 이 API 호출로 인해 얻은 임시 보안 자격 증명에 대한 액세스를 거부하려면 리소스 기반 정책의 `Principal` 요소는 다음과 같아야 합니다.

```
"Principal": {"AWS": "arn:aws:sts::ACCOUNT-ID-WITHOUT-HYPHENS:assumed-role/Accounting-Role/
Mary"}
```

리소스 기반 정책의 `Principal` 요소에 있는 IAM의 ARN을 다음 예시와 같이 지정할 수도 있습니다. 이 경우 그 정책으로 인해 `Accounting-Role`이라는 역할과 연결된 모든 임시 보안 자격 증명에 대한 액세스는 거부될 것입니다.

```
"Principal": {"AWS": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/Accounting-Role"}
```

특정 시각 이전에 발급된 임시 보안 자격 증명에 대한 액세스 거부

특정 시각 또는 날짜 이전에 생성된 임시 보안 자격 증명에 대한 액세스만 거부할 수도 있습니다. 이렇게 하려면 정책의 `aws:TokenIssueTime` 요소에 있는 `Condition`의 값을 지정해야 합니다. 다음 정책은 한 가지 예를 보여줍니다. 임시 보안 자격 증명을 생성한 IAM 사용자에게 다음 예시와 유사한 정책을 연결합니다. 그 정책은 `aws:TokenIssueTime`의 값이 지정된 날짜와 시각보다 이른 경우에만 모든 권한을 거부합니다. `aws:TokenIssueTime`의 값은 임시 보안 자격 증명이 생성된 정확한 시간과 일치합니다. `aws:TokenIssueTime` 값은 임시 보안 자격 증명으로 로그인된 AWS 요청의 콘텍스트에서만 존재하므로 정책의 `Deny` 문은 IAM 사용자의 장기 자격 증명으로 로그인한 요청에는 영향을 미치지 않습니다.

다음 정책도 역할에 연결할 수 있습니다. 이 경우 정책은 지정된 시각 및 날짜 이전에 그 역할에 의해 생성된 임시 보안 자격 증명에만 영향을 미칩니다. 자격 증명이 지정된 시각 및 날짜 이후에 그 역할에 의해 생성된 경우 정책의 `Condition` 요소가 거짓으로 평가되어 `Deny` 문은 영향을 미치지 않습니다.

Example 발급 시각을 사용해 임시 자격 증명에 대한 모든 권한을 거부하는 정책

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {"DateLessThan": {"aws:TokenIssueTime": "2014-05-07T23:47:00Z"}}
  }
}
```

이러한 식으로 세션이 취소된 유효한 사용자는 작업을 계속하려면 새 세션을 위한 임시 자격 증명을 가져와야 합니다. AWS CLI는 자격 증명이 만료될 때까지 이를 캐시합니다. CLI가 더 이상 유효하지 않은 캐시된 자격 증명을 강제로 삭제하고 새로 고치게 하려면 다음 명령 중 하나를 실행합니다.

Linux, MacOS 또는 Unix

```
$ rm -r ~/.aws/cli/cache
```

Windows

```
C:\> del /s /q %UserProfile%\.aws\cli\cache
```

임시 보안 자격 증명을 생성할 수 있는 권한 부여

기본적으로 IAM 사용자는 연동 사용자 및 역할을 위한 임시 보안 자격 증명을 생성할 수 있는 권한이 없습니다. 사용자에게 이러한 권한을 제공하려면 정책을 사용해야 합니다. 사용자에게 직접 권한을 부여할 수 있지만, 그룹에게 권한을 부여할 것을 강력히 권고합니다. 그렇게 하면 권한 관리가 훨씬 쉬워집니다. 어떤 사용자가 권한에 연결된 작업을 수행할 필요가 더 이상 없는 경우에는 그룹에서 그 사용자를 삭제하기만 하면 됩니다. 다른 어떤 사용자가 그 작업을 수행해야 한다면 해당 그룹에 추가해 권한을 부여하면 됩니다.

연동 사용자 또는 역할을 위해 임시 보안 자격 증명을 생성할 수 있는 권한을 IAM 그룹에게 부여하려면 다음 권한 중 하나 또는 둘 다를 부여하는 정책을 연결하면 됩니다.

- 연동 사용자들이 IAM 역할에 액세스하도록 하려면 AWS STS `AssumeRole`에 대한 액세스 권한을 부여하십시오.
- 역할이 필요 없는 연동 사용자에 대해서는 AWS STS `GetFederationToken`에 대한 액세스 권한을 부여하십시오.

`AssumeRole` 및 `GetFederationToken` API 작업 간의 차이점을 보려면 임시 보안 자격 증명 요청하기 (p. 304) 단원을 참조하십시오.

IAM 사용자는 `GetSessionToken`을 호출하여 임시 보안 자격 증명을 생성할 수도 있습니다. 사용자는 권한이 없어도 `GetSessionToken`을 호출할 수 있습니다. 이 작업의 목적은 MFA를 사용하는 사용자를 인증하는 것입니다. 정책을 사용하여 인증을 제어할 수는 없습니다. 즉 IAM 사용자가 임시 자격 증명을 생성할 목적으로 `GetSessionToken`을 호출하는 작업을 하지 못하게 할 수 없습니다.

Example : 역할 수임 권한을 부여하는 정책

다음 정책 예시는 AWS 계정 `AssumeRole`의 `UpdateApp` 역할을 위해 `123123123123`을 호출할 수 있는 권한을 부여합니다. `AssumeRole`을 사용하는 경우, 연합된 사용자를 대신해 보안 자격 증명을 생성하는 사용자(또는 애플리케이션)는 역할 권한 정책에 아직 지정되지 않은 어떤 권한도 위임할 수 없습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::123123123123:role/UpdateAPP"
  }]
}
```

Example : 연동 사용자를 위한 임시 보안 자격 증명을 생성할 수 있는 권한을 부여하는 정책

다음과 같은 정책 예시는 `GetFederationToken`에 액세스할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "sts:GetFederationToken",
    "Resource": "*"
  }]
}
```

> **Important**
>
> IAM 사용자에게 `GetFederationToken`을 사용해 연합된 사용자를 위한 임시 보안 자격 증명을 생성할 수 있는 권한을 부여하면 이로써 해당 사용자가 자신의 권한을 위임할 수 있게 허용하는 것이므로 주의하시기 바랍니다. 여러 IAM 사용자 및 AWS 계정에 걸쳐 권한을 위임하는 것에 대한

자세한 내용은 액세스 권한 위임을 위한 정책의 예 (p. 246) 단원을 참조하십시오. 임시 보안 자격 증명에서 권한을 제어하는 것에 대한 자세한 정보는 사용자 임시 보안 자격 증명에 대한 권한 제어 (p. 316) 단원을 참조하십시오.

Example : 연동 사용자에 대해 임시 보안 자격 증명을 생성할 수 있는 사용자 제한 권한을 부여하는 정책

IAM 사용자가 `GetFederationToken`을 호출하도록 허용할 때는 IAM 사용자가 위임할 수 있는 권한을 제한하는 것이 좋습니다. 예를 들어 다음 정책은 IAM 사용자가 이름이 Manager로 시작하는 연동 사용자에 대해서만 임시 보안 자격 증명을 생성하도록 허용하는 방법을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "sts:GetFederationToken",
    "Resource": ["arn:aws:sts::123456789012:federated-user/Manager*"]
  }]
}
```

AWS 리전에서 AWS STS 관리

기본적으로 AWS Security Token Service(AWS STS)는 글로벌 서비스로 사용 가능하고 모든 AWS STS 요청은 `https://sts.amazonaws.com`의 단일 엔드포인트로 전송됩니다. AWS는 지연 시간을 줄이고, 중복으로 구축하고, 세션 토큰 유효성을 높이려면 전역 엔드포인트 대신 리전별 AWS STS 엔드포인트를 사용할 것을 권장합니다.

- 지연 시간 감소 – 서비스 및 애플리케이션에서 지리적으로 더 가까운 엔드포인트에 AWS STS 호출을 함으로써 지연 시간 및 응답 시간을 단축하며 AWS STS 서비스에 액세스할 수 있습니다.
- 중복된 구축 – AWS STS API 호출을 다른 리전으로 전환하는 코드를 애플리케이션에 추가할 수 있습니다. 이를 통해 첫 번째 리전에서 응답이 중단되더라도 애플리케이션이 계속해서 작동합니다. 이러한 중복성은 자동으로 구축되지 않으므로 코드에 해당 기능을 구축해야 합니다.
- 세션 토큰 유효성 증가 – 리전별 AWS STS 엔드포인트의 세션 토큰은 모든 AWS 이전에서 유효합니다. 전역 STS 엔드포인트의 세션 토큰은 기본적으로 STS가 활성화된 AWS 리전에서만 유효합니다. 계정에 대해 새 리전을 활성화하려는 경우 리전별 STS 엔드포인트의 세션 토큰을 사용할 수 있습니다. 전역 엔드포인트를 사용하는 경우 전역 엔드포인트에 대한 STS 세션 토큰의 리전 호환성을 변경해야 합니다. 이를 통해 토큰이 모든 AWS 리전에서 유효합니다.

전역 엔드포인트 세션 토큰 관리

대부분의 AWS 리전은 기본적으로 모든 AWS 서비스의 작업이 활성화되어 있습니다. 이러한 리전은 AWS STS 사용이 자동으로 활성화됩니다. 아시아 태평양(홍콩)과 같은 일부 리전은 수동으로 활성화해야 합니다. AWS 리전 활성화 및 비활성화에 대한 자세한 내용은 AWS General Reference.의 AWS 리전 관리를 참조하십시오. 이러한 AWS 리전을 활성화할 때 자동으로 AWS STS 사용이 활성화됩니다. 비활성화된 리전에 대한 STS 엔드포인트를 활성화할 수는 없습니다. 모든 AWS 리전에서 유효한 토큰에는 기본적으로 활성화된 리전에서 유효한 토큰보다 더 많은 문자가 포함되어 있습니다. 이 설정을 변경하면 토큰을 임시로 저장한 기존 시스템에 영향을 미칠 수 있습니다.

AWS Management 콘솔, AWS CLI 또는 AWS API를 사용하여 이 설정을 변경할 수 있습니다.

전역 엔드포인트에 대한 세션 토큰의 리전 호환성 변경(콘솔)

1. 루트 사용자 또는 IAM 관리 작업을 수행할 권한이 있는 IAM 사용자로 로그인합니다. 세션 토큰의 호환성을 변경하려면 `iam:SetSecurityTokenServicePreferences` 작업을 허용하는 정책이 있어야 합니다.
2. IAM 콘솔을 엽니다. 탐색 창에서 계정 설정를 선택합니다.

3. 필요한 경우 Security Token Service (STS) 섹션을 확장합니다. 전역 엔드포인트 옆에 있는 첫 번째 표의 세션 토큰의 리전 호환성 열에 `Valid only in AWS Regions enabled by default`로 표시됩니다. 변경을 선택합니다.
4. 전역 엔드포인트에 대한 세션 토큰의 리전 호환성 변경 대화 상자에서 모든 AWS 리전에 유효함을 선택합니다. 변경 사항 저장을 선택합니다.

   Note

   모든 AWS 리전에서 유효한 토큰에는 기본적으로 활성화된 리전에서 유효한 토큰보다 더 많은 문자가 포함되어 있습니다. 이 설정을 변경하면 토큰을 임시로 저장한 기존 시스템에 영향을 미칠 수 있습니다.

전역 엔드포인트에 대한 세션 토큰의 리전 호환성 변경(AWS CLI)

보안 토큰 버전을 설정합니다. 버전 1 토큰은 기본적으로 이용 가능한 AWS 리전에서만 유효합니다. 이러한 토큰은 아시아 태평양(홍콩) 등과 같이 수동으로 활성화된 리전에서 작동하지 않습니다. 버전 2는 모든 리전에서 유효합니다. 하지만 버전 2 토큰에 포함된 문자가 더 많고 일시적으로 토큰을 저장하는 시스템에 영향을 미칠 수 있습니다.

- `aws iam set-security-token-service-preferences`

전역 엔드포인트에 대한 세션 토큰의 리전 호환성 변경(AWS API)

보안 토큰 버전을 설정합니다. 버전 1 토큰은 기본적으로 이용 가능한 AWS 리전에서만 유효합니다. 이러한 토큰은 아시아 태평양(홍콩) 등과 같이 수동으로 활성화된 리전에서 작동하지 않습니다. 버전 2는 모든 리전에서 유효합니다. 하지만 버전 2 토큰에 포함된 문자가 더 많고 일시적으로 토큰을 저장하는 시스템에 영향을 미칠 수 있습니다.

- `SetSecurityTokenServicePreferences`

AWS 리전에서 AWS STS 활성화 및 비활성화

리전에 대한 STS 엔드포인트를 활성화할 때 AWS STS에서 AWS STS 요청을 수행하는 계정의 사용자 및 역할에 임시 자격 증명을 발급할 수 있습니다. 이러한 자격 증명은 기본적으로 활성화되었거나 수동으로 활성화된 모든 리전에서 사용할 수 있습니다. 임시 자격 증명이 생성된 계정의 리전을 활성화해야 합니다. 요청 시 사용자가 동일한 계정으로 로그인하거나 각기 다른 계정으로 로그인하는지 여부는 중요하지 않습니다.

예를 들어, 계정 A의 사용자가 STS 리전 엔드포인트 `https://sts.us-west-2.amazonaws.com`으로 `sts:AssumeRole` API 요청을 보내려 할 수 있습니다. 이는 계정 B의 `Developer` 역할에 대한 임시 자격 증명을 요청하기 위한 것입니다. 이 요청은 계정 B의 엔터티에 대한 자격 증명을 만들기 위한 것이기 때문에 계정 B는 `us-west-2` 리전을 활성화해야 합니다. 계정 A(또는 다른 계정)의 사용자는 자신의 계정에서 리전이 활성화되었는지 여부와 상관없이 `us-west-2` 엔드포인트를 호출하여 계정 B의 자격 증명을 요청할 수 있습니다.

Note

활성 리전은 해당 계정의 임시 자격 증명을 이용하는 모두가 이용할 수 있습니다. 어떤 IAM 사용자 또는 역할이 리전에 액세스할 수 있는지 여부를 제어하려면 권한 정책에서 `aws:RequestedRegion` (p. 658) 조건 키를 사용합니다.

기본적으로 활성화된 리전에서 AWS STS 활성화 또는 비활성화(콘솔)

1. 루트 사용자 또는 IAM 관리 작업을 수행할 권한이 있는 IAM 사용자로 로그인합니다.
2. IAM 콘솔을 열고 탐색 창에서 계정 설정을 선택합니다.
3. 필요한 경우 Security Token Service (STS) 목록을 확장하고, 활성화할 리전을 찾은 다음 활성화 또는 비활성화를 선택합니다. 아시아 태평양(홍콩) 리전과 같은 일부 리전은 기본적으로 활성화되지 않습니다. 이 경우 리전을 수동으로 활성화할 때 STS가 자동으로 활성화됩니다. 이후로 AWS STS는 이러한 리전

에서 항상 활성 상태가 되고 비활성화할 수 없습니다. 리전을 수동으로 활성화하는 방법을 알아보려면 AWS General Reference의 AWS 리전 관리를 참조하십시오.

AWS STS 리전 사용을 위한 코드 작성

리전을 활성화한 후에 AWS STS API 호출을 그 리전으로 보낼 수 있습니다. 다음 Java 코드 조각은 `AWSSecurityTokenServiceClient` 객체를 구성해 `setEndpoint` 메서드로 유럽(아일랜드)(eu-west-1) 리전으로 요청하는 방법을 보여줍니다.

```
EndpointConfiguration regionEndpointConfig = new EndpointConfiguration("https://sts.eu-
west-1.amazonaws.com", "eu-west-1");
AWSSecurityTokenService stsRegionalClient = AWSSecurityTokenServiceClientBuilder.standard()
.withCredentials(credentials)
.withEndpointConfiguration(regionEndpointConfig)
.build();
```

AWS STS에서는 `setRegion` 및 `setEndpoint` 메서드를 모두 사용하여 리전별 엔드포인트에 호출할 것을 권장합니다. 아시아 태평양(홍콩)과 같이 수동으로 활성화된 리전의 경우 `setRegion` 메서드만을 사용할 수 있습니다. 이 경우 호출은 STS 리전 엔드포인트로 전달됩니다. 리전을 수동으로 활성화하는 방법을 알아보려면 AWS General Reference의 AWS 리전 관리를 참조하십시오. 기본적으로 활성화된 리전에 대해 `setRegion` 메서드를 사용하는 경우 호출은 `https://sts.amazonaws.com`의 전역 엔드포인트로 전달됩니다.

예제의 첫 번째 줄에서 `AWSSecurityTokenServiceClient`라는 `stsClient` 객체를 인스턴스화합니다. 두 번째 줄에서는 `stsClient` 메서드를 호출하고 엔드포인트의 URL을 유일한 파라미터로 전달하여 `setEndpoint` 객체를 구성합니다. `stsClient` 객체를 사용하는 모든 API 호출은 이제 지정된 엔드포인트로 전송됩니다.

다른 모든 언어 및 프로그래밍 환경의 조합에 대해서는 해당 SDK 문서를 참조하십시오.

리전 엔드포인트

다음 표에서는 해당 리전과 그 엔드포인트를 나열합니다. 기본적으로 어떤 것들이 활성화되며, 어떤 것을 활성화 또는 비활성화할 수 있는지를 보여줍니다.

리전 이름	엔드포인트	기본 활성화	활성화/비활성화 가능
--전역--	sts.amazonaws.com	예	아니요
미국 동부(오하이오)	sts.us-east-2.amazonaws.com	예	예
미국 동부(버지니아 북부)	sts.us-east-1.amazonaws.com	예	아니요
미국 서부(캘리포니아 북부 지역)	sts.us-west-1.amazonaws.com	예	예
미국 서부(오레곤)	sts.us-west-2.amazonaws.com	예	예
캐나다(중부)	sts.ca-central-1.amazonaws.com	예	예
아시아 태평양(도쿄)	sts.ap-northeast-1.amazonaws.com	예	예
아시아 태평양(서울)	sts.ap-northeast-2.amazonaws.com	예	예
아시아 태평양(뭄바이)	sts.ap-south-1.amazonaws.com	예	예

리전 이름	엔드포인트	기본 활성화	활성화/비활성화 가능
아시아 태평양(싱가포르)	sts.ap-southeast-1.amazonaws.com	예	예
아시아 태평양(시드니)	sts.ap-southeast-2.amazonaws.com	예	예
아시아 태평양(홍콩)	sts.ap-east-1.amazonaws.com	아니요(리전 활성화 전까지)	아니요
중동(바레인)	sts.me-south-1.amazonaws.com	아니요(리전 활성화 전까지)	아니요
유럽(프랑크푸르트)	sts.eu-central-1.amazonaws.com	예	예
유럽(아일랜드)	sts.eu-west-1.amazonaws.com	예	예
유럽(런던)	sts.eu-west-2.amazonaws.com	예	예
유럽(파리)	sts.eu-west-3.amazonaws.com	예	예
유럽(스톡홀름)	sts.eu-north-1.amazonaws.com	예	예
남아메리카(상파울루)	sts.sa-east-1.amazonaws.com	예	예

Note

`us-east-2.amazonaws.com`과 같은 리전 엔드포인트에 대한 호출은 리전 서비스에 대한 모든 호출과 마찬가지로 AWS CloudTrail에서 로깅됩니다. 전역적 엔드포인트 `sts.amazonaws.com`에 대한 호출은 글로벌 서비스에 대한 호출로 로깅됩니다. 자세한 내용은 AWS CloudTrail을 사용하여 IAM 및 AWS STS API 호출 로깅 (p. 334) 단원을 참조하십시오.

AWS STS 인터페이스 VPC 엔드포인트 사용

Amazon Virtual Private Cloud(Amazon VPC)를 사용하여 AWS 리소스를 호스팅하는 경우, VPC와 AWS STS 간에 프라이빗 연결을 설정할 수 있습니다. 이 연결을 사용하면 AWS STS가 퍼블릭 인터넷을 통하지 않고 VPC의 리소스와 통신하게 할 수 있습니다.

Amazon VPC란 사용자가 정의한 가상 네트워크에서 AWS 리소스를 시작할 때 사용할 수 있는 AWS 서비스입니다. VPC를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC를 AWS STS에 연결하려면 AWS STS에 대해 인터페이스 VPC 엔드포인트를 정의하십시오. 이 엔드포인트를 이용하면 인터넷 게이트웨이나 NAT(네트워크 주소 변환) 인스턴스 또는 VPN 연결 없이도 AWS STS에 안정적이고 확장 가능하게 연결됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC란 무엇입니까?를 참조하십시오.

인터페이스 VPC 엔드포인트는 프라이빗 IP 주소와 함께 탄력적 네트워크 인터페이스를 사용하여 AWS 서비스 간 프라이빗 통신을 사용할 수 있는 AWS 기술인 AWS PrivateLink에 의해 구동됩니다. 자세한 내용은 AWS 서비스를 위한 AWS PrivateLink를 참조하십시오.

다음은 Amazon VPC 사용자를 위한 단계들입니다. 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC 시작하기를 참조하십시오.

가용성

현재 AWS STS가 VPC 엔드포인트를 지원하는 리전은 다음과 같습니다.

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(캘리포니아 북부 지역)
- 미국 서부(오레곤)
- 아시아 태평양(홍콩)
- 중동(바레인)
- 아시아 태평양(뭄바이)
- 아시아 태평양(오사카-로컬)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 캐나다(중부)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(파리)
- 유럽(스톡홀름)
- 남아메리카(상파울루)

AWS STS에 대한 VPC 만들기

VPC에서 AWS STS를 사용하기 시작하려면 AWS STS에 대한 인터페이스 VPC 엔드포인트를 생성합니다. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 만들기를 참조하십시오.

VPC 엔드포인트를 만든 후 해당 리전의 엔드포인트를 사용하여 AWS STS 요청을 보내야 합니다. AWS STS에서는 `setRegion` 및 `setEndpoint` 메서드를 모두 사용하여 리전 엔드포인트에 호출할 것을 권장합니다. 아시아 태평양(홍콩)과 같이 수동으로 활성화된 리전의 경우 `setRegion` 메서드만을 사용할 수 있습니다. 이 경우 호출은 STS 리전 엔드포인트로 전달됩니다. 리전을 수동으로 활성화하는 방법을 알아보려면 AWS General Reference의 AWS 리전 관리를 참조하십시오. 기본적으로 활성화된 리전에 대해 `setRegion` 메서드를 사용하는 경우 호출은 `https://sts.amazonaws.com`의 전역 엔드포인트로 전달됩니다.

리전의 엔드포인트를 사용할 경우, AWS STS는 퍼블릭 엔드포인트 또는 프라이빗 인터페이스 VPC 엔드포인트 중 사용 중인 엔드포인트를 사용하여 다른 AWS 서비스를 호출합니다. 예를 들어 AWS STS를 위한 인터페이스 VPC 엔드포인트를 만들어 VPC에 있는 리소스의 AWS STS의 임시 자격 증명을 이미 요청한 경우를 예로 들어 보겠습니다. 이 경우 이러한 자격 증명은 기본적으로 인터페이스 VPC 엔드포인트를 통합니다. AWS STS 사용을 통한 리전 요청에 대한 자세한 내용은 AWS 리전에서 AWS STS 관리 (p. 326) 단원을 참조하십시오.

임시 자격 증명을 사용하는 샘플 애플리케이션

AWS Security Token Service(AWS STS)를 사용하면 AWS 리소스에 대한 액세스를 제어할 수 있는 임시 보안 자격 증명을 생성하여 신뢰받는 사용자에게 제공할 수 있습니다. AWS STS에 대한 자세한 내용은 임시 보안 자격 증명 (p. 302) 단원을 참조하십시오. AWS STS를 사용해 임시 보안 자격 증명을 관리하는 방법에 대해 알아보려면, 완전한 샘플 시나리오를 구현하는 다음과 같은 샘플 애플리케이션을 다운로드하십시오.

- Active Directory 사용 사례를 위한 자격 증명 연동 샘플 애플리케이션 Active Directory(.NET/C#)에서 정의된 사용자에 연결된 권한을 사용해 Amazon S3 파일 및 버킷에 액세스하기 위한 임시 보안 자격 증명을 발급하는 방법을 보여줍니다.

- AWS Management Console 연동 프록시 샘플 사용 사례 Single-Sign-On(SSO)을 가능케 하는 사용자 지정 연동 프록시를 생성해 기존 Active Directory 사용자가 AWS Management 콘솔에 로그인할 수 있게 하는 방법을 보여줍니다(.NET/C#).
- Shibboleth를 AWS Identity and Access Management와 통합하기 Shibboleth 및 SAML (p. 188)을 사용해 사용자에게 AWS Management 콘솔에 대한 SSO(Single-Sign-On) 액세스 권한을 제공하는 방법을 보여줍니다.

웹 자격 증명 연동에 대한 예시

다음 샘플 애플리케이션은 Login with Amazon, Amazon Cognito, Facebook 또는 Google 같은 공급자를 통해 웹 자격 증명 연동을 사용하는 방법을 보여 줍니다. 이러한 임시 AWS 보안 자격 증명에 대해 이러한 공급자의 인증을 얻고 AWS 서비스에 액세스할 수 있습니다.

- Amazon Cognito 자습서 – 모바일 개발용 AWS SDK를 통해 Amazon Cognito를 사용하는 것이 좋습니다. Amazon Cognito는 모바일 앱을 위한 자격 증명을 관리하는 가장 간단한 방법으로서, 동기화 및 교차 디바이스 자격 증명과 같은 부가 기능을 제공합니다. Amazon Cognito에 대한 자세한 내용은 Android용 AWS Mobile SDK Developer Guide의 Amazon Cognito 자격 증명 및 AWS Mobile SDK for iOS Developer Guide의 Amazon Cognito 자격 증명을 사용한 사용자 인증 단원을 참조하십시오.
- Web Identity Federation Playground. 이 웹 사이트는 웹 자격 증명 연동 (p. 183) 및 `AssumeRoleWithWebIdentity` API를 대화식으로 보여줍니다.
- AWS Elastic Beanstalk 및 Login with Amazon을 사용한 연동 웹 자격 증명 애플리케이션 구축 및 배포 이 블로그 게시글은 `AssumeRoleWithWebIdentity`를 사용해 웹 자격 증명 연동 및 Login with Amazon을 통해 임시 보안 자격 증명을 얻는 방법을 기술합니다. 또한, Elastic Beanstalk에서 실행되는 Python 웹 애플리케이션에서 그 자격 증명을 사용해 AWS를 호출하는 방법을 설명합니다.

임시 보안 자격 증명에 관한 추가 리소스

다음 시나리오 및 애플리케이션은 임시 보안 자격 증명 사용 방법을 안내합니다.

- 웹 자격 증명 연동에 대하여 (p. 183). 이 섹션에서는 웹 자격 증명 연동 및 `AssumeRoleWithWebIdentity` API를 사용할 때 IAM 역할을 구성하는 방법을 설명합니다.
- MFA 보호 API 액세스 구성 (p. 146). 이 주제는 역할을 사용해 멀티 팩터 인증(MFA)이 계정에서 민감한 API 작업을 보호하도록 요구하는 방법을 설명합니다.
- 자격 증명 등록을 위한 토큰 벤딩 머신. 이 샘플 Java 웹 애플리케이션은 `GetFederationToken` API를 사용해 원격 클라이언트에게 임시 보안 자격 증명을 제공합니다.

AWS의 정책 및 권한에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 액세스 관리 (p. 348)
- 정책 평가 로직 (p. 622).
- Amazon Simple Storage Service 개발자 가이드의 Amazon S3 리소스에 대한 액세스 권한 관리.
- 해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

AWS 계정 루트 사용자

Amazon Web Services(AWS) 계정을 처음 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 Single Sign-In 자격 증명으로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다.

Important

일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 마십시오. 대신, IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례 (p. 61)를 준수합니다. 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 작업을 수행할 때만 사용합니다. 루트 사용자로 로그인해야 하는 작업을 보려면 루트 사용자가 필요한 AWS 작업을 참조하십시오. 일상적 사용을 위해 관리자를 설정하는 방법에 대한 자습서는 첫 번째 IAM 관리자 및 그룹 생성 (p. 20) 단원을 참조하십시오.

AWS 계정 루트 사용자에 대한 액세스 키(액세스 키 ID 및 보안 액세스 키)를 생성, 교체, 비활성화 또는 삭제할 수 있습니다. 루트 사용자 암호를 변경할 수도 있습니다. AWS 계정에 대한 루트 사용자 자격 증명을 보유한 사람은 누구든지 결제 정보를 포함하여 해당 계정의 모든 리소스에 무제한으로 액세스할 수 있습니다.

액세스 키를 만들 때 액세스 키 ID와 보안 액세스 키를 한 세트로 생성합니다. 액세스 키 생성 중에 AWS는 액세스 키의 보안 액세스 키 부분을 확인하고 다운로드할 기회를 한 번 부여합니다. 보안 액세스 키를 다운로드하지 않았거나 분실한 경우 액세스 키를 삭제한 다음 새로 생성할 수 있습니다. IAM콘솔, AWS CLI 또는 AWS API를 사용해 루트 사용자 액세스 키를 생성할 수 있습니다.

새로 생성한 액세스 키는 활성 상태입니다. 즉, CLI 및 API 호출에 대해 액세스 키를 사용할 수 있습니다. 각 IAM 사용자에 대한 액세스 키는 두 개로 제한됩니다. 이는 액세스 키를 교체하려는 경우에 유용합니다. 또한 루트 사용자에 최대 두 개의 액세스 키를 할당할 수 있습니다. 액세스 키를 비활성화한 경우 API 호출에 액세스 키를 사용할 수 없으며, 비활성 키는 제한에 포함됩니다. 언제든지 액세스 키를 생성하거나 삭제할 수 있습니다. 그러나 액세스 키를 삭제하면 영구 삭제되어 되돌릴 수 없습니다.

보안 자격 증명 페이지에서 이메일 주소 및 암호를 변경할 수 있습니다. 또한 AWS 로그인 페이지에서 Forgot password?(암호 찾기)를 선택하여 암호를 재설정할 수 있습니다.

주제

- AWS 계정 루트 사용자의 MFA 활성화 (p. 332)
- 루트 사용자를 위한 액세스 키 생성 (p. 332)
- 루트 사용자로부터 액세스 키 삭제하기 (p. 333)
- 루트 사용자의 암호 변경 (p. 334)

AWS 계정 루트 사용자의 MFA 활성화

루트 사용자 자격 증명을 계속 사용할 경우, 보안 모범 사례에 따라 계정에 대한 멀티 팩터 인증(MFA)을 활성화하는 것이 좋습니다. 루트 사용자는 계정에서 민감한 작업을 수행할 수 있기 때문에 인증 단계를 추가하면 계정의 보안을 강화하는 데 도움이 됩니다. 여러 유형의 MFA가 있습니다. MFA 활성화에 대한 자세한 내용은 다음을 참조하십시오.

- AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) (p. 123)
- AWS 계정 루트 사용자용 하드웨어 MFA 디바이스 활성화(콘솔) (p. 133)

루트 사용자를 위한 액세스 키 생성

AWS Management 콘솔 또는 AWS 프로그래밍 도구를 사용하여 루트 사용자에 대한 액세스 키를 생성할 수 있습니다.

AWS 계정 루트 사용자에 대한 액세스 키를 생성하려면(콘솔 사용)

1. AWS 계정 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 AWS 계정 루트 사용자로 로그인합니다.

Note

텍스트 상자가 세 개 표시되면 이전에 IAM 사용자 자격 증명으로 콘솔에 로그인한 것입니다. 브라우저에서 이 기본 설정을 기억하고 로그인할 때마다 이 계정별 로그인 페이지를 열 수 있습니다. IAM 사용자 로그인 페이지에서는 계정 소유자로 로그인할 수 없습니다. IAM 사용자 로그인 페이지가 표시되면 페이지 하단에 있는 Sign in using 루트 사용자 email(이메일을 사용하여 로그인)을 선택하여 기본 로그인 페이지로 돌아갑니다. 기본 로그인 페이지에서 AWS 계정 이메일 주소와 암호를 입력하여 루트 사용자로 로그인합니다.

2. 탐색 표시줄에서 계정 이름을 선택한 다음 내 보안 자격 증명을 선택합니다.
3. AWS 계정의 보안 자격 증명에 대한 액세스와 관련해 경고가 나타나면, Continue to Security Credentials(보안 자격 증명으로 계속)을 선택하십시오.
4. Access keys(access key ID and secret access key)(액세스 키(액세스 키 ID 및 보안 액세스 키)) 섹션을 확장합니다.
5. Create New Access Key(새 액세스 키 생성)을 선택하십시오. 이 기능이 비활성화되면 새 키를 생성할 수 있기 전에 기존 액세스 키 중 하나를 삭제해야 합니다. 자세한 내용은 IAM 사용 설명서의 IAM 엔터티 객체 제한을 참조하십시오.

   보안 액세스 키를 보거나 다운로드할 수 있는 기회는 이번 한 번뿐이라는 경고가 표시됩니다. 나중에는 조회할 수 없습니다.

   - Show Access Key(액세스 키 표시)를 선택하면 브라우저 창에서 액세스 키 ID 및 보안 키를 복사해 다른 곳에 붙여넣기할 수 있습니다.
   - Download Key File(키 파일 다운로드)을 선택하면 액세스 키 ID 및 보안 키가 저장된 `rootkey.csv`라는 이름의 파일을 받게 됩니다. 파일을 안전한 곳에 저장합니다.
6. 액세스 키를 더 이상 사용하지 않을 때는 오용되지 않도록 삭제하거나 (p. 65) Make Inactive(비활성화)를 선택하여 비활성 상태로 표시할 것을 권합니다.

루트 사용자에 대한 액세스 키(AWS CLI 또는 AWS API)를 생성하려면

다음 중 하나를 사용하십시오.

- AWS CLI: aws iam create-access-key
- AWS API: CreateAccessKey

루트 사용자로부터 액세스 키 삭제하기

AWS Management 콘솔 또는 다양한 프로그래밍 도구를 사용하여 루트 사용자에 대한 액세스 키를 삭제할 수 있습니다.

AWS 계정 루트 사용자(콘솔)에서 액세스 키를 삭제하려면

1. AWS 계정 이메일 주소와 암호를 사용하여 AWS Management 콘솔에 AWS 계정 루트 사용자로 로그인합니다.

   Note

   텍스트 상자가 세 개 표시되면 이전에 IAM 사용자 자격 증명으로 콘솔에 로그인한 것입니다. 브라우저에서 이 기본 설정을 기억하고 로그인할 때마다 이 계정별 로그인 페이지를 열 수 있습니다. IAM 사용자 로그인 페이지에서는 계정 소유자로 로그인할 수 없습니다. IAM 사용자 로그인 페이지가 표시되면 페이지 하단에 있는 Sign in using 루트 사용자 email(이메일을 사용하여 로그인)을 선택하여 기본 로그인 페이지로 돌아갑니다. 기본 로그인 페이지에서 AWS 계정 이메일 주소와 암호를 입력하여 루트 사용자로 로그인합니다.
2. 탐색 표시줄에서 계정 이름을 선택한 다음 내 보안 자격 증명을 선택합니다.

3. AWS 계정의 보안 자격 증명에 대한 액세스와 관련해 경고가 나타나면, Continue to Security Credentials(보안 자격 증명으로 계속)을 선택하십시오.
4. Access keys(access key ID and secret access key)(액세스 키(액세스 키 ID 및 보안 액세스 키)) 섹션을 확장합니다.
5. 삭제하고자 하는 액세스 키를 찾은 다음, 작업 열에서 삭제를 선택합니다.

   Note

   액세스 키를 삭제하는 대신에 비활성 상태로 표시할 수 있습니다. 이렇게 하면 키 ID나 보안 키를 변경하지 않고도 나중에 액세스 키를 다시 사용할 수 있습니다. 비활성 상태에 있는 동안에는 AWS API에 대한 요청을 통해 액세스 키를 사용하려는 시도는 액세스 거부 상태로 인해 실패합니다.

루트 사용자에 대한 액세스 키(AWS CLI 또는 AWS API)를 삭제하려면

다음 중 하나를 사용하십시오.

- AWS CLI: aws iam delete-access-key
- AWS API: DeleteAccessKey

루트 사용자의 암호 변경

루트 사용자의 암호 변경에 대한 자세한 내용은 AWS 계정 루트 사용자 암호 변경 (p. 100) 단원을 참조하십시오. 루트 사용자를 변경하려면 루트 사용자 자격 증명을 사용하여 로그인해야 합니다. 루트 사용자로 로그인해야 하는 작업을 보려면 루트 사용자가 필요한 AWS 작업을 참조하십시오.

AWS CloudTrail을 사용하여 IAM 및 AWS STS API 호출 로깅

IAM 및 AWS STS은 IAM 사용자 또는 역할이 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail는 콘솔과 API 호출에서 오는 호출을 비롯하여 IAM 및 AWS STS에 대한 모든 API 호출을 이벤트로 캡처합니다. 추적을 생성하면 Amazon S3 버킷으로 CloudTrail 이벤트를 지속적으로 배포하도록 할 수 있습니다. 추적을 구성하지 않은 경우 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수도 있습니다. CloudTrail를 사용하여 IAM 또는 AWS STS에 요청한 내용의 정보를 얻을 수 있습니다. 예를 들어 어떤 IP 주소에서 요청했는지, 누가 요청했는지, 언제 생성되었는지 등 추가적인 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail User Guide을 참조하십시오.

주제

CloudTrail의 IAM 및 AWS STS 정보

CloudTrail은 계정 생성 시 AWS 계정에서 활성화됩니다. IAM 또는 AWS STS에서 활동이 수행되면 해당 활동은 이벤트 기록에서 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록에서 이벤트 보기를 참조하십시오.

IAM 및 AWS STS 이벤트를 비롯하여 AWS 계정의 이벤트 기록을 보유하려면 추적을 생성하십시오. 추적은 CloudTrail이 Amazon S3 버킷으로 로그 파일을 전송할 수 있도록 합니다. 콘솔에서 추적을 생성하면 기본적으로 모든 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

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

모든 IAM 및 AWS STS 작업은 CloudTrail에서 로깅되고 IAM API Reference 및 AWS Security Token Service API Reference에 기록됩니다.

IAM 및 AWS STS API 요청 로깅

CloudTrail은 인증된 모든 API 요청(자격 증명으로 생성)을 IAM 및 AWS STS API 작업에 기록합니다. CloudTrail은 인증되지 않은 요청을 AWS STS 작업, `AssumeRoleWithSAML` 및 `AssumeRoleWithWebIdentity`에 기록하고 자격 증명 공급자가 제공한 정보를 기록합니다. 이 정보를 사용하여 위임된 역할을 지닌 연동 사용자의 호출을 외부 연동 호출자에 다시 매핑할 수 있습니다. `AssumeRole`의 경우, 호출을 원래 AWS 서비스 또는 원래 사용자의 계정에 다시 매핑할 수 있습니다. CloudTrail 로그 항목에 있는 JSON 데이터의 `userIdentity` 섹션에는 특정 연동 사용자에게 AssumeRole* 요청을 매핑하는 데 필요한 정보가 들어 있습니다. 자세한 내용은 AWS CloudTrail User Guide의 CloudTrail userIdentity 요소를 참조하십시오.

예를 들어 IAM `CreateUser`, `DeleteRole`, `ListGroups` 및 기타 API 작업에 대한 호출은 모두 CloudTrail에 로깅됩니다.

이러한 유형의 로그 항목에 대한 예시는 이번 주제의 뒷 부분에 제시됩니다.

> **Important**
>
> 임의 리전에서 기본 글로벌 엔드포인트가 아닌 AWS STS 엔드포인트를 활성화할 경우에는 해당 리전의 CloudTrail 로깅 기능도 함께 활성화합니다. 이것은 해당 리전에서 수행된 AWS STS API 호출을 기록하는 데 필요합니다. 자세한 정보는 AWS CloudTrail User Guide의 Turning On CloudTrail in Additional Regions(추가 리전에서 CloudTrail 설정) 단원을 참조하십시오.

다른 AWS 서비스에 대한 API 요청 로깅

다른 AWS 서비스 API 작업에 대해 인증된 요청은 CloudTrail에 로깅되며, 이 로그 항목에는 요청자에 대한 정보가 저장됩니다.

예를 들어 Amazon EC2 인스턴스 나열 요청을 했거나 CodeDeploy 배포 그룹을 생성했다고 가정해 보십시오. 요청한 사람이나 서비스에 대한 세부 내용은 그 요청의 로그 항목에 들어 있습니다. 이 정보로 AWS 계정 루트 사용자, IAM 사용자, 역할, 또는 다른 AWS 서비스에 의한 요청인지 판단할 수 있습니다.

CloudTrail 로그 항목의 사용자 자격 증명 정보에 대한 자세한 정보는 AWS CloudTrail User Guide의 userIdentity Element 단원을 참조하십시오.

리전별 로그인 이벤트 로깅

CloudTrail에서 로그인 이벤트를 사용자 로그에 기록하도록 설정할 경우 CloudTrail에서 이벤트를 기록할 위치를 어떻게 선택하는지 잘 이해할 필요가 있습니다.

- 사용자가 콘솔에 직접 로그인할 경우 전역 또는 리전 로그인 엔드포인트로 리디렉션됩니다. 이 엔드포인트는 선택한 서비스 콘솔이 리전을 지원하는지 여부를 기준으로 합니다. 예를 들어 기본 콘솔 홈 페이지는 리전을 지원합니다. https://alias.signin.aws.amazon.com/console에 로그인하는 경우 https://us-east-2.signin.aws.amazon.com 같은 리전 로그인 엔드포인트로 리디렉션됩니다. 이 리디렉션은 사용자의 리전 로그에 리전별 CloudTrail 로그 항목을 생성합니다.

  반면 Amazon S3 콘솔은 리전을 지원하지 않으므로 https://alias.signin.aws.amazon.com/console/s3에 로그인할 경우 AWS에서 글로벌 로그인 엔드포인트 https://signin.aws.amazon.com으로 리디렉션합니다. 이 리디렉션은 글로벌 CloudTrail 로그 항목을 생성합니다.
- https://alias.signin.aws.amazon.com/console?region=ap-southeast-1 같은 URL을 사용하여 리전이 활성화된 메인 콘솔 홈 페이지에 로그인하면 특정 리전 로그인 엔드포인트를 수동으로 요청할 수 있습니다. 이 경우 AWS가 사용자를 `ap-southeast-1` 리전 로그인 엔드포인트로 리디렉션하고 리전 CloudTrail 로그 이벤트가 발생합니다.

로그인 이벤트가 리전 또는 글로벌 이벤트인지 여부는 사용자가 로그인하는 콘솔과 사용자가 로그인 URL을 구성하는 방식에 따라 다릅니다.

- 서비스 콘솔이 리전화되어 있습니까? 그럴 경우 로그인 요청이 리전 로그인 종단점으로 자동으로 리디렉션되고 이벤트가 해당 리전의 CloudTrail 로그에 기록됩니다. 예를 들어 리전화된 https://*alias*.signin.aws.amazon.com/console에 로그인하는 경우 https://us-east-2.signin.aws.amazon.com 같은 리전 로그인 엔드포인트로 리디렉션됩니다. 이벤트는 해당 리전의 로그에 기록됩니다.

  하지만 일부 서비스는 아직 리전화되어 있지 않습니다. 예를 들어 Amazon S3 서비스가 현재 리전화되지 않았습니다 . https://*alias*.signin.aws.amazon.com/console/s3에 로그인하는 경우 https://signin.aws.amazon.com과 같은 전역 로그인 엔드포인트로 리디렉션됩니다. 이 리디렉션은 글로벌 로그에 이벤트를 생성합니다.
- https://*alias*.signin.aws.amazon.com/console?region=ap-southeast-1과 같은 URL을 사용하여 특정 리전 로그인 엔드포인트를 수동으로 요청할 수도 있습니다. 이 URL은 `ap-southeast-1` 리전 로그인 엔드포인트로 리디렉션됩니다. 이 리디렉션은 리전 로그에 이벤트를 생성합니다.

중복 리전 로그 항목 방지

CloudTrail은 각 리전마다 별도로 추적을 생성합니다. 이러한 추적에는 해당 리전에서 발생하는 이벤트에 대한 정보와 리전별로 적용되지 않은 이벤트 및 전역 이벤트에 대한 정보가 포함됩니다. IAM API 호출, 전역 엔드포인트에 대한 AWS STS 호출, AWS 로그인 이벤트 등이 있습니다. 예를 들어, 한 리전에 두 개의 추적이 있다고 가정하겠습니다. 그런 다음 IAM 사용자를 새로 생성할 경우 `CreateUser` 이벤트가 두 리전의 로그 파일에 추가되어 로그 항목이 중복되고 맙니다.

STS(AWS Security Token Service)는 https://sts.amazonaws.com에 단일 전역 엔드포인트가 있는 전역 서비스입니다. 따라서 이 엔드포인트에 대한 호출은 글로벌 서비스에 대한 호출로 로깅됩니다. 하지만 이 엔드포인트가 물리적으로 미국 동부(버지니아 북부) 리전에 위치하기 때문에 로그가 표시되는 이벤트 리전 역시 us-east-1이 됩니다. 이때는 해당 리전에 전역 서비스 로그를 포함하도록 선택해야만 CloudTrail이 이 로그를 미국 동부(오하이오) 리전에 기록합니다. AWS STS는 `sts.eu-central-1.amazonaws.com`과 같은 리전 엔드포인트에 대한 호출도 허용합니다. CloudTrail은 모든 리전의 엔드포인트 호출을 각 리전으로 기록합니다. 예를 들어 `sts.us-east-2.amazonaws.com`에 대한 호출은 미국 동부(오하이오) 리전에 게시됩니다. `sts.eu-central-1.amazonaws.com`에 대한 호출은 유럽(프랑크푸르트) 리전 로그에 게시됩니다.

여러 리전 및 AWS STS에 대한 자세한 정보는 AWS 리전에서 AWS STS 관리 (p. 326) 단원을 참조하십시오.

아래는 각 리전을 비롯해 리전에 따른 CloudTrail의 AWS STS 요청 로깅 방식을 나타낸 표입니다. "위치" 열은 CloudTrail이 기록하는 로그를 나타냅니다. "전역"은 전역 서비스 로그를 추가하도록 선택한 모든 리전에 이벤트가 로깅된다는 것을 의미합니다. 그리고, "리전"은 엔드포인트가 위치한 리전에만 이벤트가 로깅된다는 것을 의미합니다. 마지막 열은 로그 항목에서 요청 리전의 식별 방식을 나타냅니다.

리전 이름	CloudTrail 로그의 리전 자격 증명	엔드포인트	CloudTrail 로그 위치
해당 사항 없음 - 글로벌	us-east-1	sts.amazonaws.com	전 세계
미국 동부(오하이오)	us-east-2	sts.us-east-2.amazonaws.com	Region
미국 동부(버지니아 북부)	us-east-1	sts.us-east-1.amazonaws.com	Region
미국 서부(캘리포니아 북부 지역)	us-west-1	sts.us-west-1.amazonaws.com	Region
미국 서부(오레곤)	us-west-2	sts.us-west-2.amazonaws.com	Region
캐나다(중부)	ca-central-1	sts.ca-central-1.amazonaws.com	Region
유럽(프랑크푸르트)	eu-central-1	sts.eu-central-1.amazonaws.com	Region
유럽(아일랜드)	eu-west-1	sts.eu-west-1.amazonaws.com	Region
유럽(런던)	eu-west-2	sts.eu-west-2.amazonaws.com	Region
아시아 태평양(도쿄)	ap-northeast-1	sts.ap-northeast-1.amazonaws.com	Region
아시아 태평양(서울)	ap-northeast-2	sts.ap-northeast-2.amazonaws.com	Region
아시아 태평양(뭄바이)	ap-south-1	sts.ap-south-1.amazonaws.com	Region
아시아 태평양(싱가포르)	ap-southeast-1	sts.ap-southeast-1.amazonaws.com	Region
아시아 태평양(시드니)	ap-southeast-2	sts.ap-southeast-2.amazonaws.com	Region
남아메리카(상파울루)	sa-east-1	sts.sa-east-1.amazonaws.com	Region

계정 내 다양한 리전의 추적 정보를 단일 Amazon S3 버킷으로 통합하도록 CloudTrail을 구성할 경우, IAM 이벤트가 로그에 중복 저장됩니다. 즉, 각 리전의 추적이 동일한 IAM 이벤트를 통합 로그에 기록합니다. 이러한 중복 문제를 해결하기 위해 글로벌 이벤트를 선택적으로 추가할 수 있습니다. 일반적인 접근 방식은 하나의 추적에서 전역 이벤트를 활성화하는 것입니다. 그런 다음 동일한 Amazon S3 버킷에 쓰는 다른 모든 추적에서 전역 이벤트를 비활성화합니다. 이렇게 하면 글로벌 이벤트는 항상 한 곳에만 기록됩니다.

자세한 정보는 AWS CloudTrail User Guide의 Aggregating Logs 단원을 참조하십시오.

사용자 로그인 이벤트 로깅

CloudTrail에서는 로그인 이벤트를 AWS Management 콘솔, AWS 토론 포럼 및 AWS Marketplace에 기록합니다. CloudTrail은 IAM 사용자 및 연동 사용자에 대해 성공 및 실패한 로그인 시도를 기록합니다.

AWS 계정 루트 사용자의 경우 성공적인 로그인 이벤트만 기록됩니다. 단, 루트 사용자의 로그인 이벤트는 CloudTrail에 로깅되지 않습니다.

보안 모범 사례의 일환으로 AWS는 잘못된 사용자 이름으로 인해 로그인에 실패하더라도 입력한 IAM 사용자 이름 텍스트를 기록하지 않습니다. 사용자 이름 텍스트는 `HIDDEN_DUE_TO_SECURITY_REASONS` 값으로 마스킹 처리됩니다. 마스킹 처리의 예는 이번 주제 후반부의 잘못된 사용자 이름으로 인한 로그인 실패 이벤트 예제 (p. 346) 단원을 참조하십시오. 이러한 오류는 사용자 오류로 인해 발생할 수 있으므로 사용자 이름 텍스트는 가려집니다. 이러한 오류를 기록하면 잠재적으로 중요한 정보가 노출될 수 있습니다. 예:

- 우발적으로 사용자 이름 상자에 암호를 입력한 경우
- AWS 계정의 로그인 페이지 링크를 선택하고서 다른 계정의 계정 번호를 입력하는 경우
- 로그인하려는 계정을 잊고 우발적으로 개인 이메일 계정의 사용자 이름, 금융 서비스 로그인 식별자, 또는 기타 프라이빗 ID를 입력하는 경우

임시 자격 증명에 대한 로그인 이벤트 로깅

보안 주체가 임시 자격 증명을 요청할 때 보안 주체 유형에 의해 CloudTrail에서 이벤트를 로그에 기록하는 방법이 결정됩니다. 보안 주체가 다른 계정의 역할을 맡는 경우 이는 복잡할 수 있습니다. 역할 교차 계정 작업과 관련된 작업을 수행하기 위한 여러 API 호출이 있습니다. 먼저 보안 주체는 AWS STS API를 호출하여 임시 자격 증명을 검색합니다. 해당 작업은 호출 계정과 AWS STS 작업이 수행되는 계정에 기록됩니다. 그런 다음 보안 주체는 역할을 사용하여 맡은 역할의 계정에서 다른 API 호출을 수행합니다.

다음 표는 임시 자격 증명을 생성하는 각 API 호출에 대해 CloudTrail에서 다양한 정보를 로그에 기록하는 방법을 보여줍니다.

보안 주체 유형	STS API	호출자 계정에 대한 CloudTrail 로그의 사용자 자격 증명	맡은 역할 계정에 대한 CloudTrail 로그의 사용자 자격 증명	역할의 후속 API 호출에 대한 CloudTrail 로그의 사용자 자격 증명
AWS 계정 루트 사용자 자격 증명	GetSessionToken	루트 사용자 자격 증명	역할 소유자 계정은 호출 계정과 동일	루트 사용자 자격 증명
IAM user	GetSessionToken	IAM 사용자 자격 증명	역할 소유자 계정은 호출 계정과 동일	IAM 사용자 자격 증명
IAM user	GetFederationToken	IAM 사용자 자격 증명	역할 소유자 계정은 호출 계정과 동일	IAM 사용자 자격 증명
IAM user	AssumeRole	IAM 사용자 자격 증명	계정 번호 및 보안 주체 ID(사용자인 경우) 또는 AWS 서비스 보안 주체	역할 자격 증명만 (사용자 없음)
외부에서 인증된 사용자	AssumeRoleWithSAML	해당 사항 없음	SAML 사용자 자격 증명	역할 자격 증명만 (사용자 없음)
외부에서 인증된 사용자	AssumeRoleWithWebIdentity	해당 사항 없음	OIDC/웹 사용자 자격 증명	역할 자격 증명만 (사용자 없음)

CloudTrail 로그의 IAM API 이벤트 예제

CloudTrail 로그 파일에는 JSON 형식의 이벤트 정보가 포함되어 있습니다. API 이벤트는 단일 API 요청을 나타내며 보안 주체, 요청된 작업, 모든 파라미터, 작업 날짜 및 시간에 대한 정보를 포함합니다.

CloudTrail 로그 파일의 IAM API 이벤트 예제

다음은 IAM `GetUserPolicy` 작업 요청에 대한 CloudTrail 로그 항목 예제입니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::444455556666:user/JaneDoe",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "JameDoe",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-07-15T21:39:40Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2014-07-15T21:40:14Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "GetUserPolicy",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "signin.amazonaws.com",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "userName": "JaneDoe",
    "policyName": "ReadOnlyAccess-JaneDoe-201407151307"
  },
  "responseElements": null,
  "requestID": "9EXAMPLE-0c68-11e4-a24e-d5e16EXAMPLE",
  "eventID": "cEXAMPLE-127e-4632-980d-505a4EXAMPLE"
}
```

위 이벤트 정보에서 `ReadOnlyAccess-JaneDoe-201407151307` 요소에 지정한 것처럼 사용자 `JaneDoe`을 의미하는 `requestParameters`이라는 이름의 사용자 정책을 가져오는 요청인 것을 알 수 있습니다. 또한 `JaneDoe`라는 이름의 IAM 사용자가 2014년 7월 15일 오후 9시 40분(UTC)에 요청했음을 확인할 수 있습니다. 여기서는 `userAgent` 요소를 통해 요청이 AWS Management 콘솔에서 이루어진 것도 알 수 있습니다.

CloudTrail 로그의 AWS STS API 이벤트 예제

CloudTrail 로그 파일에는 JSON 형식의 이벤트 정보가 포함되어 있습니다. API 이벤트는 단일 API 요청을 나타내며 보안 주체, 요청된 작업, 모든 파라미터, 작업 날짜 및 시간에 대한 정보를 포함합니다.

CloudTrail 로그 파일의 교차 계정 AWS STS API 이벤트 예제

777788889999 계정의 `JohnDoe`라는 IAM 사용자가 AWS STS `AssumeRole` 작업을 호출하여 111122223333 계정의 `EC2-dev` 역할을 맡습니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAQRSTUVWXYZEXAMPLE",
    "arn": "arn:aws:iam::777788889999:user/JohnDoe",
    "accountId": "777788889999",
    "accessKeyId": "AKIAQRSTUVWXYZEXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-07-18T15:07:39Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "AssumeRole",
```

```
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.101",
  "userAgent": "aws-cli/1.11.10 Python/2.7.8 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.4.67",
  "requestParameters": {
    "roleArn": "arn:aws:iam::111122223333:role/EC2-dev",
    "roleSessionName": "JohnDoe-EC2-dev"
    "serialNumber": "arn:aws:iam::777788889999:mfa"
  },
  "responseElements": {
    "credentials": {
      "sessionToken": "<encoded session token blob>",
      "accessKeyId": "AKIAQRSTUVWXYZEXAMPLE",
      "expiration": "Jul 18, 2014 4:07:39 PM"
      },
    "assumedRoleUser": {
      "assumedRoleId": "AIDAQRSTUVWXYZEXAMPLE:JohnDoe-EC2-dev",
      "arn": "arn:aws:sts::111122223333:assumed-role/EC2-dev/JohnDoe-EC2-dev"
    }
  },
  "resources": [
    {
      "ARN": "arn:aws:iam::111122223333:role/EC2-dev",
      "accountId": "111122223333",
      "type": "AWS::IAM::Role"
    }
  ],
  "requestID": "4EXAMPLE-0e8d-11e4-96e4-e55c0EXAMPLE",
  "sharedEventID": "bEXAMPLE-efea-4a70-b951-19a88EXAMPLE",
  "eventID": "dEXAMPLE-ac7f-466c-a608-4ac8dEXAMPLE"
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

두 번째 예제는 동일한 요청에 대해 맡은 역할 계정(111122223333)의 CloudTrail 로그 항목입니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AWSAccount",
    "principalId": "AIDAQRSTUVWXYZEXAMPLE",
    "accountId": "777788889999"
  },
  "eventTime": "2014-07-18T15:07:39Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "AssumeRole",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.101",
  "userAgent": "aws-cli/1.11.10 Python/2.7.8 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.4.67",
  "requestParameters": {
    "roleArn": "arn:aws:iam:: 111122223333:role/EC2-dev",
    "roleSessionName": "JohnDoe-EC2-dev",
    "serialNumber": "arn:aws:iam::777788889999:mfa"
  },
  "responseElements": {
    "credentials": {
      "sessionToken": "<encoded session token blob>",
      "accessKeyId": "AKIAQRSTUVWXYZEXAMPLE",
      "expiration": "Jul 18, 2014 4:07:39 PM"
    },
    "assumedRoleUser": {
      "assumedRoleId": "AIDAQRSTUVWXYZEXAMPLE:JohnDoe-EC2-dev",
      "arn": "arn:aws:sts::111122223333:assumed-role/EC2-dev/JohnDoe-EC2-dev"
    }
```

```
  },
  "requestID": "4EXAMPLE-0e8d-11e4-96e4-e55c0EXAMPLE",
  "sharedEventID": "bEXAMPLE-efea-4a70-b951-19a88EXAMPLE",
  "eventID": "dEXAMPLE-ac7f-466c-a608-4ac8dEXAMPLE"
}
```

CloudTrail 로그 파일의 AWS STS 역할 체인 API 이벤트 예제

다음은 111111111111 계정의 John Doe가 만든 요청에 대한 CloudTrail 로그 항목 예제입니다. John은 이전에 자신의 `JohnDoe` 사용자를 사용하여 `JohnRole1` 역할을 맡았습니다. 이 요청에 대해 그는 해당 역할의 자격 증명을 사용하여 `JonRole2` 역할을 맡습니다. 이를 역할 체인 (p. 176)이라고 합니다. John은 요청에 두 개의 세션 태그 (p. 294)를 전달합니다. 그는 두 태그를 전이적으로 설정합니다. John은 `JohnRole1`을 맡을 때 전이적으로 설정했기 때문에 요청은 `Department` 태그를 전이적으로 상속합니다. 역할 체인의 전이적 키에 대한 자세한 내용은 세션 태그를 사용하는 역할 체인 (p. 300) 단원을 참조하십시오.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIN5ATK5U7KEXAMPLE:JohnRole1",
        "arn": "arn:aws:sts::111111111111:assumed-role/JohnDoe/JohnRole1",
        "accountId": "111111111111",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-10-02T21:50:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
               "principalId": "AROAIN5ATK5U7KEXAMPLE",
                "arn": "arn:aws:iam::111111111111:role/JohnRole1",
                "accountId": "111111111111",
                "userName": "JohnDoe"
            }
        }
    },
    "eventTime": "2019-10-02T22:12:29Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "123.145.67.89",
    "userAgent": "aws-cli/1.16.248 Python/3.4.7
 Linux/4.9.184-0.1.ac.235.83.329.metal1.x86_64 botocore/1.12.239",
    "requestParameters": {
        "incomingTransitiveTags": {
            "Department": "Engineering"
        },
        "tags": [
            {
                "value": "johndoe@example.com",
                "key": "Email"
            },
            {
                "value": "12345",
                "key": "CostCenter"
            }
        ],
        "roleArn": "arn:aws:iam::111111111111:role/JohnRole2",
        "roleSessionName": "Role2WithTags",
        "transitiveTagKeys": [
            "Email",
            "CostCenter"
```

```
        ],
        "durationSeconds": 3600
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAWHOJDLGPOEXAMPLE",
            "expiration": "Oct 2, 2019 11:12:29 PM",
            "sessionToken": "AgoJb3JpZ2luX2VjEB4aCXVzLXdlc3QtMSJHMEXAMPLETOKEN
+//rJb8Lo30mFc5MlhFCEbubZvEj0wHB/mDMwIgSEe9gk/Zjr09tZV7F1HDTMhmEXAMPLETOKEN/iEJ/
rkqngII9/////////////
ARABGgw0MjgzMDc4NjM5NjYiDLZjZFKwP4qxQG5sFCryASO4UPz5qE97wPPH1eLMvs7CgSDBSWfonmRTCfokm2FN1+hWUdQQH6adjbb
+C+WKFZb701eiv9J5La2EXAMPLETOKEN/c7S5Iro1WUJ0q3Cxuo/8HUoSxVhQHM7zF7mWWLhXLEQ52ivL
+F6q5dpXu4aTFedpMfnJa8JtkWwG9x1Axj0Ypy2ok8v5unpQGWych1vwdvj6ez1Dm8Xg1+qIzXILiEXAMPLETOKEN/
vQGqu8H+nxp3kabcrtOvTFTvxX6vsc8OGwUfHhzAfYGEXAMPLETOKEN/
L6v1yMM3B1OwFOrQBno1HEjf1oNI8RnQiMNFdUOtwYj7HUZIOCZmjfN8PPHq77N7GJl9lzvIZKQA0Owcjg
+mc78zHCj8y0siY8C96paEXAMPLETOKEN/
E3cpksxWdgs91HRzJWScjN2+r2LTGjYhyPqcmFzzo2mCE7mBNEXAMPLETOKEN/oJy
+2o83YNW5tOiDmczgDzJZ4UKR84yGYOMfSnF4XcEJrDgAJ3OJFwmTcTQICAlSwLEXAMPLETOKEN"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROAIFR7WHDTSOYQYHFUE:Role2WithTags",
            "arn": "arn:aws:sts::111111111111:assumed-role/test-role/Role2WithTags"
        }
    },
    "requestID": "b96b0e4e-e561-11e9-8b3f-7b396EXAMPLE",
    "eventID": "1917948f-3042-46ec-98e2-62865EXAMPLE",
    "resources": [
        {
            "ARN": "arn:aws:iam::111122223333:role/JohnRole2",
            "accountId": "111111111111",
            "type": "AWS::IAM::Role"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```


CloudTrail 로그 파일의 AWS 서비스 AWS STS API 이벤트 예제

다음은 서비스 역할의 권한을 사용하여 다른 서비스 API를 호출하는 AWS 서비스의 요청에 대한 CloudTrail 로그 항목 예제입니다. 777788889999 계정에서 만든 요청에 대한 CloudTrail 로그 항목을 보여 줍니다.


```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAQRSTUVWXYZEXAMPLE:devdsk",
    "arn": "arn:aws:sts::777788889999:assumed-role/AssumeNothing/devdsk",
    "accountId": "777788889999",
    "accessKeyId": "AKIAQRSTUVWXYZEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2016-11-14T17:25:26Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAQRSTUVWXYZEXAMPLE",
        "arn": "arn:aws:iam::777788889999:role/AssumeNothing",
        "accountId": "777788889999",
        "userName": "AssumeNothing"
      }
    }
  },
```

```
  "eventTime": "2016-11-14T17:25:45Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "DeleteBucket",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.1",
  "userAgent": "[aws-cli/1.11.10 Python/2.7.8 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.4.67]",
  "requestParameters": {
    "bucketName": "my-test-bucket-cross-account"
  },
  "responseElements": null,
  "requestID": "EXAMPLE463D56D4C",
  "eventID": "dEXAMPLE-265a-41e0-9352-4401bEXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "777788889999"
}
```

CloudTrail 로그 파일의 SAML AWS STS API 이벤트 예제

다음은 AWS STS `AssumeRoleWithSAML` 작업 요청에 대한 CloudTrail 로그 항목 예제입니다. 이 요청에는 SAML 어설션을 통해 세션 태그 (p. 294)로 전달되는 SAML 속성 `CostCenter` 및 `Project`가 포함됩니다. 이러한 태그는 역할 체인 시나리오에서 지속 (p. 300)되도록 전이적으로 설정됩니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "SAMLUser",
        "principalId": "SampleUkh1i4+ExamplexL/jEvs=:SamlExample",
        "userName": "SamlExample",
        "identityProvider": "bdGOnTesti4+ExamplexL/jEvs="
    },
    "eventTime": "2019-11-01T19:14:36Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRoleWithSAML",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.101",
    "userAgent": "aws-cli/1.16.263 Python/3.4.7
 Linux/4.9.184-0.1.ac.235.83.329.metal1.x86_64 botocore/1.12.253",
    "requestParameters": {
        "sAMLAssertionID": "_c0046cEXAMPLEb9d4b8eEXAMPLE2619aEXAMPLE",
        "roleSessionName": "MyAssignedRoleSessionName",
        "principalTags": {
            "CostCenter": "987654",
            "Project": "Unicorn",
            "Department": "Engineering"
        },
        "transitiveTagKeys": [
            "CostCenter",
            "Project"
        ],
        "durationSeconds": 3600,
        "roleArn": "arn:aws:iam::444455556666:role/SAMLTestRoleShibboleth",
        "principalArn": "arn:aws:iam::444455556666:saml-provider/Shibboleth"
    },
    "responseElements": {
        "subjectType": "transient",
        "issuer": "https://server.example.com/idp/shibboleth",
        "credentials": {
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "expiration": "Mar 23, 2016 2:39:57 AM",
            "sessionToken": "<encoded session token blob>"
        },
        "nameQualifier": "bdGOnTesti4+ExamplexL/jEvs=",
        "assumedRoleUser": {
```

```
            "assumedRoleId": "AROAD35QRSTUVWEXAMPLE:MyAssignedRoleSessionName",
            "arn": "arn:aws:sts::444455556666:assumed-role/SAMLTestRoleShibboleth/
MyAssignedRoleSessionName"
        },
        "subject": "SamlExample",
        "audience": "https://signin.aws.amazon.com/saml"
    },
    "resources": [
        {
            "ARN": "arn:aws:iam::444455556666:role/SAMLTestRoleShibboleth",
            "accountId": "444455556666",
            "type": "AWS::IAM::Role"
        },
        {
            "ARN": "arn:aws:iam::444455556666:saml-provider/test-saml-provider",
            "accountId": "444455556666",
            "type": "AWS::IAM::SAMLProvider"
        }
    ],
    "requestID": "6EXAMPLE-e595-11e5-b2c7-c974fEXAMPLE",
    "eventID": "dEXAMPLE-265a-41e0-9352-4401bEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

CloudTrail 로그 파일의 웹 자격 증명 AWS STS API 이벤트 예제

다음은 AWS STS `AssumeRoleWithWebIdentity` 작업 요청에 대한 CloudTrail 로그 항목 예제입니다. 이 요청에는 자격 증명 공급자 토큰을 통해 세션 태그 (p. 294)로 전달되는 속성 `CostCenter` 및 `Project`가 포함됩니다. 이러한 태그는 역할 체인 시나리오에서 지속 (p. 300)되도록 전이적으로 설정됩니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:<id-of-application>.apps.googleusercontent.com:<id-
of-user>",
    "userName": "<id of user>",
    "identityProvider": "accounts.google.com"
  },
  "eventTime": "2016-03-23T01:39:51Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "AssumeRoleWithWebIdentity",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.101",
  "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
  "requestParameters": {
    "durationSeconds": 3600,
    "roleArn": "arn:aws:iam::444455556666:role/FederatedWebIdentityRole",
    "roleSessionName": "MyAssignedRoleSessionName"
        "principalTags": {
            "CostCenter": "24680",
            "Project": "Pegasus"
        },
        "transitiveTagKeys": [
            "CostCenter",
            "Project"
        ],
  },
  "responseElements": {
    "provider": "accounts.google.com",
    "subjectFromWebIdentityToken": "<id of user>",
    "audience": "<id of application>.apps.googleusercontent.com",
    "credentials": {
```

```
      "accessKeyId": "ASIACQRSTUVWRAOEXAMPLE",
      "expiration": "Mar 23, 2016 2:39:51 AM",
      "sessionToken": "<encoded session token blob>"
    },
    "assumedRoleUser": {
      "assumedRoleId": "AROACQRSTUVWRAOEXAMPLE:MyAssignedRoleSessionName",
      "arn": "arn:aws:sts::444455556666:assumed-role/FederatedWebIdentityRole/
MyAssignedRoleSessionName"
    }
  },
  "resources": [
    {
      "ARN": "arn:aws:iam::444455556666:role/FederatedWebIdentityRole",
      "accountId": "444455556666",
      "type": "AWS::IAM::Role"
    }
  ],
  "requestID": "6EXAMPLE-e595-11e5-b2c7-c974fEXAMPLE",
  "eventID": "bEXAMPLE-0b30-4246-b28c-e3da3EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "444455556666"
}
```

CloudTrail 로그의 로그인 이벤트 예제

CloudTrail 로그 파일에는 JSON 형식의 이벤트 정보가 포함되어 있습니다. 로그인 이벤트는 단일 로그인 요청을 나타내며 로그인 보안 주체, 리전, 작업 날짜 및 시간에 대한 정보를 포함합니다.

CloudTrail 로그 파일의 로그인 성공 이벤트 예제

다음은 성공한 로그인 이벤트에 대한 CloudTrail 로그 항목을 나타낸 예제입니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn":"arn:aws:iam::111122223333:user/JohnDoe",
    "accountId": "111122223333",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-07-16T15:49:27Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.110",
  "userAgent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "MobileVersion": "No",
    "LoginTo": "https://console.aws.amazon.com/s3/",
    "MFAUsed": "No"
  },
  "eventID": "3fcfb182-98f8-4744-bd45-10a395ab61cb"
}
```

CloudTrail 로그 파일에 저장된 정보에 대한 자세한 정보는 AWS CloudTrail User Guide의 CloudTrail 이벤트 참조 단원을 참조하십시오.

CloudTrail 로그 파일의 로그인 실패 이벤트 예제

다음은 실패한 로그인 이벤트에 대한 CloudTrail 로그 항목을 나타낸 예제입니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn":"arn:aws:iam::111122223333:user/JaneDoe",
    "accountId": "111122223333",
    "userName": "JaneDoe"
  },
  "eventTime": "2014-07-08T17:35:27Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.100",
  "userAgent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0",
  "errorMessage": "Failed authentication",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Failure"
  },
  "additionalEventData": {
    "MobileVersion": "No",
    "LoginTo": "https://console.aws.amazon.com/sns",
    "MFAUsed": "No"
  },
  "eventID": "11ea990b-4678-4bcd-8fbe-62509088b7cf"
}
```

이 정보에서 `userIdentity` 요소에도 나와 있듯이 `JaneDoe`라는 이름의 IAM 사용자가 로그인을 시도한 것을 알 수 있습니다. 또한 `responseElements` 요소를 보면 로그인 시도가 실패한 것도 확인됩니다. 그리고 `JaneDoe`가 Amazon SNS 콘솔에 로그인하려고 시도한 일시는 2014년 7월 8일 오후 5시 35분(UTC)입니다.

잘못된 사용자 이름으로 인한 로그인 실패 이벤트 예제

다음은 잘못된 사용자 이름을 입력하여 로그인을 실패한 이벤트의 CloudTrail 로그 항목을 나타낸 예제입니다. 이때 AWS는 `userName` 텍스트를 `HIDDEN_DUE_TO_SECURITY_REASONS`로 마스킹 처리하여 잠재적으로 민감한 정보의 노출을 차단합니다.

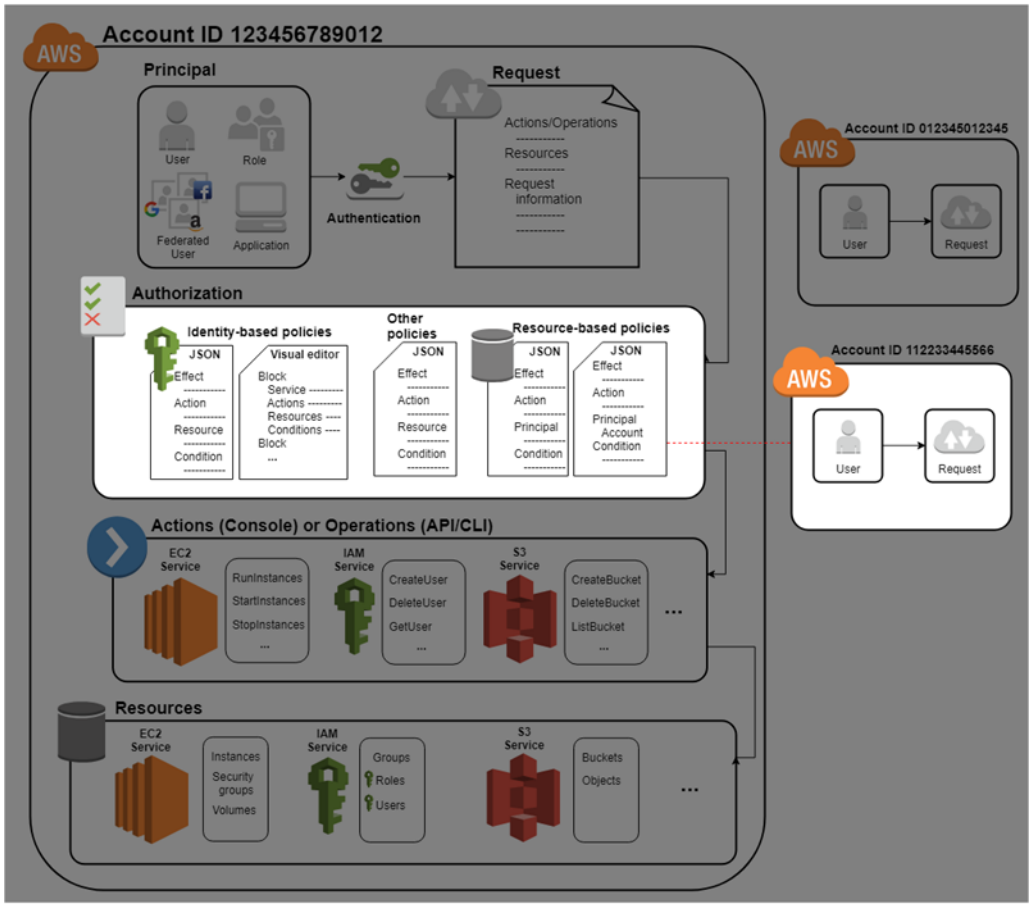
```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "eventTime": "2015-03-31T22:20:42Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.101",
  "userAgent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0",
  "errorMessage": "No username found in supplied account",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Failure"
  },
  "additionalEventData": {
```

```
    "LoginTo": "https://console.aws.amazon.com/console/home?state=hashArgs
%23&isauthcode=true",
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "a7654656-0417-45c6-9386-ea8231385051",
  "eventType": "AwsConsoleSignin",
  "recipientAccountId": "123456789012"
}
```

액세스 관리

AWS Identity and Access Management(IAM)는 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스입니다. 보안 주체 (p. 5)가 AWS에 요청하면 AWS 적용 코드는 해당 보안 주체가 인증(로그인) 및 권한 부여(권한 있음)되었는지 확인합니다. 정책을 생성하고 IAM 자격 증명 또는 AWS 리소스에 연결하여 AWS 액세스를 관리합니다. 정책은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 AWS의 JSON 정책 문서입니다. 정책 유형 및 활용에 대한 자세한 정보는 정책 및 권한 (p. 349) 단원을 참조하십시오.

인증 및 권한 부여 프로세스의 나머지 부분에 대한 자세한 정보는 IAM 작동 방식 이해 (p. 3) 단원을 참조하십시오.



권한 부여 중 AWS 적용 코드는 요청 콘텍스트 (p. 5)의 값을 사용하여 일치하는 정책을 확인하고 요청을 허용할지 거부할지 여부를 결정합니다.

AWS은 요청 콘텍스트에 적용되는 각 정책을 확인합니다. 단일 정책이 요청을 거부한 경우 AWS는 전체 요청을 거부하고 정책 평가를 중지합니다. 이를 명시적 거부라고 합니다. 요청은 기본적으로 거부되므로 IAM은 사용 가능한 정책이 요청의 모든 부분을 허용하는 경우에만 요청에 권한을 부여합니다. 단일 계정 내 요청 평가 로직 (p. 622)은 다음 규칙을 따릅니다.

- 기본적으로 모든 요청이 묵시적으로 거부됩니다. 또는 기본적으로 AWS 계정 루트 사용자에 모든 권한이 부여됩니다.
- 자격 증명 기반 또는 리소스 기반 정책에 포함된 명시적 허용은 이 기본 작동을 재정의합니다.
- 권한 경계, 조직 SCP 또는 세션 정책이 있는 경우 이러한 정책 유형이 명시적 거부로 허용을 재정의할 수도 있습니다.

- 어떠한 정책의 명시적 거부도 허용을 무시합니다.

요청이 인증 및 권한 부여된 후 AWS이 요청을 승인합니다. 다른 계정에서 요청해야 하는 경우 다른 계정의 정책에서 요청자에게 해당 리소스에 대한 액세스를 허용해야 합니다. 또한 요청하는 데 사용하는 IAM 엔터티에 해당 요청을 허용하는 자격 증명 기반 정책이 있어야 합니다.

액세스 관리 리소스

권한 및 정책 생성에 대한 자세한 정보는 다음 리소스를 참조하십시오.

AWS 보안 블로그의 다음 게시물에서는 Amazon S3 버킷과 객체에 액세스하기 위한 정책을 작성하는 일반적인 방법을 소개합니다.

- IAM 정책 작성: Amazon S3 버킷에 대한 액세스를 허용하는 방법
- IAM 정책 작성: Amazon S3 버킷의 사용자별 폴더에 대한 액세스 허용
- IAM 정책 및 버킷 정책과 ACL ACL (S3 리소스에 대한 액세스 제어)
- RDS 리소스 수준 권한에 대한 소개
- EC2 리소스 수준 권한 설명

정책 및 권한

정책을 생성하고 IAM 자격 증명(사용자, 사용자 그룹 또는 역할) 또는 AWS 리소스에 연결하여 AWS에서 액세스를 관리합니다. 정책은 자격 증명이나 리소스와 연결될 때 해당 권한을 정의하는 AWS의 객체입니다. AWS는 IAM 보안 주체(사용자 또는 역할)가 요청을 보낼 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지 여부를 결정합니다. 대부분의 정책은 AWS에 JSON 문서로 저장됩니다. AWS에서는 자격 증명 기반 정책, 리소스 기반 정책, 권한 경계, 조직 SCP, ACL 및 세션 정책이라는 6가지 정책 유형을 지원합니다.

IAM 정책은 작업을 실행하기 위한 방법과 상관없이 작업을 정의합니다. 예를 들어, 정책이 GetUser 작업을 허용한다면 이 정책이 있는 사용자는 AWS Management 콘솔, AWS CLI, 또는 AWS API에서 사용자 정보를 얻을 수 있습니다. IAM 사용자를 생성할 경우 콘솔 또는 프로그래밍 방식 액세스를 허용하도록 선택할 수 있습니다. 콘솔 액세스가 허용되는 경우 IAM 사용자는 사용자 이름 및 암호를 사용하여 콘솔에 로그인할 수 있습니다. 또는 프로그래밍 방식의 액세스가 허용되는 경우 사용자는 액세스 키를 사용하여 CLI 또는 API로 작업할 수 있습니다.

정책 유형

빈도수에 따라 나열된 다음 정책 유형은 AWS에서 사용 가능합니다. 자세한 정보는 각 정책 유형에 따른 섹션을 참조하십시오.

- 자격 증명 기반 정책 (p. 350) – 관리형 및 인라인 정책을 IAM 자격 증명(사용자, 사용자가 속한 그룹, 또는 역할)에 연결합니다. 자격 증명 기반 정책은 자격 증명에 권한을 부여합니다.
- 리소스 기반 정책 (p. 350) – 인라인 정책을 리소스에 연결합니다. 리소스 기반 정책의 가장 일반적인 예제는 Amazon S3 버킷 정책 및 IAM 역할 신뢰 정책입니다. 리소스 기반 정책은 정책에 지정된 보안 주체에 권한을 부여합니다. 보안 주체는 리소스와 동일한 계정 또는 다른 계정에 있을 수 있습니다.
- 권한 경계 (p. 351) – 관리형 정책을 IAM 엔터티(사용자 또는 역할)에 대한 권한 경계로 사용합니다. 해당 정책은 자격 증명 기반 정책을 통해 엔터티에 부여할 수 있는 최대 권한을 정의하지만, 권한을 부여하지는 않습니다. 권한 경계는 리소스 기반 정책을 통해 엔터티에 부여할 수 있는 최대 권한을 정의하지 않습니다.
- 조직 SCP (p. 351) – AWS Organizations 서비스 제어 정책(SCP)을 사용하여 조직 또는 조직 단위(OU)의 계정 멤버에 대한 최대 권한을 정의합니다. SCP는 자격 증명 기반 정책이나 리소스 기반 정책을 통해 계정 내 엔터티(사용자나 역할)에 부여하는 권한을 제한하지만, 권한을 부여하지는 않습니다.

- 액세스 제어 목록(ACL) (p. 351) – ACL을 사용하여 ACL이 연결된 리소스에 액세스할 수 있는 다른 계정의 보안 주체를 제어합니다. ACL는 리소스 기반 정책과 비슷합니다. 다만 JSON 정책 문서 구조를 사용하지 않은 유일한 정책 유형입니다. ACL은 지정된 보안 주체에 권한을 부여하는 교차 계정 권한 정책입니다. ACL은 동일 계정 내 엔터티에 권한을 부여할 수 없습니다.
- 세션 정책 (p. 351) – AWS CLI 또는 AWS API를 사용하여 역할이나 연합된 사용자를 수임할 때 고급 세션 정책을 전달합니다. 세션 정책은 역할이나 사용자의 자격 증명 기반 정책을 통해 세션에 부여하는 권한을 제한합니다. 세션 정책은 생성된 세션에 대한 권한을 제한하지 않지만, 권한을 부여하지도 않습니다. 자세한 정보는 세션 정책을 참조하십시오.

자격 증명 기반 정책

자격 증명 기반 정책은 자격 증명(사용자, 사용자 그룹 또는 역할)에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 엔터티(사용자 또는 역할)가 수행할 수 있는 작업, 작업의 대상 리소스 또는 작업 수행 조건을 제어합니다. 자격 증명 기반 정책을 추가로 분류할 수 있습니다.

- 관리형 정책 – AWS 계정에 속한 다수의 사용자, 그룹 및 역할에게 독립적으로 연결할 수 있는 자격 증명 기반 정책입니다. 사용할 수 있는 관리형 정책은 두 가지가 있습니다.
  - AWS 관리형 정책 – AWS에서 생성 및 관리하는 관리형 정책입니다. 정책 사용이 처음이라면 AWS 관리형 정책 사용을 먼저 권장합니다.
  - 고객 관리형 정책 – 사용자가 자신의 AWS 계정에서 생성 및 관리하는 관리형 정책입니다. 고객 관리형 정책은 AWS 관리형 정책보다 정책에 대해 더욱 정밀하게 제어할 수 있습니다. 시각적 편집기에서 또는 JSON 정책 문서를 직접 생성하여 IAM 정책을 생성 및 편집할 수 있습니다. 자세한 정보는 IAM 정책 만들기 (p. 435) 및 IAM 정책 편집 (p. 460)을(를) 참조하십시오.
- 인라인 정책 – 자신이 생성 및 관리하며, 단일 사용자, 그룹 또는 역할에 직접 포함되는 정책입니다. 대부분의 경우 인라인 정책을 사용하지 않는 것이 좋습니다.

관리형 정책을 사용할지 아니면 인라인 정책을 사용할지를 선택하는 방법은 관리형 정책과 인라인 정책 (p. 357) 단원을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 Amazon S3 버킷과 같은 리소스에 연결하는 JSON 정책 문서입니다. 이러한 정책은 지정된 보안 주체에 해당 리소스에 대한 특정 작업을 수행할 수 있는 권한을 부여하고 이러한 권한이 적용되는 조건을 정의합니다. 리소스 기반 정책은 인라인 정책입니다. 관리형 리소스 기반 정책은 없습니다.

교차 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 교차 계정 보안 주체를 추가하는 것은 신뢰 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 또한 보안 주체와 리소스가 별도의 AWS 계정에 있는 경우 자격 증명 기반 정책을 사용하여 보안 주체에 리소스에 대한 액세스 권한을 부여해야 합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다.

IAM 서비스는 역할 신뢰 정책이라고 하는 리소스 기반 정책 유형 하나만 지원하며, 이 유형은 IAM 역할에 연결됩니다. IAM 역할은 자격 증명이기도 하고 리소스 기반 정책을 지원하는 리소스이기도 합니다. 그러므로 IAM 역할에 신뢰 정책과 자격 증명 기반 정책을 모두 연결해야 합니다. 신뢰 정책은 역할을 수임할 수 있는 보안 주체 엔터티(계정, 사용자, 역할 및 연합된 사용자)를 정의합니다. IAM 역할과 다른 리소스 기반 정책 간의 차이에 대해 알아보려면 IAM 역할과 리소스 기반 정책의 차이 (p. 287) 단원을 참조하십시오.

리소스 기반 정책을 지원하는 다른 서비스를 확인하려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 리소스 기반 정책에 대해 자세히 알아보려면 자격 증명 기반 정책 및 리소스 기반 정책 (p. 372) 단원을 참조하십시오.해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

IAM 권한 경계

권한 경계는 자격 증명 기반 정책을 통해 IAM 엔터티에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 엔터티에 대한 권한 경계를 설정할 경우 해당 엔터티는 자격 증명 기반 정책 및 관련 권한 경계 모두에서 허용되는 작업만 수행할 수 있습니다. 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계에 제한을 받지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 엔터티에 대한 권한 경계 (p. 363) 단원을 참조하십시오.

서비스 제어 정책(SCP)

AWS Organizations는 기업이 소유하는 AWS 계정을 그룹화하고 중앙에서 관리할 수 있는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 조직 또는 조직 단위(OU)에 최대 권한을 지정하는 JSON 정책입니다. SCP는 각 AWS 계정 루트 사용자를 비롯하여 멤버 계정의 엔터티에 대한 권한을 제한합니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다.

조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP의 작동 방식 단원을 참조하십시오.

ACL(액세스 제어 목록)

ACL(액세스 제어 목록)은 리소스에 액세스할 수 있는 다른 계정의 보안 주체를 제어할 수 있는 서비스 정책입니다. ACL은 동일 계정 내에서 보안 주체에 대한 액세스를 제어하는 데 사용할 수 없습니다. ACL는 리소스 기반 정책과 비슷합니다. 다만 JSON 정책 문서 형식을 사용하지 않은 유일한 정책 유형입니다. Amazon S3, AWS WAF, Amazon VPC는 ACL을 지원하는 서비스의 예입니다. ACL에 대한 자세한 정보는 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요 단원을 참조하십시오.

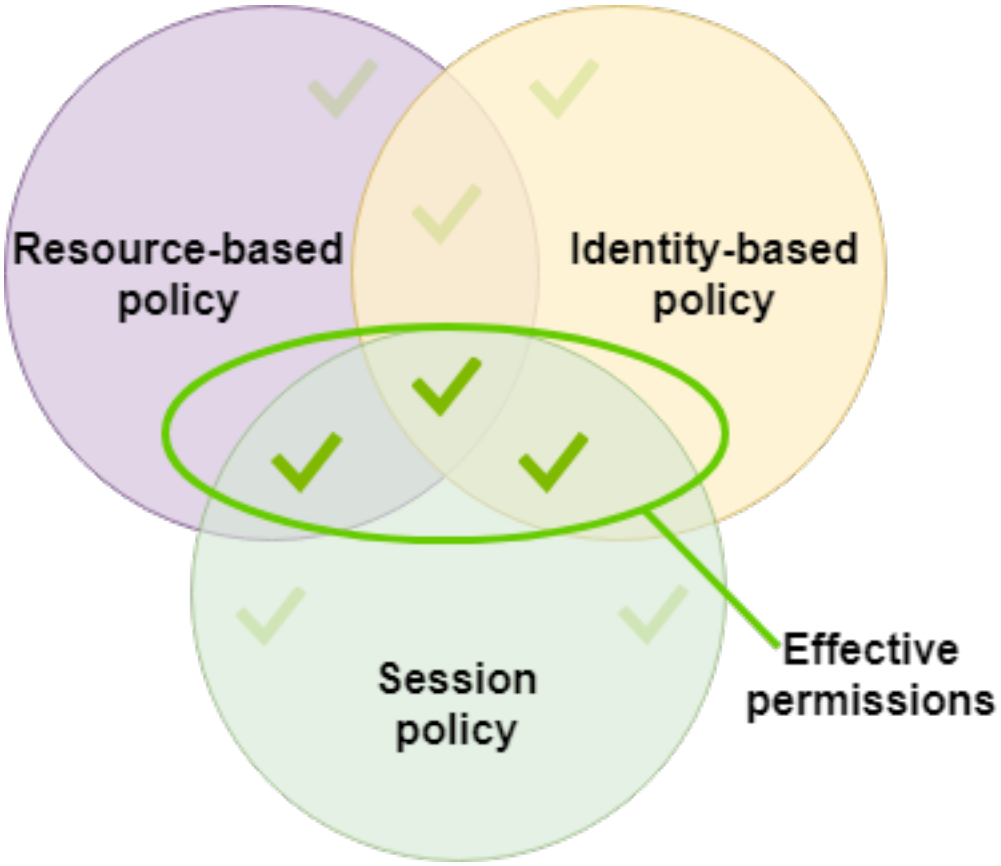
세션 정책

세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 세션에 대한 권한은 세션을 생성하는 데 사용되는 IAM 엔터티(사용자 또는 역할)에 대한 자격 증명 기반 정책과 세션 정책의 교집합입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다.

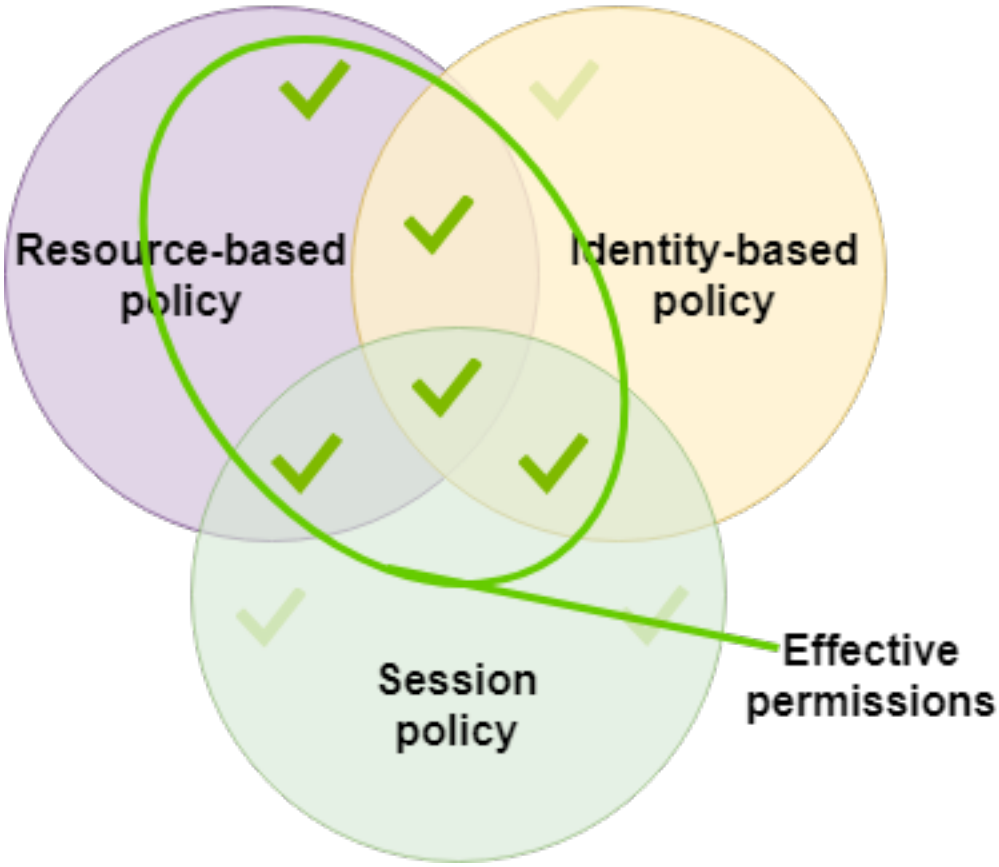
`AssumeRole`, `AssumeRoleWithSAML` 또는 `AssumeRoleWithWebIdentity` API 작업을 사용하여 프로그래밍 방식으로 역할 세션을 생성하고 세션 정책을 전달할 수 있습니다. `Policy` 파라미터를 사용하여 단일 JSON 인라인 세션 정책 문서를 전달할 수 있습니다. `PolicyArns` 파라미터를 사용하여 최대 10개까지 관리형 세션 정책을 지정할 수 있습니다. 역할 세션 생성에 대한 자세한 정보는 임시 보안 자격 증명 요청하기 (p. 304) 단원을 참조하십시오.

연합된 사용자 세션을 생성할 경우 IAM 사용자의 액세스 키를 사용하여 `GetFederationToken` API 작업을 프로그래밍 방식으로 호출할 수 있습니다. 또한 세션 정책도 전달해야 합니다. 결과적으로 얻는 세션의 권한은 IAM 사용자의 자격 증명 기반 정책과 세션 정책의 교집합입니다. 연합된 사용자 생성에 대한 자세한 정보는 GetFederationToken—사용자 지정 자격 증명 브로커를 통한 연동 (p. 308) 단원을 참조하십시오.

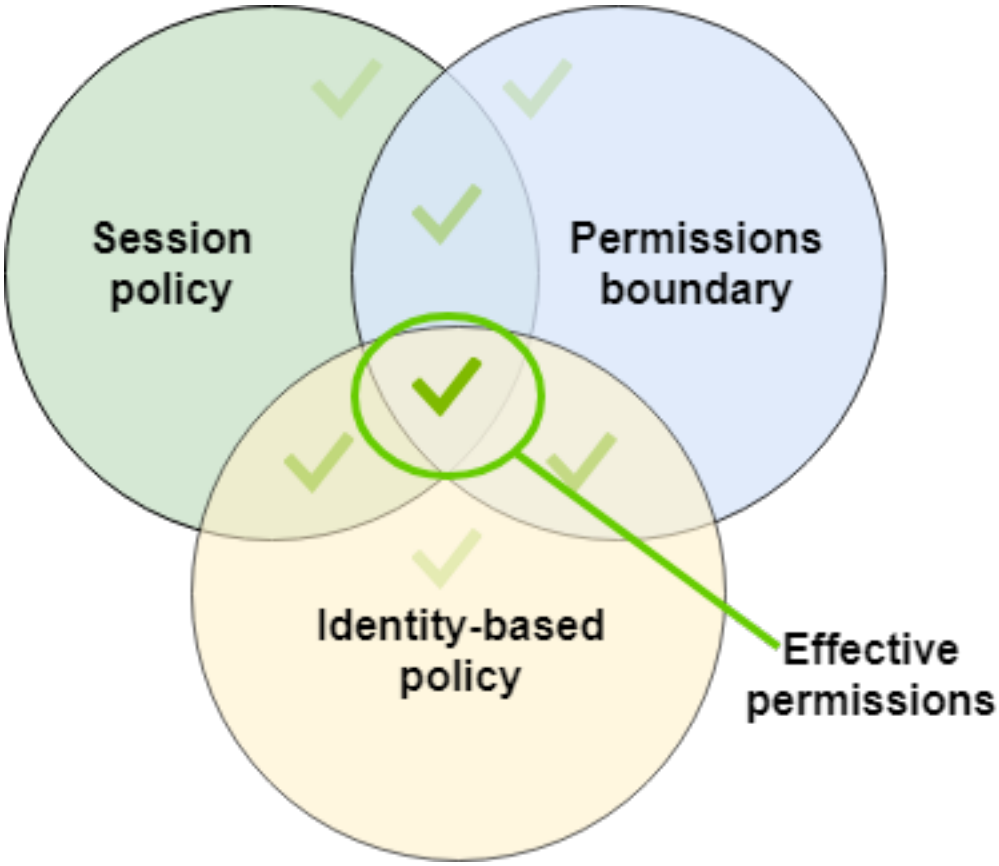
리소스 기반 정책에서 사용자 또는 역할의 ARN을 보안 주체로 지정할 수 있습니다. 이 경우, 세션이 생성되기 전에 리소스 기반 정책의 권한이 역할 또는 사용자의 자격 증명 기반 정책에 추가됩니다. 이 세션 정책은 리소스 기반 정책 및 자격 증명 기반 정책을 통해 부여되는 모든 권한을 제한합니다. 결과적으로 얻는 세션의 권한은 세션 정책과 리소스 기반 정책 또는 자격 증명 기반 정책의 교집합입니다.



리소스 기반 정책에서 세션의 ARN을 보안 주체로 지정할 수 있습니다. 이 경우, 세션이 생성된 후 리소스 기반 정책의 권한이 추가됩니다. 리소스 기반 정책 권한은 세션 정책에 제한을 받지 않습니다. 결과 세션에는 리소스 기반 정책의 모든 권한 + 자격 증명 기반 정책과 세션 정책의 권한 교집합이 부여됩니다.



권한 경계를 사용하여 세션을 생성하는 데 사용되는 사용자 또는 역할의 최대 권한 설정할 수 있습니다. 이 경우, 결과적으로 얻는 세션의 권한은 세션 정책, 권한 경계 및 자격 증명 기반 정책의 교집합입니다. 단, 권한 경계는 결과 세션의 ARN을 지정하는 리소스 기반 정책이 부여하는 권한을 제한할 수 없습니다.



정책 및 루트 사용자

AWS 계정 루트 사용자는 어떤 정책에는 영향을 받지만 이외의 정책에는 영향을 받지 않습니다. 자격 증명 기반 정책을 루트 사용자로 연결할 수 없고 루트 사용자에 대한 권한 경계를 설정할 수 없습니다. 그러나, 루트 사용자를 리소스 기반 정책 또는 ACL의 보안 주체로 지정할 수 있습니다. 계정의 멤버로서 루트 사용자는 계정의 SCP에 의해 영향을 받습니다.

JSON 정책 개요

대부분의 정책은 AWS에 JSON 문서로서 저장됩니다. 자격 증명 기반 정책, 경계를 설정할 수 있는 정책은 사용자 또는 역할에 연결할 수 있는 JSON 정책 문서입니다. 리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. SCP는 AWS Organizations 조직 단위(OU)에 연결하는 제한된 구문이 있는 JSON 정책 문서입니다. ACL은 리소스에도 연결되지만 다른 구문을 사용해야 합니다. 세션 정책은 역할 또는 연합된 사용자 세션을 수임할 때 제공하는 JSON 정책입니다.

JSON 구문을 이해할 필요가 없습니다. AWS Management 콘솔의 시각적 편집기를 사용하면 JSON을 사용하지 않고 고객 관리형 정책을 생성하고 편집할 수 있습니다. 그러나 그룹 또는 복잡한 정책에 대해 인라인 정책을 사용하는 경우에는 콘솔을 사용하여 JSON 편집기에서 해당 정책을 생성하고 편집해야 합니다. 시각적 편집기 사용에 대한 자세한 정보는 IAM 정책 만들기 (p. 435) 및 IAM 정책 편집 (p. 460) 단원을 참조하십시오.

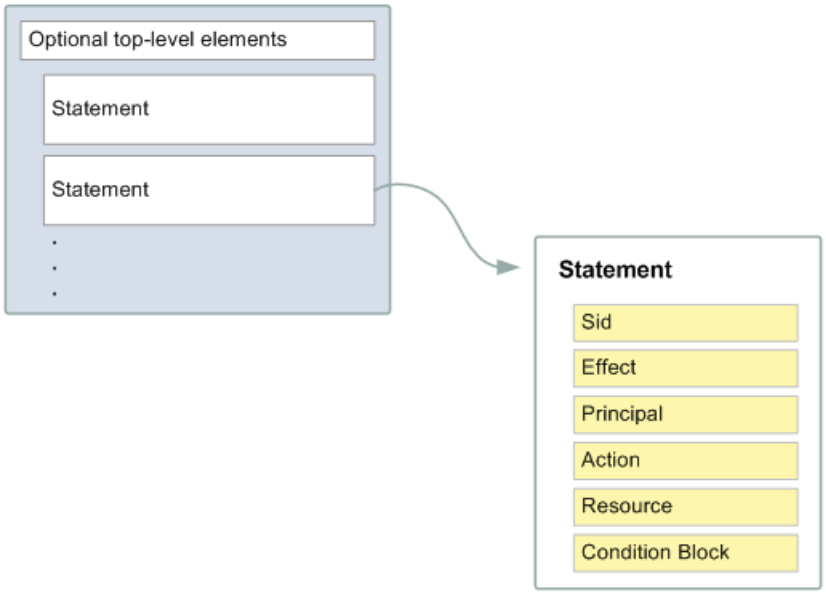
JSON 정책 문서 구조

다음 그림처럼 JSON 정책 문서는 이러한 요소를 포함합니다.

- 문서 상단에 위치하는 정책 전반의 선택적 정보

- 하나 이상의 개별 문

각 설명문에는 단일 권한에 대한 정보가 포함되어 있습니다. 정책에 설명문이 여러 개 포함되어 있는 경우, AWS는 설명문을 평가하는 동안 전체에 대해 논리 OR을 적용합니다. 요청 하나에 적용되는 정책이 여럿인 경우, AWS는 정책을 평가하는 동안 전체에 걸쳐 논리 OR을 적용합니다.



문의 정보는 일련의 요소 안에 포함되어 있습니다.

- Version – 사용하고자 하는 정책 언어의 버전을 지정합니다. 가장 좋은 방법은 최신 `2012-10-17` 버전을 사용하는 것입니다.
- Statement – 이 주요 정책 요소를 다음 요소의 컨테이너로 사용합니다. 정책에 설명문 둘 이상을 포함할 수 있습니다.
- Sid (선택 사항) – 선택 설명문 ID를 포함하여 설명문들을 구분합니다.
- Effect – `Allow` 또는 `Deny`를 사용하여 정책에서 액세스를 허용하는지 또는 거부하는지 여부를 설명합니다.
- Principal (일부 상황에서만 필요) – 리소스 기반 정책을 생성하는 경우 액세스를 허용하거나 거부할 계정, 사용자, 역할 또는 연동 사용자를 표시해야 합니다. 사용자 또는 역할에 연결할 IAM 권한 정책을 생성하면 이 요소를 포함할 수 없습니다. 보안 주체는 사용자 또는 역할을 의미합니다.
- Action – 정책이 허용하거나 거부하는 작업 목록을 포함합니다.
- Resource (일부 상황에서만 필요) – IAM 권한 정책을 생성하는 경우 작업이 적용되는 리소스 목록을 지정해야 합니다. 리소스 기반 정책을 생성하는 경우 이 요소는 선택 사항입니다. 이 요소를 포함하지 않으면 작업이 적용되는 리소스는 정책이 연결된 리소스입니다.
- Condition (선택 사항) – 정책에서 권한을 부여하는 상황을 지정합니다.

이러한 요소와 기타 더 고급 정책 요소에 대한 자세한 정보는 IAM JSON 정책 요소 참조 (p. 586) 단원을 참조하십시오.

복수의 문 및 복수의 정책

엔터티(사용자, 그룹 또는 역할)에 부여할 권한을 하나 이상 정의하고자 할 경우, 단일 정책에 여러 설명문을 사용할 수 있습니다. 여러 정책을 연결할 수도 있습니다. 단일한 설명문에 여러 권한을 정의하고자 할 경우,

정책이 기대하는 액세스를 보장하지 않을 수 있습니다. 가장 좋은 방법은 리소스 유형에 따라 정책을 나누는 것입니다.

정책의 제한된 크기 (p. 569)로 인해 더 복잡한 권한에 대해서는 여러 정책을 사용해야 할 수도 있습니다. 개별 사용자 관리형 정책에 권한의 기능적 그룹화를 만드는 방법이 좋습니다. 예를 들어, IAM 사용자 관리용 정책 하나, 자기 관리용 하나 및 S3 버킷 관리용 기타 정책 하나를 생성합니다. 여러 설명문과 여러 정책의 조합과 상관없이 AWS는 동일한 방식으로 정책을 평가 (p. 622)합니다.

예를 들어, 다음 정책에는 설명문이 세 개 있으며 각 설명문은 단일 계정에 별도의 권한 세트를 부여합니다. 설명문은 다음을 정의합니다.

- `Sid`(설명문 ID)의 `FirstStatement` 첫 번째 설명문은 연결된 정책으로 사용자가 자체 암호를 변경하도록 허용합니다. 이 문에서 `Resource` 요소는 "`*`"("모든 리소스"를 의미)이지만 실제로 `ChangePassword` API 작업(또는 동등한 `change-password` CLI 명령)은 요청을 수행한 사용자의 암호에만 영향을 미칩니다.
- 두 번째 문은 사용자가 자신의 AWS 계정에 있는 모든 Amazon S3 버킷을 나열할 수 있도록 합니다. 이 문에서 `Resource` 요소는 "`*`"("모든 리소스를 의미)이지만 정책에서 다른 계정의 리소스에 대한 액세스 권한을 부여하지 않으므로 사용자는 자신의 AWS 계정에 있는 버킷만 나열할 수 있습니다.
- 세 번째 설명문은 사용자가 `confidential-data`라는 버킷에 있는 객체를 나열 및 검색할 수 있도록 하지만, 이는 사용자가 멀티 팩터 인증(MFA)에서 인증한 경우에 한합니다. 정책의 `Condition` 요소는 MFA 인증을 수행합니다.

  정책 문에 `Condition` 요소가 포함된 경우, `Condition` 요소가 true로 평가된 경우에만 해당 문이 유효합니다. 이때 `Condition`은 사용자가 MFA 인증된 경우 true로 평가됩니다. 사용자가 MFA 인증되지 않은 경우, 이 `Condition`은 false로 평가됩니다. 이 경우 이 정책의 세 번째 설명문과 사용자는 `confidential-data` 버킷을 적용하지 않고 이에 액세스할 수 없습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "FirstStatement",
      "Effect": "Allow",
      "Action": ["iam:ChangePassword"],
      "Resource": "*"
    },
    {
      "Sid": "SecondStatement",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Sid": "ThirdStatement",
      "Effect": "Allow",
      "Action": [
        "s3:List*",
        "s3:Get*"
      ],
      "Resource": [
        "arn:aws:s3:::confidential-data",
        "arn:aws:s3:::confidential-data/*"
      ],
      "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
    }
  ]
}
```

JSON 정책 구문 예제

다음 자격 증명 기반 정책은 `example_bucket`이라는 하나의 Amazon S3 버킷 목록에 암시된 보안 주체를 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example_bucket"
  }
}
```

다음 리소스 기반 정책은 Amazon S3 버킷에 연결될 수 있습니다. 이 정책에서는 특정 AWS 계정 구성원이 `mybucket`라는 버킷의 모든 Amazon S3 작업을 수행할 수 있도록 합니다. 작업 내 버킷 또는 객체에 수행될 수 있는 모든 작업을 허용합니다. (이 정책은 계정에만 신뢰를 부여하므로, 해당 계정의 개별 사용자는 지정된 Amazon S3 작업에 대한 권한을 다시 부여받아야 합니다.)

```
{
  "Version": "2012-10-17",
  "Id": "S3-Account-Permissions",
  "Statement": [{
    "Sid": "1",
    "Effect": "Allow",
    "Principal": {"AWS": ["arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:root"]},
    "Action": "s3:*",
    "Resource": [
      "arn:aws:s3:::mybucket",
      "arn:aws:s3:::mybucket/*"
    ]
  }]
}
```

공통 시나리오가 포함되는 예제 정책은 IAM 자격 증명 기반 정책 예제 (p. 387) 단원을 참조하십시오.

관리형 정책과 인라인 정책

IAM에서 자격 증명에 대한 권한을 설정해야 할 경우 AWS 관리형 정책, 고객 관리형 정책 또는 인라인 정책 중 어느 것을 사용할지를 결정해야 합니다. 다음 단원에서는 각 자격 증명 기반 정책 유형과 사용 시기에 대해 자세히 살펴보겠습니다.

주제

AWS 관리형 정책

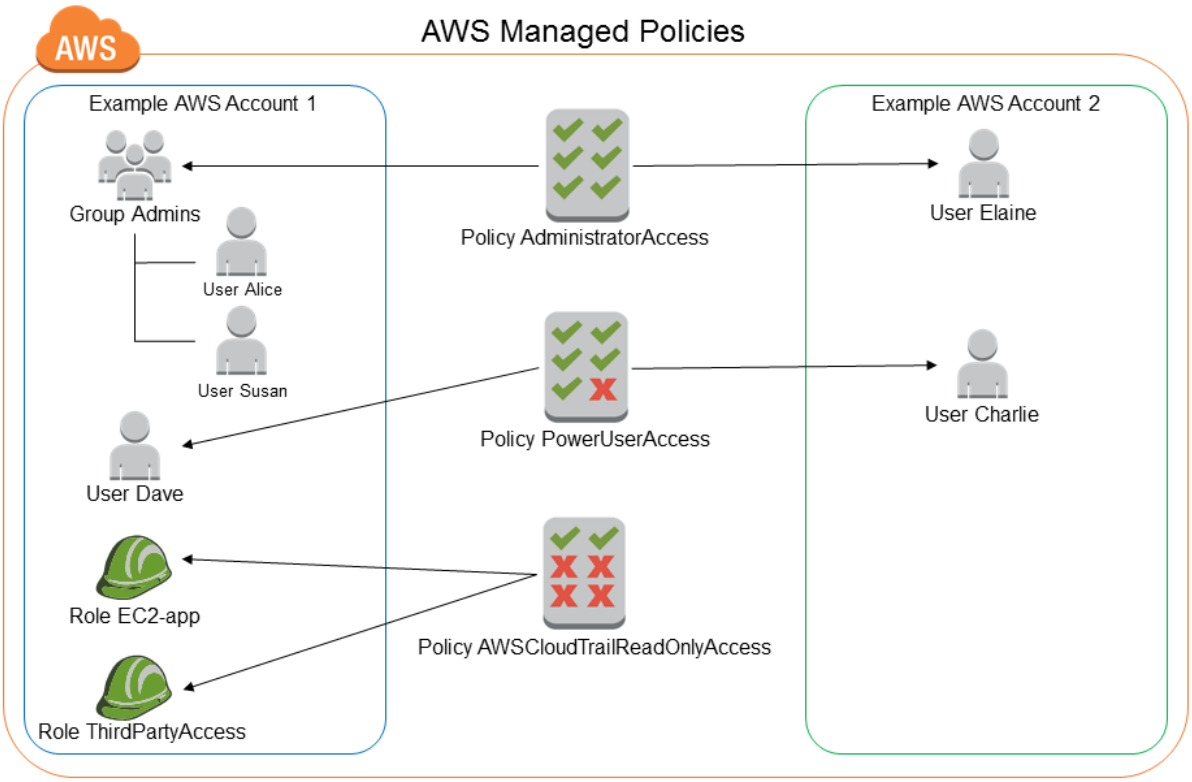
AWS 관리형 정책은 AWS에서 생성 및 관리하는 독립적인 정책입니다. 여기에서 독립적인 정책이란 정책 스스로 정책 이름이 포함된 Amazon 리소스 이름(ARN)을 갖고 있다는 것을 의미합니다. 예를 들어 `arn:aws:iam::aws:policy/IAMReadOnlyAccess`는 AWS 관리형 정책입니다. ARN에 대한 자세한 내용은 IAM ARN (p. 564) 단원을 참조하십시오.

AWS 관리형 정책은 여러 가지 일반 사용 사례에서 권한을 제공할 목적으로 설계되었습니다. AmazonDynamoDBFullAccess 및 IAMFullAccess와 같은 전체 액세스 AWS 관리형 정책은 서비스에 대한 전체 액세스 권한을 부여하여 서비스 관리자에 대한 권한을 정의합니다. AWSCodeCommitPowerUser 및 AWSKeyManagementServicePowerUser와 같은 파워 사용자 AWS 관리형 정책은 파워 사용자용으로 설계되었습니다. AmazonMobileAnalyticsWriteOnlyAccess 및 AmazonEC2ReadOnlyAccess와 같은 부분 액세스 AWS 관리형 정책은 권한 관리 권한을 허용하지 않고 AWS 서비스에 대한 특정 액세스 수준을 제공합니다. AWS 관리형 정책을 사용하면 정책을 직접 작성하는 것보다 쉽게 사용자, 그룹 및 역할에 적절한 권한을 할당할 수 있습니다.

AWS 관리형 정책에서 특히 유용한 범주 중 하나로, 직무 기능에 대한 범주를 들 수 있습니다. 이러한 정책은 IT 업계에서 일반적으로 사용되는 직무 기능과 긴밀하게 연결됩니다. 이러한 일반적인 직무 기능에 대한 권한 부여를 쉽게 만들기 위해서입니다. 직무 정책을 사용하는 큰 장점 중 하나는 새로운 서비스와 API 작업이 도입될 때마다 AWS가 이를 유지하고 업데이트할 수 있다는 점입니다. 예를 들어 AdministratorAccess 직무는 AWS의 모든 서비스 및 리소스에 대한 모든 액세스 권한 및 작업 권한을 위임합니다. 이 정책은 계정 관리자에게만 사용하는 것이 좋습니다. IAM 및 조직에 대해서는 제한적인 액세스 권한만 있으면 되지만 그 밖의 모든 서비스에 대해 모든 액세스 권한이 필요한 고급 사용자의 경우, PowerUserAccess 직무를 사용하십시오. 직무 정책의 목록과 설명은 직무 기능에 대한 AWS 관리형 정책 (p. 642) 단원을 참조하십시오.

AWS 관리형 정책에 정의되어 있는 권한은 변경할 수 없습니다. AWS가 AWS 관리형 정책에서 정의한 권한을 간혹 업데이트합니다. AWS에서 업데이트할 경우 정책이 추가되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에게도 업데이트가 적용됩니다. 새로운 AWS 제품을 실행하거나 새로운 API 호출을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다. 예를 들어 ReadOnlyAccess라는 이름의 AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스 권한을 제공합니다. AWS에서 새로운 서비스가 실행될 때는 AWS가 ReadOnlyAccess 정책을 업데이트하여 새로운 서비스에 대한 읽기 전용 권한을 추가합니다. 이렇게 업데이트된 권한은 정책이 추가되는 모든 보안 주체 엔터티에게 적용됩니다.

다음은 AWS 관리형 정책을 나타낸 다이어그램입니다. 다이어그램을 보면 AdministratorAccess, PowerUserAccess, 그리고 AWSCloudTrailReadOnlyAccess 등 3개의 AWS 관리형 정책이 있습니다. 다이어그램에도 나와있지만 단일 AWS 관리형 정책을 다른 AWS 계정의 보안 주체 엔터티에 추가할 수도 있고, 단일 AWS 계정의 다른 보안 주체 엔터티에 추가할 수도 있습니다.

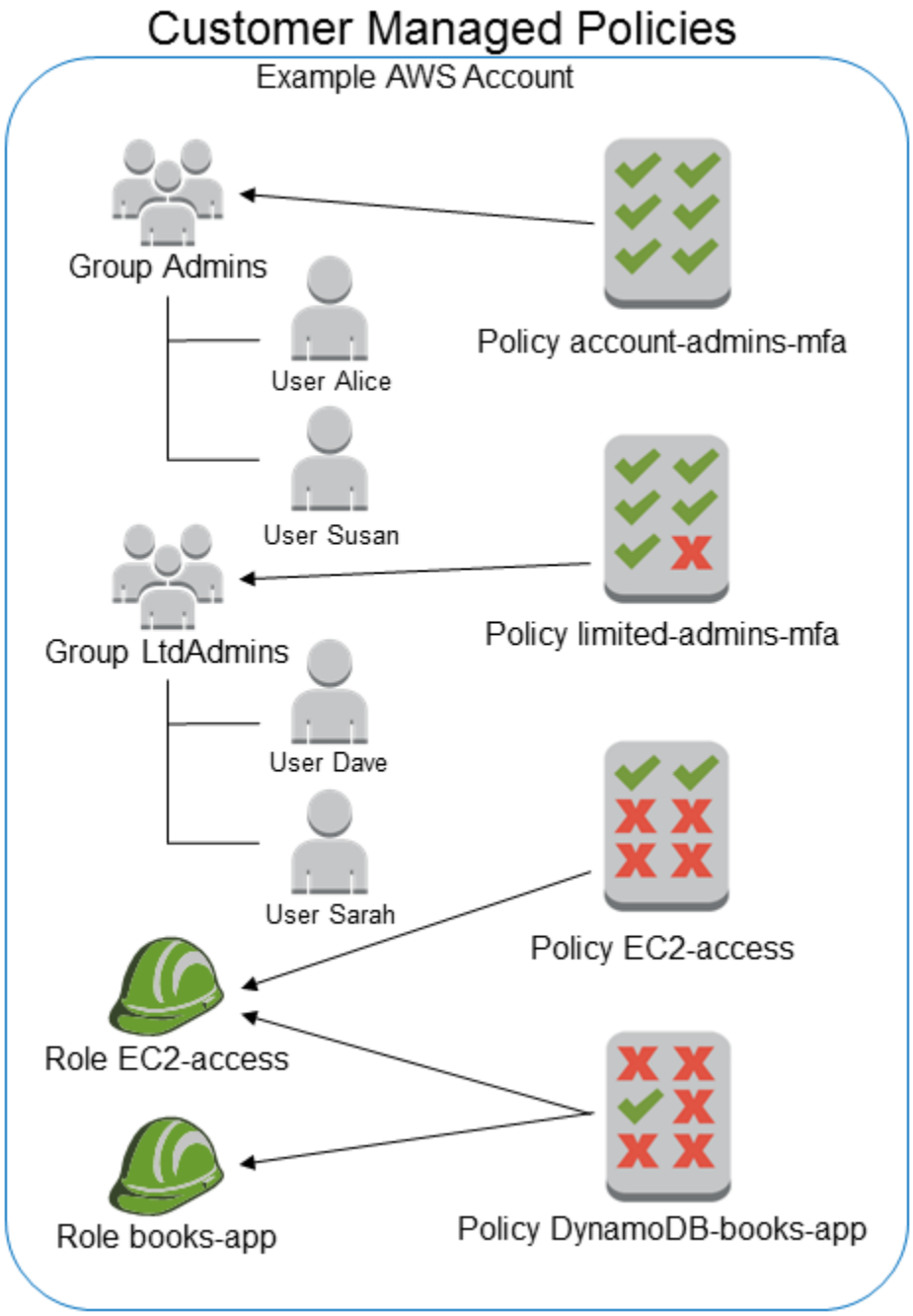


고객 관리형 정책

독립적인 정책은 사용자 자신의 AWS 계정에서 관리하도록 생성할 수도 있습니다. 이러한 정책을 고객 관리형 정책이라고 합니다. 이렇게 생성된 정책은 AWS 계정에 속한 다수의 보안 주체 엔터티에 추가할 수 있습니다. 정책을 보안 주체 엔터티에 추가할 경우 정책에서 정의한 권한까지 엔터티에게 부여하게 됩니다.

고객이 관리하는 정책을 생성하는 좋은 방법은 AWS에서 관리하는 기존의 정책을 복사하여 시작하는 것입니다. 이렇게 하면 시작 시 올바른 정책으로 시작하므로 해당 환경에 맞게 사용자 지정만 하면 됩니다.

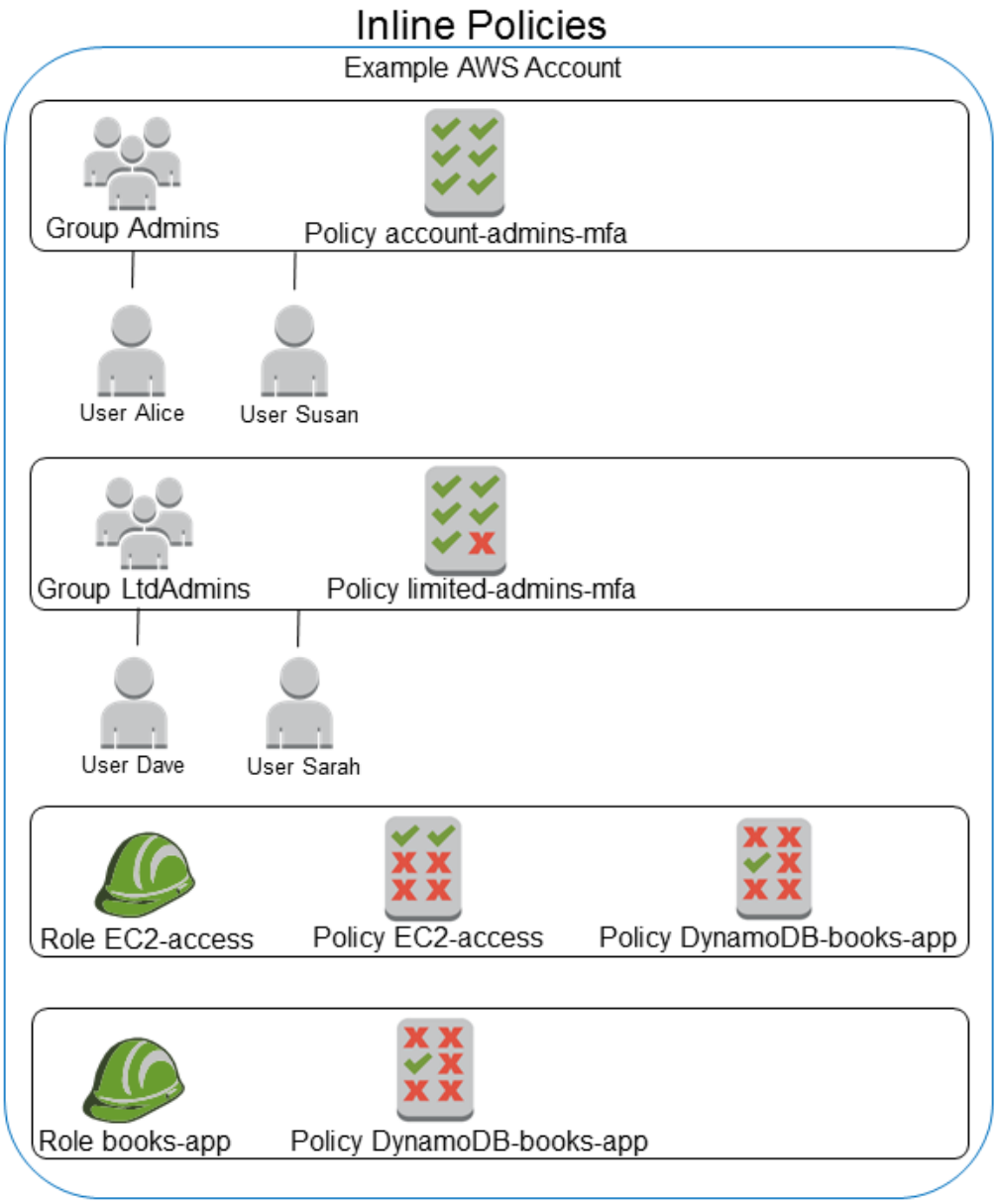
다음은 고객 관리형 정책을 나타낸 다이어그램입니다. 각 정책은 자체적으로 정책 이름이 포함된 Amazon 리소스 이름(ARN) (p. 564)을 갖고 있는 IAM 엔터티입니다. 다이어그램을 보면 동일한 정책을 여러 보안 주체 엔터티에 추가할 수 있습니다.—예를 들어 동일한 DynamoDB-books-app 정책이 2개의 다른 IAM 역할에 추가됩니다.



인라인 정책

인라인 정책은 IAM 자격 증명(사용자, 그룹 또는 역할)에 포함되는 정책입니다. 즉, 정책은 자격 증명의 고유한 부분입니다. 이 정책은 자격 증명 생성 시, 혹은 나중에라도 생성하여 자격 증명에 삽입할 수 있습니다.

다음은 인라인 정책을 나타낸 다이어그램입니다. 각 정책은 사용자, 그룹 또는 역할에서 내재된 부분입니다. 다이어그램을 보면 2개의 역할에 동일한 정책(the DynamoDB-books-app 정책)이 추가되어 있지만, 단 하나의 정책도 공유하지 않고 역할마다 자체적으로 정책 사본을 갖고 있습니다.



관리형 정책과 인라인 정책의 선택

정책 유형이 다르면 사용 사례도 다릅니다. 대부분 경우 인라인 정책보다는 관리형 정책의 사용을 권장합니다.

관리형 정책은 다음과 같은 기능을 제공합니다.

재사용성

단일 관리형 정책은 다수의 보안 주체 개체(사용자, 그룹 및 역할)에 추가할 수 있습니다. 실제로 정책 라이브러리를 생성하여 AWS 계정에 유용한 권한을 정의한 다음 필요에 따라 생성한 정책을 보안 주체 엔터티에 추가하는 것이 가능합니다.

중앙 변경 관리

관리형 정책 변경 시 정책이 추가되어 있는 모든 보안 주체 엔터티에 변경 사항이 적용됩니다. 예를 들어 AWS API 권한을 추가할 경우 관리형 정책을 업데이트하여 권한을 추가할 수 있습니다. (AWS 관리형 정책을 사용할 때는 AWS가 정책을 업데이트합니다) 정책이 업데이트되면 정책이 추가되어 있는 모든 보안 주체 엔터티에 변경 사항이 적용됩니다. 이와는 대조적으로 인라인 정책을 변경하려면 정책이 추가되어 있는 자격 증명을 일일이 편집해야 합니다. 예를 들어 그룹과 역할에 모두 동일한 인라인 정책이 추가되어 있더라도 정책을 변경하기 위해서는 두 보안 주체 개체를 개별적으로 편집해야만 합니다.

버전 관리 및 롤백

고객 관리 정책을 변경할 경우 변경된 정책은 기존 정책을 덮어쓰지 않습니다. 대신 IAM에서 관리형 정책의 새 버전을 만듭니다. IAM은 고객 관리 정책을 최대 5개 버전까지 저장합니다. 정책 버전은 필요에 따라 정책을 이전 버전으로 되돌리는 데도 사용됩니다.

정책 버전은 `Version` 정책 요소와 다릅니다. `Version` 정책 요소는 정책 내에서 사용되며 정책 언어의 버전을 정의합니다. 정책 버전에 대한 자세한 내용은 the section called “IAM 정책 버전 관리” (p. 458) 단원을 참조하십시오. `Version` 정책 요소에 대한 자세한 내용은 IAM JSON 정책 요소: Version (p. 587) 단원을 참조하십시오.

권한 위임 관리

정책으로 정의한 권한을 지속적으로 제어하면서 AWS 계정에 속한 사용자가 정책을 추가 및 분리하도록 허용할 수 있습니다. 실제로 일부 사용자에게는 전체 관리자 권한을 위임할 수 있습니다. 다시 말해, 전체 관리자란 정책을 생성, 업데이트 및 삭제할 수 있는 것을 말합니다. 제한된 관리자로서 다른 사용자를 지정할 수 있습니다. 다시 말해, 관리자는 다른 보안 주체 개체에게 정책을 추가할 수 있지만 이때 정책은 추가가 허용된 정책으로 제한됩니다.

권한 위임 관리에 대한 자세한 내용은 정책에 대한 액세스 제어 (p. 378) 단원을 참조하십시오.

AWS 관리형 정책의 자동 업데이트

AWS는 AWS 관리형 정책을 유지하면서 필요에 따라 자동으로 업데이트하기 때문에(예를 들어 새로운 AWS 서비스 권한을 추가하기 위해) 직접 변경할 필요가 없습니다. 업데이트는 AWS 관리형 정책을 추가한 보안 주체 엔터티에게 자동으로 적용됩니다.

인라인 정책 사용

인라인 정책은 정책과 정책이 추가된 자격 증명을 정확히 1대 1 관계로 유지할 때 유용합니다. 예를 들어 정책 권한을 의도하지 않은 자격 증명에 실수로 할당하는 일을 배제하려고 합니다. 이때 인라인 정책을 사용하면 정책 권한이 잘못된 자격 증명에 실수로 추가되는 일이 사라집니다. 그 밖에도 AWS Management 콘솔을 사용하여 자격 증명을 삭제할 경우 자격 증명에 삽입된 정책 역시 삭제됩니다. 정책도 보안 주체 개체의 일부이기 때문입니다.

사용되지 않는AWS 관리형 정책

권한 할당을 간편하게 하기 위해 AWS는 IAM 사용자, 그룹 및 역할에 연결할 수 있도록 사전에 정의된 관리형 정책 (p. 357)을 제공합니다.

새로운 서비스가 나왔을 때와 같이 AWS는 때때로 기존 정책에 새 권한을 추가해야 합니다. 기존 정책에 새 권한을 추가해도 특성이나 권한이 제거되거나 방해를 받지는 않습니다.

하지만 AWS는 필요한 변경이 기존 정책에 적용될 경우 고객에게 영향을 줄 수 있기 때문에 새로 정책을 만듭니다. 예를 들어 기존 정책에서 권한을 제거하면 이 정책을 사용하는 IAM 주체나 애플리케이션의 권한이 손상되어 중요한 작업에 방해가 될 수 있습니다.

따라서 이러한 변경이 필요할 경우 AWS는 해당 사항을 변경한 정책을 새로 만들어서 고객에게 제공합니다. 기존 정책은 사용되지 않음으로 표시됩니다. 사용되지 않는 관리형 정책은 IAM 콘솔의 정책 목록에서 옆에 경고 아이콘이 표시됩니다.

사용되지 않는 정책은 다음과 같은 특성을 갖습니다.

- 현재 연결된 모든 사용자, 그룹 및 역할에 계속 적용됩니다. 연결이 해제되지 않습니다.
- 새로운 사용자, 그룹 또는 역할에 연결할 수 없습니다. 현재 주체에서 연결을 해제할 경우 다시 연결할 수 없습니다.
- 현재의 모든 주체로부터 연결을 해제하면 더 이상 표시되지 않으며 어떤 경우에도 다시 사용할 수 없습니다.

사용자, 그룹 또는 역할에 정책이 필요할 경우 새로운 정책을 연결해야 합니다. 정책이 사용되지 않음으로 설정되었다고 알림을 받으면 모든 사용자, 그룹 및 역할을 대체 정책에 연결하고 사용되지 않는 정책으로부터 연결을 해제하는 것이 좋습니다. 사용되지 않는 정책을 계속 사용하면 위험이 수반될 수 있으므로 대체 정책으로 전환하는 것이 좋습니다.

IAM 엔터티에 대한 권한 경계

AWS에서는 IAM 엔터티(사용자 또는 역할)에 대한 권한 경계를 지원합니다. 권한 경계는 관리형 정책을 사용하여 자격 증명 기반 정책을 통해 IAM 엔터티에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 엔터티의 권한 경계는 자격 증명 기반 정책 및 관련 권한 경계 모두에서 허용되는 작업만 수행하도록 허용합니다.

정책 유형에 대한 자세한 정보는 정책 유형 (p. 349) 단원을 참조하십시오.

AWS 관리형 정책 또는 고객 관리형 정책을 사용하여 IAM 엔터티(사용자 또는 역할) 경계를 설정할 수 있습니다. 이 정책은 사용자 또는 역할에 대해 최대 권한을 제한합니다.

예를 들어, `ShirleyRodriguez`라는 IAM 사용자에 대해 Amazon S3, Amazon CloudWatch 및 Amazon EC2만 관리하도록 허용되어야 한다고 가정해 보겠습니다. 이 규칙을 시행하려면 다은 정책을 사용하여 `ShirleyRodriguez` 사용자의 권한 경계를 설정합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "cloudwatch:*",
                "ec2:*"
            ],
            "Resource": "*"
        }
    ]
}
```

정책을 사용하여 사용자 권한 경계를 설정하면 이 정책은 사용자 권한을 제한하지만 자체적으로 권한을 제공하지 않습니다. 이 예제에서 정책은 `ShirleyRodriguez`의 최대 권한을 Amazon S3, CloudWatch 및 Amazon EC2의 모든 작업으로 설정합니다. Shirley가 작업을 허용하는 권한 정책이 있다고 해도 IAM을 포함한 다른 서비스에서는 이 작업을 절대 수행할 수 없습니다. 예를 들어 다음 정책을 `ShirleyRodriguez` 사용자에게 추가할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:CreateUser",
    "Resource": "*"
  }
}
```

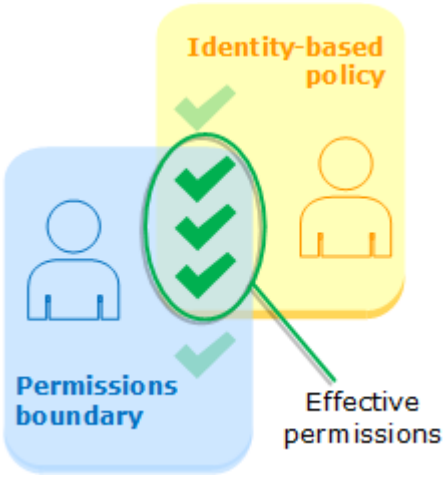
이 정책은 IAM에서 사용자 생성을 허용합니다. 이 권한 정책을 `ShirleyRodriguez` 사용자에 연결하고 Shirley가 사용자를 생성하고자 할 경우 작업은 실패합니다. 그 이유는 권한 경계가 `iam:CreateUser` 작업을 허용하지 않기 때문입니다. 이 두 가지 정책을 감안할 때 Shirley는 AWS에서 작업을 수행할 권한이 없습니다. 다른 서비스(예: Amazon S3)에서 작업을 허용하려면 다른 권한 정책을 추가해야 합니다. 또는 권한 경계를 업데이트하여 그녀에게 IAM에서 사용자를 생성하도록 허용할 수도 있습니다.

경계가 있는 효과적인 권한 평가

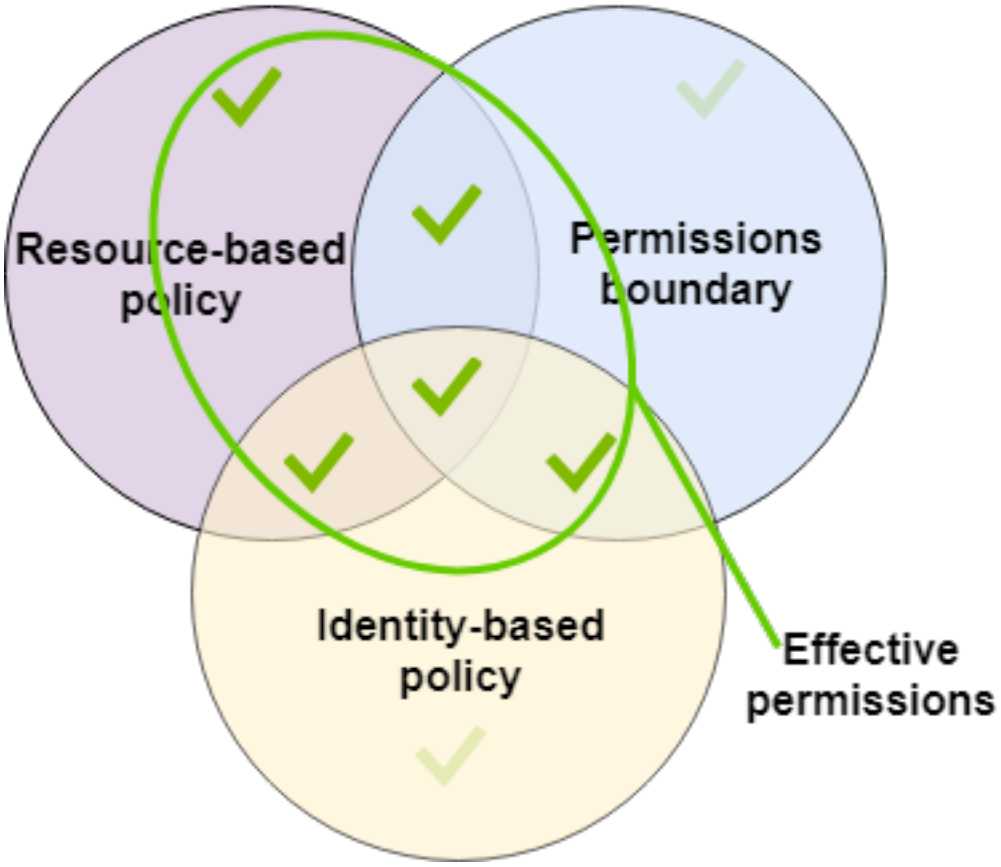
IAM 엔터티(사용자 또는 역할)에 대한 권한 경계는 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 사용자 또는 역할에 대한 효과적 권한을 변경할 수 있습니다. 사용자 또는 역할에 영향을 주는 모든 정책을 통해 부여되는 권한이 개체에 대한 유효 권한입니다. 계정 내에서 엔터티에 대한 권한은 자격 증명 기반 정책, 리소스 기반 정책, 권한 경계, 조직 SCP 또는 세션 정책에 영향을 받을 수 있습니다. 다양한 유형의 정책에 대한 자세한 정보는 정책 및 권한 (p. 349) 단원을 참조하십시오.

이러한 정책 유형 중 하나에서 작업에 대한 액세스가 명시적으로 거부된 경우 해당 요청이 거부됩니다. 여러 권한 유형에 의해 엔터티에 부여된 권한은 훨씬 더 복잡합니다. AWS의 정책 평가에 대한 자세한 정보는 정책 평가 로직 (p. 622) 단원을 참조하십시오.

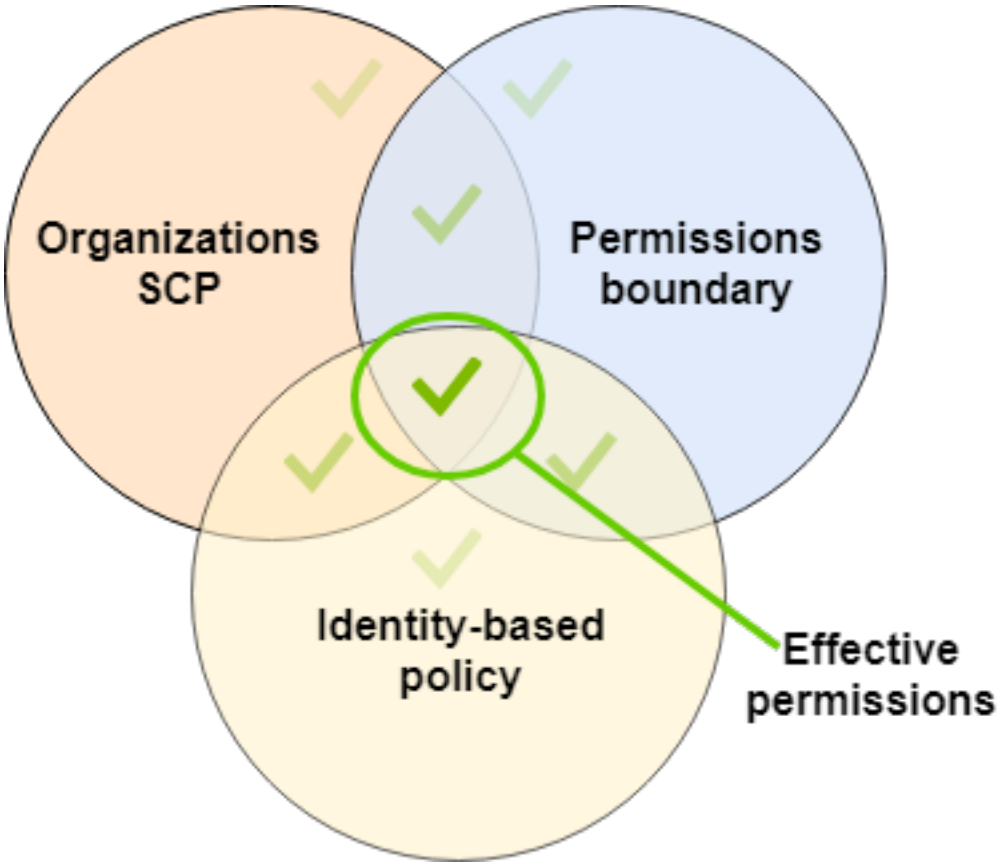
자격 증명 기반 정책과 경계 – 자격 증명 기반 정책은 사용자, 사용자 그룹 또는 역할에 연결된 인라인 또는 관리형 정책입니다. 자격 증명 기반 정책은 엔터티에 권한을 부여하며, 권한 경계는 이러한 권한을 제한합니다. 유효 권한은 두 정책 유형의 교집합입니다. 이들 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다.



리소스 기반 정책 – 리소스 기반 정책은 지정된 보안 주체가 정책이 연결된 리소스에 액세스하는 방식을 제어합니다. 계정 내에서 권한 경계의 암시적 거부는 리소스 기반 정책에서 부여한 권한을 제한하지 않습니다. 권한 경계가 자격 증명 기반 정책을 통해 엔터티에 부여된 권한을 축소하고 나서, 리소스 기반 정책이 엔터티에 추가 권한을 제공합니다. 이 경우, 유효 권한은 리소스 기반 정책이 허용하는 모든 권한 및 권한 경계와 자격 증명 기반 정책의 교집합입니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다.

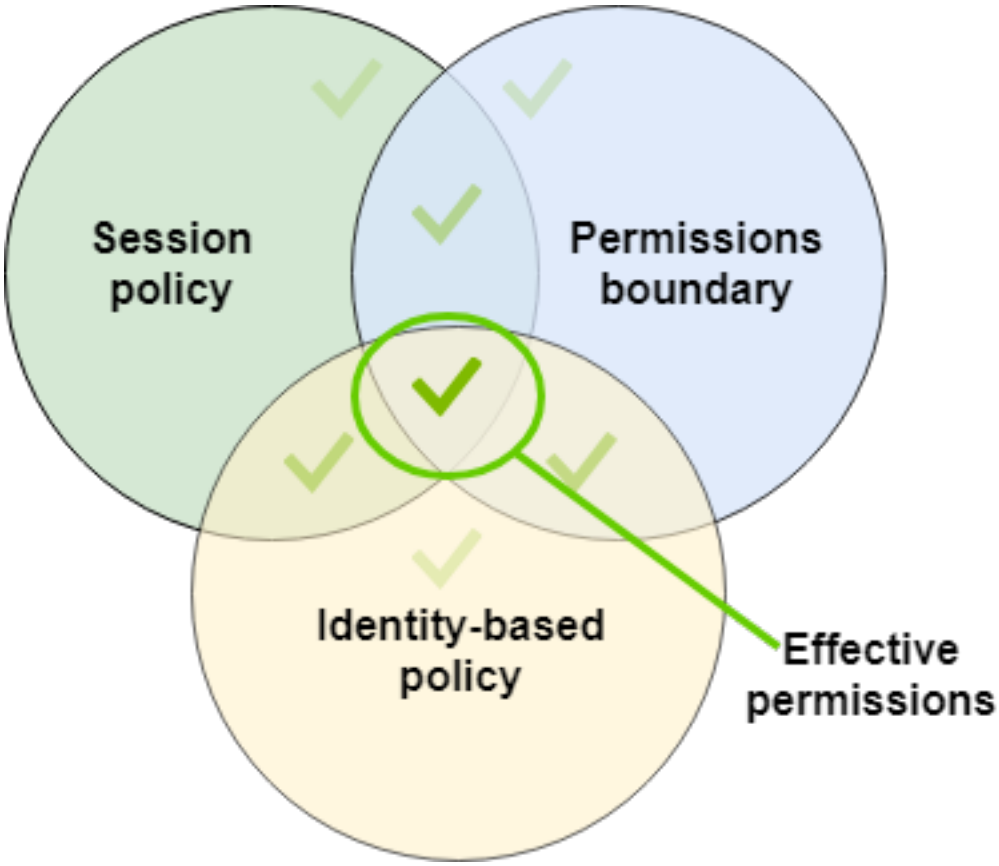


조직 SCP – SCP는 전체 AWS 계정에 적용됩니다. SCP는 해당 계정 내 보안 주체가 보낸 모든 요청에 대한 권한을 제한합니다. IAM 엔터티(사용자 또는 역할)는 SCP, 권한 경계 및 자격 증명 기반 정책의 영향을 받는 요청을 수행할 수 있습니다. 이 경우, 세 정책 유형 모두에서 허용하는 경우에만 해당 요청이 허용됩니다. 유효 권한은 세 정책 유형 모두의 교집합입니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다.



AWS Organizations에서 계정이 조직의 멤버인지 여부를 알아볼 수 있습니다. 조직 멤버가 SCP의 영향을 받을 수 있습니다. AWS CLI 명령 또는 AWS API 작업을 사용하여 이 데이터를 보려면 조직 엔터티에 대해 `organizations:DescribeOrganization` 작업 권한이 있어야 합니다. 조직 콘솔에서 작업을 수행할 추가 권한이 있어야 합니다. SCP가 특정 요청에 대한 액세스를 거부하는지 여부를 확인하거나 유효 권한을 변경하려면 AWS Organizations 관리자에게 문의하십시오.

세션 정책 – 세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 세션에 대한 권한은 세션을 생성하는 데 사용되는 IAM 엔터티(사용자 또는 역할)와 세션 정책에서 가져옵니다. 엔터티의 자격 증명 기반 정책 권한은 세션 정책과 권한 경계에 제한을 받습니다. 이 정책 유형 집합의 유효 권한은 세 정책 유형 모두의 교집합입니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 세션 정책에 대한 자세한 정보는 세션 정책을 참조하십시오.



권한 경계를 사용하여 다른 것에 책임 위임

권한 경계를 사용하여 사용자 생성과 같은 권한 관리 작업을 계정의 IAM 사용자에 위임할 수 있습니다. 이로써 권한의 특정 경계 내에서 다른 사용자가 작업을 대신 수행할 수 있는 권한이 부여됩니다.

예를 들어, María가 X-Company AWS 계정 관리자라고 가정하십시오. Maria가 Zhang에게 사용자 생성 업무를 위임하고자 합니다. 하지만 Zhang이 다음 회사 규칙에 따라 사용자를 생성하는지 확신해야 합니다.

- 사용자는 IAM를 사용하여 사용자, 그룹, 역할 또는 정책을 생성하고 관리할 수 없습니다.
- 사용자의 Amazon S3 `logs` 버킷 액세스가 거부되고 사용자가 `i-1234567890abcdef0`Amazon EC2 인스턴스로 액세스할 수 없습니다.
- 사용자는 사용자 자체 경계 정책을 제거할 수 없습니다.

이런 규칙을 시행하기 위해서는 María는 아래와 같은 세부 정보가 포함된 작업을 완료합니다.

1. María는 `XCompanyBoundaries` 관리형 정책을 생성하여 계정의 모든 새로운 사용자에 대한 권한 경계로서 사용할 수 있습니다.
2. María는 `DelegatedUserBoundary` 관리형 정책을 생성하여 Zhang에 대한 권한 경계로서 할당합니다. Maria는 관리자 IAM 사용자의 ARN을 기록하고 정책에서 사용하여 Zhang이 해당 ARN에 액세스하지 못하도록 합니다.
3. María는 `DelegatedUserPermissions` 관리형 정책을 생성하여 Zhang에 대한 권한 정책으로서 연결합니다.
4. María가 Zhang에서 그의 새로운 책임과 제한을 알려줍니다.

작업 1: María는 먼저 관리형 정책을 생성하여 새로운 사용자에 대한 경계를 정의해야 합니다. María는 Zhang이 사용자에게 필요한 권한 정책을 사용자에게 부여할 수 있도록 허용하지만 사용자를 제한하고자 합니다. 이렇게 하기 위해서는 마리아는 `XCompanyBoundaries`라는 다음 고객 관리형 정책을 생성합니다. 이 정책은 다음을 수행합니다.

- 사용자에게 여러 서비스에 대한 전체 액세스 권한을 부여
- IAM 콘솔에서 제한된 자체 관리 액세스 허용 즉, 콘솔에 로그인한 후 암호를 변경할 수 있습니다. 초기 암호를 설정할 수 없습니다. 이 작업을 허용하려면 `"*LoginProfile"` 작업을 `AllowManageOwnPasswordAndAccessKeys` 문에 추가합니다.
- 사용자가 Amazon S3 로그 버킷 또는 `i-1234567890abcdef0` Amazon EC2 인스턴스에 액세스하는 것을 금지

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ServiceBoundaries",
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "cloudwatch:*",
                "ec2:*",
                "dynamodb:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowIAMConsoleForCredentials",
            "Effect": "Allow",
            "Action": [
                "iam:ListUsers",
                "iam:GetAccountPasswordPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowManageOwnPasswordAndAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:*AccessKey*",
                "iam:ChangePassword",
                "iam:GetUser",
                "iam:*ServiceSpecificCredential*",
                "iam:*SigningCertificate*"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "DenyS3Logs",
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::logs",
                "arn:aws:s3:::logs/*"
            ]
        },
        {
            "Sid": "DenyEC2Production",
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "arn:aws:ec2:*:*:instance/i-1234567890abcdef0"
        }
```

```
    ]
}
```

각 설명문은 다른 목적이 있습니다.

1. 이 정책의 `ServiceBoundaries` 설명문은 지정된 AWS 서비스에 대한 완전한 액세스를 허용합니다. 이런 서비스의 새로운 사용자 작업이 사용자에 연결된 권한 정책에 따라서만 제한된다는 의미입니다.
2. `AllowIAMConsoleForCredentials` 문에서 모든 IAM 사용자를 나열할 수 있는 액세스를 허용합니다. 이 액세스는 AWS Management 콘솔의 사용자 페이지를 탐색하는 데 필요합니다. 또한 계정의 암호 요구 사항을 확인하도록 허용합니다. 이 액세스는 자신의 고유 암호를 변경할 때 필요합니다.
3. `AllowManageOwnPasswordAndAccessKeys` 문은 사용자가 자신의 고유 콘솔 암호와 프로그래밍 방식의 액세스 키만 관리하도록 허용합니다. 이는 Zhang 또는 다른 관리자가 새로운 사용자에게 전체 IAM 액세스를 포함하는 권한 정책을 부여할 때 중요합니다. 이 경우, 해당 사용자가 자신 또는 다른 사용자의 권한을 변경할 수 있습니다. 이 설명문은 이런 상황을 방지할 수 있습니다.
4. `DenyS3Logs` 설명문은 `logs` 버킷 액세스를 명시적으로 거부합니다.
5. `DenyEC2Production` 설명문은 `i-1234567890abcdef0` 인스턴스 액세스를 명시적으로 거부합니다.

작업 2: María는 Zhang이 모든 X-Company 사용자를 생성하도록 허용하지만 `XCompanyBoundaries` 권한 경계를 통해서만 허용하고자 합니다. 마리아는 `DelegatedUserBoundary`라는 다음 고객 관리형 정책을 생성합니다. 이런 정책은 Zhang이 가질 수 있는 최대 권한을 정의합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateOrChangeOnlyWithBoundary",
            "Effect": "Allow",
            "Action": [
                "iam:CreateUser",
                "iam:DeleteUserPolicy",
                "iam:AttachUserPolicy",
                "iam:DetachUserPolicy",
                "iam:PutUserPermissionsBoundary",
                "iam:PutUserPolicy"
            ],
            "Resource": "*",
            "Condition": {"StringEquals":
                {"iam:PermissionsBoundary": "arn:aws:iam::123456789012:policy/
XCompanyBoundaries"}}
        },
        {
            "Sid": "CloudWatchAndOtherIAMTasks",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:*",
                "iam:GetUser",
                "iam:ListUsers",
                "iam:DeleteUser",
                "iam:UpdateUser",
                "iam:CreateAccessKey",
                "iam:CreateLoginProfile",
                "iam:GetAccountPasswordPolicy",
                "iam:GetLoginProfile",
                "iam:ListGroups",
                "iam:ListGroupsForUser",
                "iam:CreateGroup",
                "iam:GetGroup",
                "iam:DeleteGroup",
                "iam:UpdateGroup",
                "iam:CreatePolicy",
```

```
                "iam:DeletePolicy",
                "iam:DeletePolicyVersion",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetUserPolicy",
                "iam:GetRolePolicy",
                "iam:ListPolicies",
                "iam:ListPolicyVersions",
                "iam:ListEntitiesForPolicy",
                "iam:ListUserPolicies",
                "iam:ListAttachedUserPolicies",
                "iam:ListRolePolicies",
                "iam:ListAttachedRolePolicies",
                "iam:SetDefaultPolicyVersion",
                "iam:SimulatePrincipalPolicy",
                "iam:SimulateCustomPolicy"
            ],
            "NotResource": "arn:aws:iam::123456789012:user/Maria"
        },
        {
            "Sid": "NoBoundaryPolicyEdit",
            "Effect": "Deny",
            "Action": [
                "iam:CreatePolicyVersion",
                "iam:DeletePolicy",
                "iam:DeletePolicyVersion",
                "iam:SetDefaultPolicyVersion"
            ],
            "Resource": [
                "arn:aws:iam::123456789012:policy/XCompanyBoundaries",
                "arn:aws:iam::123456789012:policy/DelegatedUserBoundary"
            ]
        },
        {
            "Sid": "NoBoundaryUserDelete",
            "Effect": "Deny",
            "Action": "iam:DeleteUserPermissionsBoundary",
            "Resource": "*"
        }
    ]
}
```

각 설명문은 다른 목적이 있습니다.

1. `CreateOrChangeOnlyWithBoundary` 설명문은 Zhang이 IAM 사용자를 생성하도록 허용하지만 장이 권한 경계를 설정할 때 `XCompanyBoundaries` 정책을 사용할 때만 가능합니다. 이 설명문은 또한 장이 기존 사용자에 대한 권한 경계를 설정하도록 허용하지만 장이 동일한 정책을 사용할 때만 가능합니다. 마지막으로, 이 설명문은 Zhang이 이 권한 경계 설정을 통해 사용자에 대한 권한 정책을 관리하도록 허용합니다.
2. `CloudWatchAndOtherIAMTasks` 설명문은 Zhang이 사용자, 그룹 및 정책 관리 작업을 완료하도록 허용합니다. 그는 조건 키에 나열되지 않은 IAM 사용자의 암호를 재설정하고 액세스 키를 생성할 수 있는 권한이 있습니다. 따라서 그는 사용자가 로그인 문제를 해결하도록 지원할 수 있습니다.
3. `NoBoundaryPolicyEdit` 설명문은 Zhang이 `XCompanyBoundaries` 정책을 업데이트할 수 있는 액세스를 거부합니다. 장은 자신 또는 다른 사용자에 대한 권한 경계를 설정하는 데 사용되는 어떤 정책도 변경할 수 없습니다.
4. `NoBoundaryUserDelete` 문에서는 Zhang이 자신 또는 다른 사용자에 대해 권한 경계를 삭제하기 위해 액세스할 때 이를 거부합니다.

그런 다음 María는 `Zhang` 사용자에 대한 권한 경계로서 (p. 98) `DelegatedUserBoundary` 정책을 할당합니다.

작업 3: 권한 경계가 최대 권한을 제한하지만 자체 액세스를 허용하지 않기 때문에 Maria는 Zhang에 대한 권한 정책을 생성해야 합니다. 마리아는 `DelegatedUserPermissions`라는 다음 정책을 생성합니다. 이 정책은 정의된 경계 내에서 Zhang이 수행할 수 있는 작업을 정의합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IAM",
            "Effect": "Allow",
            "Action": "iam:*",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLimited",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetDashboard",
                "cloudwatch:GetMetricData",
                "cloudwatch:ListDashboards",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3BucketContents",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::ZhangBucket"
        }
    ]
}
```

각 설명문은 다른 목적이 있습니다.

1. 정책의 `IAM` 설명문은 IAM에 대한 Zhang의 완전한 액세스를 허용합니다. 그러나, Zhang 권한 경계가 몇 가지 IAM 작업만 허용하기 때문에 Zhang의 효과적인 IAM 권한은 그의 권한 경계에 의해서만 제한됩니다.
2. `CloudWatchLimited` 설명문은 Zhang이 CloudWatch에서 5가지 작업을 수행할 수 있도록 허용합니다. Zhang 권한 경계는 CloudWatch의 모든 작업을 허용하기 때문에 그의 효과적인 CloudWatch 권한은 그의 권한 정책에 의해서만 제한됩니다.
3. `S3BucketContents` 설명문은 Zhang이 `ZhangBucket` Amazon S3 버킷을 나열할 수 있도록 허용합니다. 그러나, Zhang 권한 경계는 어떠한 Amazon S3 작업도 허용하지 않기 때문에 Zhang은 그의 권한 정책과 상관없이 어떠한 S3 작업을 수행할 수 없습니다.

   Note

   Zhang의 정책을 통해 그는 액세스할 수 없는 Amazon S3 리소스에 액세스할 수 있는 사용자를 만들 수 있습니다. Maria는 이러한 관리 작업을 위임하여 Amazon S3에 대한 액세스 권한이 있는 Zhang을 효과적으로 신뢰합니다.

그러면 María는 `DelegatedUserPermissions` 정책을 `Zhang` 사용자에 대한 권한 정책으로서 연결합니다.

작업 4: María는 새로운 사용자를 생성하도록 Zhang에게 지침을 내립니다. María는 Zhang에게 새로운 사용자가 원하는 모든 권한을 통해 새로운 사용자를 생성할 수 있지만 `XCompanyBoundaries` 정책을 권한 경계로서 할당해야 한다고 말합니다.

Zhang은 다음 작업을 완료합니다.

1. Zhang은 AWS Management 콘솔로 사용자를 생성 (p. 88)합니다. 그는 사용자 이름 `Nikhil`를 입력하고 사용자에 대한 콘솔 액세스를 가능하게 합니다. 위의 정책은 Zhang이 IAM 콘솔에 로그인한 후에만 암호를 변경할 수 있으므로 Requires password reset(암호 재설정 필요) 옆의 확인란 선택을 취소합니다.
2. 권한 설정 페이지에서 Zhang은 Nikhil가 업무를 할 수 있도록 허용하는 IAMFullAccess 및 AmazonS3ReadOnlyAccess 권한 정책을 선택합니다.
3. Zhang은 María의 지침을 잊고 Set permissions boundary(권한 경계 설정) 섹션을 넘깁니다.
4. Zhang은 사용자 세부 정보를 검토하고 사용자 생성을 선택합니다.

   작업은 실패하고 액세스는 거부됩니다. Zhang의 `DelegatedUserBoundary` 권한 경계는 그가 생성하는 어떠한 사용자도`XCompanyBoundaries` 정책을 권한 경계로서 가지고 있어야 합니다.
5. Zhang은 이전 페이지로 돌아갑니다. 그는 Set permissions boundary(권한 경계 설정) 페이지에서 `XCompanyBoundaries` 정책을 선택합니다.
6. Zhang은 사용자 세부 정보를 검토하고 사용자 생성을 선택합니다.

   사용자가 생성됩니다.

Nikhil이 로그인할 경우, 그는 권한 경계에 의해 거부된 작업 이외의 IAM 및 Amazon S3에 액세스할 수 있습니다. 예를 들어, 그는 IAM에 자신의 암호를 변경할 수 있지만 다른 사용자를 생성하거나 그의 정책을 편집할 수 없습니다. Nikhil은 Amazon S3에 대한 읽기 전용 액세스 권한이 있습니다.

누군가가 `logs` 버킷에 Nikhil이 버킷에 객체를 넣을 수 있도록 허용하는 리소스 기반 정책을 추가하더라도 그는 여전히 이 버킷에 액세스할 수 없습니다 `logs` 버킷에 대한 작업이 권한 경계에 의해 명시적으로 거부되었기 때문입니다. 정책 유형에 포함된 명시적 거부로 인해 요청이 거부됩니다. 하지만 Secrets Manager 암호에 연결된 리소스 기반 정책이 Nikhil이 `secretsmanager:GetSecretValue` 작업을 수행하도록 허용하는 경우 Nikhil은 암호를 불러와서 암호화를 해제할 수 있습니다. 그 이유는 Secrets Manager 작업이 Nikhill의 권한 경계에 의해 명시적으로 거부되지 않았고 권한 경계에서의 묵시적 거부가 리소스 기반 정책을 제한하지 않기 때문입니다.

자격 증명 기반 정책 및 리소스 기반 정책

정책은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 AWS의 객체입니다. 리소스에 대한 액세스를 제한하는 권한 정책을 생성할 때 자격 증명 기반 정책 또는 리소스 기반 정책을 선택할 수 있습니다.

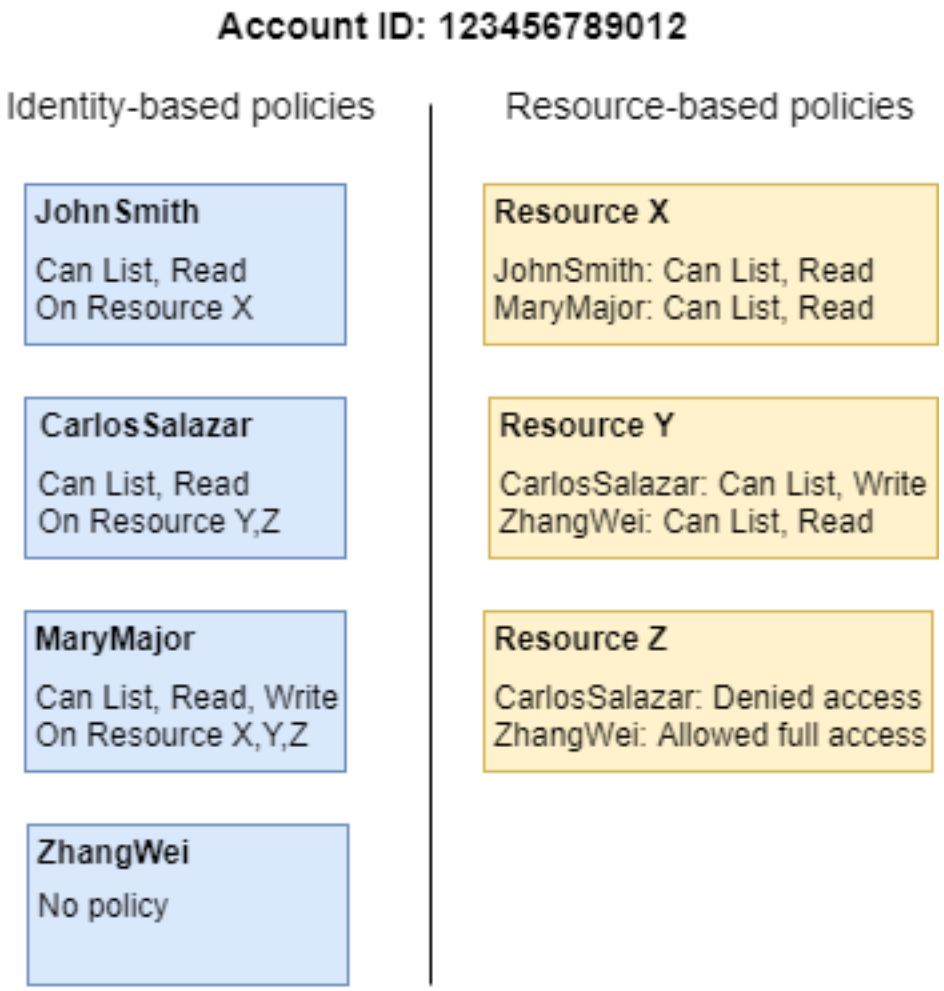
자격 증명 기반 정책은 IAM 사용자, 그룹 또는 역할에 연결됩니다. 이러한 정책으로 자격 증명이 수행할 수 있는 작업(권한)을 지정할 수 있습니다. 예를 들어, John이라는 IAM 사용자에게 Amazon EC2 `RunInstances` 작업을 수행하도록 허용하는 정책을 연결할 수 있습니다. 이 정책은 John이 `MyCompany`라는 Amazon DynamoDB 테이블에서 항목을 가져오도록 허용되었다는 내용도 명시할 수 있습니다. 또한 John에게 자신의 IAM 보안 자격 증명을 관리하도록 허용할 수도 있습니다. 자격 증명 기반 정책은 관리형 권한 또는 인라인 권한 (p. 357)이 될 수 있습니다.

리소스 기반 정책은 리소스에 연결됩니다. 예를 들어, Amazon S3 버킷, Amazon SQS 대기열 및 AWS Key Management Service 암호화 키에 리소스 기반 정책을 연결할 수 있습니다. 리소스 기반 정책을 지원하는 서비스 목록은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

리소스 기반 정책을 사용하면 이러한 리소스에 액세스할 수 있는 대상 및 해당 대상이 리소스에서 수행할 수 있는 작업을 지정할 수 있습니다. 해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오. 리소스 기반 정책은 인라인 정책으로, 관리형이 아닙니다.

> **Note**
>
> 리소스 기반 정책은 리소스 수준 권한과 다릅니다. 이 주제에서 설명한 바와 같이 리소스 기반 정책을 리소스에 직접 연결할 수 있습니다. 리소스 수준 권한이란 ARN (p. 564)을 사용하여 정책에서 개별 리소스를 지정하는 기능을 말합니다. 리소스 기반 정책은 일부 AWS 서비스에서만 지원됩니다. 리소스 기반 정책 및 리소스 수준 권한을 지원하는 서비스 목록은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

이러한 개념에 대한 이해도를 높이려면 다음 그림 단원을 참조하십시오. `123456789012` 계정의 관리자는 `JohnSmith`, `CarlosSalazar` 및 `MaryMajor` 사용자에게 자격 증명 기반 정책을 연결했습니다. 이 정책의 일부 작업은 특정 리소스에서 수행할 수 있습니다. 예를 들어 사용자 `JohnSmith`는 `Resource X`에 대해 일부 작업을 수행할 수 있습니다. 이는 자격 증명 기반 정책에서 리소스 수준 권한입니다. 관리자는 또한 리소스 기반 정책을 `Resource X`, `Resource Y` 및 `Resource Z`에 추가했습니다. 리소스 기반 정책을 통해 해당 리소스에 액세스할 수 있는 사용자를 지정할 수 있습니다. 예를 들어 `Resource X`의 리소스 기반 정책은 `JohnSmith` 및 `MaryMajor` 사용자 목록을 표시하고 리소스에 대한 읽기 권한을 허용합니다.



`123456789012` 계정의 예를 사용하면 다음 사용자가 나열된 작업을 수행할 수 있습니다.

- JohnSmith – John은 `Resource X`에서 나열 및 읽기 작업을 수행할 수 있습니다. John은 사용자에 대한 자격 증명 기반 정책과 `Resource X`에 대한 리소스 기반 정책을 통해 이 권한을 부여 받습니다.
- CarlosSalazar – Carlos는 `Resource Y`에서 나열, 읽기 및 쓰기 작업을 수행할 수 있지만 `Resource Z`에 대한 액세스는 거부됩니다. Carlos의 자격 증명 기반 정책을 통해 `Resource Y`에서 나열 및 읽기 작업을 수행할 수 있습니다. `Resource Y` 리소스 기반 정책을 사용하면 Carlos에게 쓰기 권한도 허용됩니다. 그러나 자격 증명 기반 정책을 통해 `Resource Z`에 대한 액세스가 허용되더라도 `Resource Z` 리소스 기반 정책으로 인해 해당 액세스가 거부됩니다. 명시적 `Deny`는 `Allow`를 재정의하므로 Carlos의 `Resource Z`에 대한 액세스가 거부됩니다. 자세한 정보는 정책 평가 로직 (p. 622) 단원을 참조하십시오.
- MaryMajor – Mary는 `Resource X`, `Resource Y` 및 `Resource Z`에 대해 나열, 읽기 및 쓰기 작업을 수행할 수 있습니다. Mary의 자격 증명 기반 정책을 통해 리소스 기반 정책보다 더 많은 리소스에 대해 더 많은 작업을 수행할 수 있지만 액세스를 거부하는 정책은 없습니다.

- ZhangWei – Zhang에게는 `Resource Z`에 대한 모든 액세스 권한이 있습니다. Zhang은 자격 증명 기반 정책이 없지만 `Resource Z` 리소스 기반 정책을 사용하면 리소스에 대한 전체 액세스 권한을 가질 수 있습니다. Zhang은 `Resource Y`에서 나열 및 읽기 작업을 수행할 수도 있습니다.

자격 증명 기반 정책과 리소스 기반 정책은 모두 권한 정책이며 함께 평가됩니다. 권한 정책만 적용되는 요청의 경우 AWS는 먼저 모든 정책에서 `Deny`를 확인합니다. 이 정책이 존재하는 경우 요청이 거부됩니다. 그런 다음 AWS는 각 `Allow`를 확인합니다. 적어도 하나의 정책 설명이 요청의 작업을 허용하는 경우 요청이 허용됩니다. `Allow`가 자격 증명 기반 정책인지 리소스 기반 정책인지는 중요하지 않습니다.

> **Important**
>
> 이 논리는 요청이 하나의 AWS 계정에서 이루어진 경우에만 적용됩니다. 하나의 계정에서 다른 계정으로 요청한 경우 `Account A`의 요청자는 `Account B`의 리소스에 대한 요청을 허용하는 자격 증명 기반 정책을 가지고 있어야 합니다. 또한 `Account B`의 리소스 기반 정책은 `Account A`의 요청자가 리소스에 액세스할 수 있도록 허용해야 합니다. 두 계정 모두에 작업을 허용하는 정책이 있어야 합니다. 그렇지 않으면 요청이 실패합니다. 교차 계정 액세스에 대해 리소스 기반 정책을 사용하는 방법에 대한 자세한 정보는 IAM 역할과 리소스 기반 정책의 차이 (p. 287) 단원을 참조하십시오.

특정 권한이 있는 사용자는 해당 권한에 연결된 권한 정책이 있는 리소스를 요청할 수 있습니다. 이 경우 AWS는 해당 리소스에 대한 액세스 권한을 부여할지 여부를 결정할 때 두 권한 세트를 모두 평가합니다. 정책이 평가되는 방식에 대한 자세한 정보는 정책 평가 로직 (p. 622) 단원을 참조하십시오.

> **Note**
>
> Amazon S3는 자격 증명 기반 정책 및 리소스 기반 정책(버킷 정책이라고 함)을 지원합니다. 또한 Amazon S3은 IAM 정책 및 권한과 독립적인 ACL(액세스 제어 목록)이라는 권한 메커니즘을 지원합니다. IAM 정책을 Amazon S3 ACL과 함께 사용할 수 있습니다. 자세한 정보는 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 단원을 참조하십시오.

정책을 사용하여 액세스 제어

정책을 사용하여 IAM 또는 모든 AWS 내 리소스에 대한 액세스를 제어할 수 있습니다.

정책 (p. 349)을 사용하여 AWS에서 액세스를 제어하려면 AWS이 액세스를 부여하는 방식을 이해해야 합니다. AWS는 리소스 모음으로 구성되어 있습니다. IAM 사용자는 리소스입니다. Amazon S3 버킷도 리소스입니다. AWS API, AWS CLI 또는 AWS Management 콘솔을 사용하여 작업을 수행할 경우(예: 사용자 생성) 해당 작업에 대한 요청을 전송합니다. 이 요청은 작업, 리소스, 보안 주체 엔터티(사용자 또는 역할), 보안 주체 계정 및 필요한 요청 정보를 지정합니다. 이러한 모든 정보는 콘텍스트를 제공합니다.

그런 다음 AWS은 사용자(보안 주체)가 지정된 리소스에 대해 지정된 작업을 수행할 수 있도록 인증(로그인) 및 권한 부여(권한 있음)되었는지 확인합니다. 권한을 부여하는 동안 AWS는 요청 콘텍스트에 적용되는 모든 정책을 확인합니다. 대부분의 정책은 AWS에 JSON 문서 (p. 354)로 저장되며 보안 주체 엔터티에 대한 권한을 지정합니다. 정책 유형 및 활용에 대한 자세한 내용은 정책 및 권한 (p. 349) 단원을 참조하십시오.

AWS는 정책이 요청의 각 부분을 허용한 경우에만 요청에 권한을 부여합니다. 이러한 프로세스의 다이어그램을 보려면 IAM 작동 방식 이해 (p. 3) 단원을 참조하십시오. AWS가 요청이 허용되는지 여부를 결정하는 방법에 대한 자세한 정보는 정책 평가 로직 (p. 622) 단원을 참조하십시오.

IAM 정책을 생성하면 다음에 대한 액세스를 제어할 수 있습니다.

- 보안 주체 (p. 375) – 요청하는 사용자(보안 주체 (p. 5))가 수행하도록 허용된 사항을 제어합니다.
- IAM 자격 증명 (p. 376) – 어떤 IAM 자격 증명(그룹, 사용자 및 역할)에 액세스할 수 있는지 및 그 방법을 제어합니다.
- IAM 정책 (p. 378) – 고객 관리형 정책을 생성, 편집 및 삭제할 수 있는 대상과 모든 관리형 정책을 연결하고 분리할 수 있는 대상을 제어합니다.
- AWS 리소스 (p. 381) – 자격 증명 기반 정책 또는 리소스 기반 정책을 사용하여 리소스에 액세스할 수 있는 대상을 제어합니다.

- AWS 계정 (p. 381) – 요청이 특정 계정의 멤버에만 허용되는지 여부를 제어합니다.

이러한 정책을 사용하여 AWS 리소스에 액세스할 수 있는 대상과 액세스한 대상이 리소스에서 수행할 수 있는 작업을 지정할 수 있습니다. 모든 IAM 사용자는 처음에 권한이 없습니다. 다시 말해, 기본적으로 사용자는 아무 작업도 할 수 없으며, 심지어 자신의 액세스 키를 볼 수도 없습니다. 사용자에게 작업을 수행할 권한을 부여하기 위해 사용자에게 권한을 추가(즉 사용자에게 정책 연결)하거나 의도한 권한을 보유한 그룹에 사용자를 추가할 수 있습니다.

예를 들어, 자신의 액세스 키를 나열할 사용자 권한을 부여할 수 있습니다. 해당 권한을 확장하여 각 사용자가 자신의 키를 생성, 업데이트 및 삭제하도록 할 수도 있습니다.

그룹에 권한을 부여하면 그룹에 속한 모든 사용자가 해당 권한을 얻습니다. 예를 들어, Administrators 그룹에 IAM 계정 리소스에서 AWS 작업을 수행할 권한을 부여할 수 있습니다. 또 다른 예로 Managers 그룹에 AWS 계정의 Amazon EC2 인스턴스를 설명할 권한을 부여할 수 있습니다.

사용자, 그룹 및 역할에 기본 권한을 위임하는 방법에 대한 자세한 정보는 IAM 리소스에 액세스하는 데 필요한 권한 (p. 507) 단원을 참조하십시오. 기본 권한을 보여주는 정책의 예를 더 보려면 IAM 리소스를 관리하기 위한 정책의 예 (p. 510) 단원을 참조하십시오.

보안 주체에 대한 액세스 제어

정책을 사용하여 요청하는 사용자(보안 주체)가 수행하도록 허용된 사항을 제어할 수 있습니다. 이렇게 하려면 자격 증명 기반 정책을 해당 사용자의 자격 증명(사용자, 사용자 그룹 또는 역할)에 연결해야 합니다. 또한 권한 경계 (p. 363)를 사용하여 엔터티(사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정할 수 있습니다.

예를 들어 사용자 Zhang Wei의 CloudWatch, Amazon DynamoDB, Amazon EC2 및 Amazon S3에 대한 완전한 액세스를 허용하고자 한다고 가정해보십시오. 다른 사용자에 대해 권한 세트 한 개가 필요한 경우 나중에 분리할 수 있도록 두 가지 다른 정책을 생성할 수 있습니다. 또는 모든 권한을 단일 정책으로 모은 다음 이 정책을 이름이 Zhang Wei인 IAM 사용자에게 연결할 수 있습니다. 정책을 Zhang Wei가 속한 그룹 또는 Zhang Wei가 수임하는 역할에 연결할 수도 있습니다. 그 결과, Zhang이 S3 버킷의 내용을 볼 경우 해당 요청이 허용됩니다. 새 IAM 사용자를 생성하려고 시도할 경우에는 권한이 없으므로 요청이 거부됩니다.

Zhang의 권한 경계를 사용하여 Zhang에게 `CompanyConfidential` S3 버킷으로의 액세스 권한을 부여해야 합니다. 이렇게 하기 위해서는 Zhang에게 부여하고자 하는 최대 권한을 결정합니다. 이런 경우, Zhang이 그의 권한 정책으로 하는 일을 제어합니다. 여기서는 Zhang이 기밀 버킷으로 액세스하지만 않도록 신경 씁니다. 따라서 다음 정책을 사용하여 Zhang의 경계를 정의하여 Amazon S3에 대한 모든 AWS 작업 및 몇 가지 기타 서비스를 허용하지만 `CompanyConfidential` S3 버킷으로의 액세스는 거부합니다. 권한 경계가 모든 IAM 작업을 허용하지 않기 때문에 권한 경계는 Zhang이 그의(또는 어떠한 사람의) 경계를 삭제하지 못하도록 방지합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SomeServices",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:*",
                "dynamodb:*",
                "ec2:*",
                "s3:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "NoConfidentialBucket",
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
```

```
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

이 사용자에 대한 권한 경계처럼 정책을 할당할 경우 어떠한 권한도 허용하지 않는다는 점을 유의하십시오. 권한 경계는 자격 증명 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 권한 경계에 대한 자세한 정보는 IAM 엔터티에 대한 권한 경계 (p. 363) 단원을 참조하십시오.

이전 절차에 대한 자세한 정보는 이러한 리소스 단원을 참조하십시오.

- 보안 주체에 연결할 수 있는 IAM 정책의 생성에 대해 자세히 알아보려면 IAM 정책 만들기 (p. 435) 단원을 참조하십시오.
- 보안 주체에 IAM 정책을 연결하는 방법에 대해 자세히 알아보려면 IAM 자격 증명 권한 추가 및 제거 (p. 450) 단원을 참조하십시오.
- EC2에 전체 액세스 권한을 부여하는 예제 정책을 보려면 Amazon EC2: 특정 리전 내에서의 모든 EC2 액세스를 프로그래밍 방식으로 콘솔에서 허용 (p. 409) 단원을 참조하십시오.
- S3 버킷에 읽기 전용 액세스를 허용하려면 Amazon S3: S3 버킷에 있는 객체에 대한 읽기 및 쓰기 액세스 권한을 프로그래밍 방식으로 콘솔에서 허용 (p. 434) 예제 정책의 첫 번째 두 설명문을 사용하십시오.
- 사용자에게 콘솔 암호, 프로그래밍 방식 액세스 키, MFA 디바이스 등 본인의 자격 증명을 설정 또는 교체할 수 있도록 허용하는 예제 정책을 보려면 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391) 단원을 참조하십시오.

자격 증명에 대한 액세스 제어

IAM 정책에서 그룹 전반의 모든 사용자에게 연결하는 정책을 생성함으로써 사용자가 자격 증명에 대해 수행할 수 있는 사항을 제어할 수 있습니다. 이렇게 하려면 자격 증명에 수행할 수 있는 사항 또는 자격 증명에 액세스할 수 있는 대상을 제어하는 정책을 생성합니다.

예를 들어, 이름이 AllUsers인 그룹을 생성한 다음 해당 그룹을 모든 사용자에 연결할 수 있습니다. 그룹을 생성할 때 이전 섹션에서 설명한 대로 모든 사용자에게 자격 증명을 교체하기 위한 액세스 권한을 부여할 수 있습니다. 그런 다음 정책 조건에 사용자 이름이 포함되지 않은 경우 그룹을 변경하는 액세스를 거부하는 정책을 생성할 수 있습니다. 그러나 정책에서 이 부분은 나열된 사용자를 제외한 모든 사용자의 액세스만 거부합니다. 또한 그룹 사용자 모두에 대한 모든 그룹 관리 작업을 허용하는 권한을 포함해야 합니다. 마지막으로, 모든 사용자에게 적용되도록 이 정책을 그룹에 연결합니다. 그 결과, 정책에 지정되지 않은 사용자가 그룹을 변경하려고 하면 해당 요청이 거부됩니다.

시각적 편집기를 사용하여 이 정책을 생성하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.

   정책를 처음으로 선택하는 경우 Welcome to Managed Policies 페이지가 나타납니다. [Get Started]를 선택합니다.
3. [Create policy]를 선택합니다.
4. Visual editor(시각적 편집기) 탭에서 Choose a service(서비스 선택)을 선택하여 시작합니다. 그런 다음 IAM을 선택합니다.
5. Select actions(작업 선택)을 선택한 다음 검색 상자에 **`group`**을 입력합니다. 시각적 편집기에 `group`이라는 단어가 포함된 모든 IAM 작업이 표시됩니다. 모든 확인란을 선택합니다.
6. 리소스를 선택하여 정책에 대한 리소스를 지정합니다. 선택한 작업에 따라 group, group-path 및 user 리소스 유형이 표시됩니다.

- group – Add ARN(ARN 추가)를 선택합니다. 리소스에서 모두 선택 옆에 있는 확인란을 선택합니다. Group Name With Path(그룹 이름과 경로)에서 그룹 이름 **`AllUsers`**를 입력합니다. 그런 다음 추가를 선택합니다.
- group-path – 모두 선택 옆에 있는 확인란을 선택합니다.
- user – 모두 선택 옆에 있는 확인란을 선택합니다.

선택한 작업 중 하나인 `ListGroups`는 특정 리소스 사용을 지원하지 않습니다. 해당 작업에서 All resources(모든 리소스)를 선택할 필요가 없습니다. 정책을 저장하거나 JSON 탭에서 정책을 보는 경우 IAM이 모든 리소스에 대해 이 작업 권한을 부여하는 새 권한 블록을 자동으로 생성하는 것을 확인할 수 있습니다.

7. 다른 권한 블록을 추가하려면 Add additional permissions(권한 추가)를 선택합니다.
8. Choose a service(서비스 선택)을 선택한 다음 IAM을 선택합니다.
9. Select actions(작업 선택)을 선택한 다음 Switch to deny permissions(권한 거부로 전환)을 선택합니다. 이렇게 하면 권한을 거부할 때 전체 블록이 사용됩니다.
10. 검색 상자에 **`group`**을 입력합니다. 시각적 편집기에 `group`이라는 단어가 포함된 모든 IAM 작업이 표시됩니다. 다음 작업 옆에 있는 확인란을 선택합니다.
    - CreateGroup
    - DeleteGroup
    - RemoveUserFromGroup
    - AttachGroupPolicy
    - DeleteGroupPolicy
    - DetachGroupPolicy
    - PutGroupPolicy
    - UpdateGroup
11. 리소스를 선택하여 정책에 대한 리소스를 지정합니다. 선택한 작업에 따라 group 리소스 유형이 표시됩니다. Add ARN(ARN 추가)를 선택합니다. 리소스에서 모두 선택 옆에 있는 확인란을 선택합니다. Group Name With Path(그룹 이름과 경로)에서 그룹 이름 **`AllUsers`**를 입력합니다. 그런 다음 추가를 선택합니다.
12. Specify request conditions(optional)(요청 조건 지정(선택 사항))을 선택한 다음 조건 추가를 선택합니다. 다음 값을 사용하여 양식 입력을 완료합니다.
    - 키 – aws:username을 선택합니다.
    - 한정어 – 기본값을 선택합니다.
    - 연산자 – StringNotEquals를 선택합니다.
    - 값 – **`srodriguez`** 를 입력한 다음 Add another condition value(다른 조건 값 추가)를 선택합니다. **`mjackson`**을 입력한 다음 Add another condition value(다른 조건 값 추가)를 선택합니다. **`adesai`**를 입력한 다음 추가를 선택합니다.

    이 조건은 호출한 사용자가 목록에 포함되지 않은 경우 지정된 그룹 관리 작업 액세스가 거부됩니다. 이는 명시적으로 권한을 거부하므로 해당 사용자가 작업을 호출할 수 있도록 허용된 이전 블록을 무시합니다. 목록에 있는 사용자는 액세스가 거부되지 않으며 첫 번째 권한 블록의 권한이 부여되므로 그룹을 전체적으로 관리할 수 있습니다.
13. 작업이 완료되면 [Review policy]를 선택합니다.

    Note

    언제든지 Visual editor(시각적 편집기) 및 JSON 탭을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 정보는 정책 재구성 (p. 538) 단원을 참조하십시오.

14. 정책 검토 페이지에서 이름에 **`LimitAllUserGroupManagement`**를 입력합니다. 설명에 **`Allows all users Read-only access to a specific group, and allows only specific users access to make changes to the group`**을 입력합니다. 정책 요약을 검토하여 의도한 권한을 부여했는지 확인합니다. 그런 다음 정책 생성을 선택하여 새 정책을 저장합니다.
15. 그룹에 정책을 연결합니다. 자세한 정보는 IAM 자격 증명 권한 추가 및 제거 (p. 450) 단원을 참조하십시오.

또는 이러한 예제 JSON 정책 문서를 사용하여 동일한 정책을 생성할 수 있습니다. 이 JSON 정책을 보려면 IAM: 특정 IAM 사용자가 프로그래밍 방식으로, 그리고 콘솔에서 그룹을 관리하도록 허용 (p. 420) 단원을 참조하십시오. JSON 문서를 사용하여 정책을 생성하는 자세한 지침은 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

정책에 대한 액세스 제어

사용자가 AWS 관리형 정책을 적용하는 방식을 제어할 수 있습니다. 이렇게 하려면 이 정책을 모든 사용자에게 연결합니다. 이 작업에 그룹을 사용하는 것이 좋습니다.

예를 들어, 사용자가 새 IAM 사용자, 그룹 또는 역할에 IAMUserChangePassword 및 PowerUserAccess AWS 관리형 정책만 연결하도록 허용하는 정책을 생성할 수 있습니다.

고객 관리형 정책의 경우 이러한 정책을 생성, 업데이트 및 삭제할 수 있는 대상을 제어할 수 있습니다. 정책을 보안 주체 개체(그룹, 사용자 및 역할)에 연결하고 해당 개체에서 분리할 수 있는 대상을 제어할 수 있습니다. 또한 사용자가 어떤 정책을 어떤 주체에 연결하거나 분리할지 제어할 수 있습니다.

예를 들어 계정 관리자에게 정책을 생성, 업데이트 및 삭제할 권한을 부여할 수 있습니다. 그런 다음 팀 리더 또는 기타 제한된 관리자에게 제한된 관리자가 관리하는 보안 주체 개체에 이러한 정책을 연결하고 분리할 권한을 부여합니다.

자세한 정보는 다음 리소스 단원을 참조하십시오.

- 보안 주체에 연결할 수 있는 IAM 정책의 생성에 대해 자세히 알아보려면 IAM 정책 만들기 (p. 435) 단원을 참조하십시오.
- 보안 주체에 IAM 정책을 연결하는 방법에 대해 자세히 알아보려면 IAM 자격 증명 권한 추가 및 제거 (p. 450) 단원을 참조하십시오.
- 관리형 정책 사용을 제한하는 예제 정책을 보려면 IAM: IAM 사용자, 그룹 또는 역할에 적용 가능한 관리형 정책을 제한 (p. 425) 단원을 참조하십시오.

고객 관리형 정책을 생성, 업데이트 및 삭제할 권한 제어

IAM 정책 (p. 349)을 사용하여 AWS 계정에서 고객 관리형 정책을 생성, 업데이트 및 삭제할 수 있는 대상을 제어할 수 있습니다. 다음 목록에는 정책 또는 정책 버전을 생성, 업데이트 및 삭제하는 것과 직접적으로 관련된 API 작업이 포함되어 있습니다.

- CreatePolicy
- CreatePolicyVersion
- DeletePolicy
- DeletePolicyVersion
- SetDefaultPolicyVersion

위 목록의 API 작업은 IAM 정책을 사용하여 허용하거나 거부할 수 있는 작업, 다시 말해 부여할 수 있는 권한에 해당합니다.

다음 예제 정책을 고려하십시오. 사용자가 AWS 계정에서 모든 고객 관리형 정책의 기본 버전을 생성, 업데이트(즉, 새 정책 버전 생성), 삭제 및 설정하도록 허용합니다. 또한 이 정책 예에서는 사용자가 정책을 나열

하고 가져오도록 허용합니다. 이 예제 JSON 정책 문서를 사용하여 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

Example 모든 정책의 기본 버전을 생성, 업데이트, 삭제, 나열, 가져오기 및 설정하도록 허용하는 정책

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "iam:CreatePolicy",
      "iam:CreatePolicyVersion",
      "iam:DeletePolicy",
      "iam:DeletePolicyVersion",
      "iam:GetPolicy",
      "iam:GetPolicyVersion",
      "iam:ListPolicies",
      "iam:ListPolicyVersions",
      "iam:SetDefaultPolicyVersion"
    ],
    "Resource": "*"
  }
}
```

이러한 API 작업의 사용을 제한하는 정책을 생성하여 지정하는 관리형 정책에만 영향을 줄 수 있습니다. 예를 들어, 특정 고객 관리형 정책의 경우에만 사용자가 기본 버전을 설정하고 정책 버전을 삭제하도록 허용해야 할 수 있습니다. 이렇게 하려면 이러한 권한을 부여하는 정책의 `Resource` 요소에 정책 ARN을 지정합니다.

다음 예제는 사용자가 정책 버전을 삭제하고 기본 버전을 설정할 수 있는 정책을 보여줍니다. 이런 작업은 /TEAM-A/ 경로를 포함하는 고객 관리형 정책에만 허용됩니다. 고객 관리형 정책 ARN은 그 정책의 `Resource` 요소에 지정되어 있습니다. (이 예에서 ARN에는 경로와 와일드카드가 포함되어 있으므로 경로 /TEAM-A/를 포함하는 모든 고객 관리형 정책과 일치합니다.) 이 예제 JSON 정책 문서를 사용하여 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

고객 관리형 정책 이름에서 경로를 사용하는 방법에 대한 자세한 정보는 표시 이름 및 경로 (p. 563) 단원을 참조하십시오.

Example 특정 정책의 경우에만 정책 버전 삭제와 기본 버전 설정을 허용하는 정책

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "iam:DeletePolicyVersion",
      "iam:SetDefaultPolicyVersion"
    ],
    "Resource": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:policy/TEAM-A/*"
  }
}
```

관리형 정책을 연결 및 분리하는 권한 제어

IAM 정책을 사용하여 사용자가 특정 관리형 정책만 사용하도록 허용할 수도 있습니다. 사실상 사용자가 다른 보안 주체에 부여할 수 있는 권한을 제어할 수 있습니다.

다음은 보안 주체 개체에 관리형 정책을 연결하고 분리하는 것과 직접적으로 관련된 API 작업 목록입니다.

- AttachGroupPolicy
- AttachRolePolicy
- AttachUserPolicy
- DetachGroupPolicy
- DetachRolePolicy
- DetachUserPolicy

이러한 API 작업의 사용을 제한하는 정책을 생성하여 지정하는 특정 관리형 정책 및/또는 보안 주체 개체에만 영향을 줄 수 있습니다. 예를 들어, 사용자가 지정하는 관리형 정책에만 연결하도록 허용해야 할 수 있습니다. 또는 사용자가 지정하는 보안 주체 엔터티에만 관리형 정책을 연결하도록 허용해야 할 수 있습니다.

다음 정책 예에서는 사용자가 경로 /TEAM-A/를 포함하는 그룹 및 역할에만 관리형 정책을 연결하도록 허용합니다. 그룹 및 역할 ARN은 정책의 `Resource` 요소에서 지정됩니다. (이 예에서 ARN에는 경로와 와일드카드 문자가 포함되어 있으므로 경로 /TEAM-A/를 포함하는 모든 그룹 및 역할과 일치합니다.) 이 예제 JSON 정책 문서를 사용하여 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

Example 특정 그룹 또는 역할에만 관리형 정책 연결을 허용하는 정책

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "iam:AttachGroupPolicy",
      "iam:AttachRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:group/TEAM-A/*",
      "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/TEAM-A/*"
    ]
  }
}
```

앞 예에서 지정하는 정책에만 영향을 주도록 작업의 사용을 제한할 수 있습니다. 정책에 조건을 추가함으로써 사실상 사용자가 다른 보안 주체에 연결할 수 있는 권한을 제어할 수 있습니다.

다음 예에서 조건은 연결된 정책이 지정된 정책 가운데 하나와 일치하는 경우에만 `AttachGroupPolicy` 및 `AttachRolePolicy` 권한이 허용되도록 합니다. 이 조건은 `iam:PolicyARN` 조건 키 (p. 598)를 사용하여 연결할 수 있는 정책을 결정합니다. 다음은 위의 예제를 확장한 예제 정책입니다. 사용자가 경로 /TEAM-A/ 경로를 포함하는 그룹 및 역할에만 /TEAM-A/ 경로를 포함하는 관리형 정책만 연결하도록 허용합니다. 이 예제 JSON 정책 문서를 사용하여 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "iam:AttachGroupPolicy",
      "iam:AttachRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:group/TEAM-A/*",
      "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/TEAM-A/*"
    ],
    "Condition": {"ArnLike":
      {"iam:PolicyARN": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:policy/TEAM-A/*"}
```

```
    }
  }
}
```

ARN에 와일드카드 문자가 있으므로 이 정책은 `ArnLike` 조건 연산자를 사용합니다. 특정 ARN의 경우 `ArnEquals` 조건 연산자를 사용합니다. `ArnLike` 및 `ArnEquals`에 대한 자세한 정보는 정책 요소 참조의 조건 유형 단원에서 Amazon 리소스 이름(ARN) 조건 연산자 (p. 606) 단원을 참조하십시오.

예를 들어, 지정하는 관리형 정책만 포함하도록 작업 사용을 제한할 수 있습니다. 이렇게 하려면 이러한 권한을 부여하는 정책의 `Condition` 요소에 정책 ARN을 지정합니다. 예를 들어, 고객 관리형 정책의 ARN을 지정하려면:

```
"Condition": {"ArnEquals":
  {"iam:PolicyARN": "arn:aws:iam::123456789012:policy/POLICY-NAME"}
}
```

AWS 관리형 정책의 `Condition` 요소에서도 정책의 ARN을 지정할 수 있습니다. AWS 관리형 정책의 ARN은 다음 예와 같이 정책 ARN에 계정 ID 대신 `aws`라는 특별한 별칭을 사용합니다.

```
"Condition": {"ArnEquals":
  {"iam:PolicyARN": "arn:aws:iam::aws:policy/AmazonEC2FullAccess"}
}
```

리소스에 대한 액세스 제어

자격 증명 기반 정책 또는 리소스 기반 정책을 사용하여 리소스에 대한 액세스를 제어할 수 있습니다. 자격 증명 기반 정책에서 자격 증명에 정책을 연결하고 자격 증명이 액세스할 수 있는 리소스를 지정합니다. 리소스 기반 정책에서 제어하려는 리소스에 정책을 연결합니다. 정책에서 해당 리소스에 액세스할 수 있는 보안 주체를 지정합니다. 두 정책 유형에 대한 자세한 정보는 자격 증명 기반 정책 및 리소스 기반 정책 (p. 372) 단원을 참조하십시오.

자세한 정보는 다음 리소스 단원을 참조하십시오.

- 보안 주체에 연결할 수 있는 IAM 정책의 생성에 대해 자세히 알아보려면 IAM 정책 만들기 (p. 435) 단원을 참조하십시오.
- 보안 주체에 IAM 정책을 연결하는 방법에 대해 자세히 알아보려면 IAM 자격 증명 권한 추가 및 제거 (p. 450) 단원을 참조하십시오.
- Amazon S3은 해당 버킷의 리소스 기반 정책 사용을 지원합니다. 자세한 정보는 버킷 정책 예제 단원을 참조하십시오.

리소스 생성자에게 권한이 자동으로 부여되지는 않음

AWS 계정 루트 사용자 자격 증명을 사용하여 로그인한 경우 해당 계정에 속한 리소스에서 모든 작업을 수행할 수 있는 권한이 부여됩니다. 그러나 IAM 사용자의 경우에는 그렇지 않습니다. IAM 사용자는 리소스를 생성할 권한을 받을 수 있지만, 그러한 리소스에 대한 권한은 명시적으로 부여받은 권한으로 제한됩니다. 즉, IAM 역할과 같은 리소스를 생성했다는 이유만으로 해당 역할을 편집 또는 삭제할 권한이 자동으로 부여되지는 않습니다. 또한 사용자의 권한은 계정 소유자 또는 해당 권한을 관리할 권한이 있는 다른 사용자가 언제든지 취소할 수 있습니다.

특정 계정에서 보안 주체에 대한 액세스 제어

계정의 IAM 사용자에게 리소스에 대한 액세스 권한을 직접 부여할 수 있습니다. 다른 계정의 사용자가 리소스에 액세스할 필요가 있다면 IAM 역할을 생성합니다. 역할은 권한을 포함한 개체이지만 특정 사용자와 관련이 없습니다. 다른 계정의 사용자는 해당 역할을 수임하여 해당 역할에 할당된 권한에 따라 리소스에 액세스할 수 있습니다. 자세한 정보는 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공 (p. 178) 단원을 참조하십시오.

Note

일부 서비스는 자격 증명 기반 정책 및 리소스 기반 정책 (p. 372)에 설명된 대로 리소스 기반 정책을 지원합니다(Amazon S3, Amazon SNS, Amazon SQS 등). 그런 서비스의 역할 사용 대안은 공유할 리소스(버킷, 주제 또는 대기열)에 정책을 연결하는 것입니다. 리소스 기반 정책은 리소스에 대한 액세스 허가를 받은 AWS 계정을 지정할 수 있습니다.

IAM 리소스 태그를 사용하여 IAM 사용자 및 역할에 대한 액세스 제어

다음 섹션의 정보를 사용하여 IAM 사용자 및 역할에 액세스할 수 있는 사람과 사용자 및 역할이 액세스할 수 있는 리소스를 제어합니다. 다른 AWS 리소스에 대한 액세스 제어를 위한 자세한 일반 정보 및 예는 리소스 태그를 사용하여 AWS 리소스에 대한 액세스 제어 (p. 384)를 참조하십시오.

태그는 IAM 리소스에 연결하거나 요청에 전달하거나 요청을 하는 보안 주체에 연결할 수 있습니다. IAM 사용자 또는 역할은 리소스 및 보안 주체 둘 다일 수 있습니다. 예를 들어 사용자가 사용자 그룹을 나열하도록 허용하는 정책을 작성할 수 있습니다. 이 작업은 요청을 하는 사용자(보안 주체)가 보려는 사용자와 동일한 `project=blue` 태그를 갖고 있는 경우에만 허용됩니다. 이 예에서 사용자는 동일한 프로젝트에서 작업하는 동안 자신을 비롯하여 모든 사용자에 대한 그룹 구성원 자격을 볼 수 있습니다.

태그를 기반으로 액세스를 제어하려면 정책의 조건 요소 (p. 598)에 태그 정보를 제공하십시오. IAM 정책을 생성할 때 IAM 태그 및 연관된 태그 조건 키를 사용하여 다음 중 하나에 대한 액세스를 제어할 수 있습니다.

- 리소스 (p. 382) – 태그를 기반으로 사용자 또는 역할 리소스에 대한 액세스를 제어합니다. 이를 위해 iam:ResourceTag/***key-name*** 조건 키를 사용하여 리소스에 연결해야 하는 태그 키-값 페어를 지정합니다. 비슷한 서비스별 키(예: `ec2:ResourceTag`)가 다른 AWS 리소스에서 사용됩니다. 자세한 내용은 AWS 리소스에 대한 액세스 제어 (p. 385) 단원을 참조하십시오.
- 요청 (p. 383) – 어떤 태그가 IAM 요청에 전달될 수 있는지 제어합니다. 이를 수행하려면 aws:RequestTag/***key-name*** 조건 키를 사용하여 어떤 태그를 IAM 사용자 또는 역할에서 추가, 변경 또는 제거할 수 있는지 지정합니다. 이 키는 IAM 리소스 및 기타 AWS 리소스에서 동일한 방식으로 사용됩니다. 자세한 내용은 AWS 요청 중 액세스 제어 (p. 386) 단원을 참조하십시오.
- 보안 주체 (p. 383) – 요청을 하는 사람(보안 주체)이 자신의 IAM 사용자 또는 역할에 연결된 태그를 기반으로 수행할 수 있는 권한을 제어합니다. 이를 위해 aws:PrincipalTag/***key-name*** 조건 키를 사용하여 요청이 허용되기 전에 IAM 사용자 또는 역할에 연결해야 하는 태그를 지정합니다.
- 권한 부여 프로세스의 일부 (p. 384) – aws:TagKeys 조건 키를 사용하여 특정 태그 키를 리소스, 요청 또는 보안 주체에서 사용할 수 있는지 여부를 제어합니다. 이 경우 키 값은 중요하지 않습니다. 이 키는 IAM 리소스 및 기타 AWS 리소스에서 비슷하게 작동합니다. 그러나 IAM에서 사용자를 태그 지정하면 보안 주체가 모든 서비스에 대한 요청을 할 수 있는지 여부도 제어할 수 있습니다. 자세한 내용은 태그 키를 기반으로 액세스 제어 (p. 386) 단원을 참조하십시오.

시각적 편집기를 사용하거나 JSON을 사용하거나 기존 관리형 정책을 가져와서 IAM 정책을 생성할 수 있습니다. 자세한 내용은 IAM 정책 만들기 (p. 435) 단원을 참조하십시오.

IAM 리소스에 대한 액세스 제어

IAM 정책에 태그를 사용하여 IAM 사용자 및 역할 리소스에 대한 액세스를 제어할 수 있습니다. 그러나 IAM은 그룹에 대한 태그를 지원하지 않으므로 태그를 사용하여 그룹에 대한 액세스를 제어할 수 없습니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.를 사용하면 `status=terminated` 태그를 통해 사용자를 삭제할 수 있습니다.이 정책을 사용하려면 정책 예제의 ***#### ## ### ###***를 본인의 정보로 대체하십시오.

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

```
    "Statement": [{
        "Effect": "Allow",
        "Action": "iam:DeleteUser",
        "Resource": "*",
        "Condition": {"StringLike": {"iam:ResourceTag/status": "terminated"}}
    }]
}
```

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 `jobFunction = employee` 태그가 지정된 모든 사용자에 대해 태그 편집을 허용합니다.이 정책을 사용하려면 정책 예제의 *#### ## ## # ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
                "iam:ListUserTags",
                "iam:TagUser",
                "iam:UntagUser"
            ],
        "Resource": "*",
        "Condition": {"StringLike": {"iam:ResourceTag/jobFunction": "employee"}}
    }]
}
```

IAM 요청 중 액세스 제어

IAM 정책에 태그를 사용하여 IAM 요청에서 전달할 수 있는 태그를 제어할 수 있습니다. IAM 사용자 또는 역할에서 추가, 변경 또는 제거할 수 있는 태그 키-값 페어를 지정할 수 있습니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 `department = HR` 또는 `department = CS` 태그만을 사용하는 사용자 태그 지정을 허용합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "iam:TagUser",
        "Resource": "*",
        "Condition": {"StringLike": {"aws:RequestTag/department": [
            "HR",
            "CS"
        ]}}
    }]
}
```

IAM 보안 주체에 대한 액세스 제어

IAM 태그를 사용하면 보안 주체가 자신의 자격 증명에 연결된 태그를 기반으로 수행할 수 있는 권한을 제어할 수 있습니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 보안 주체가 Amazon EC2 인스턴스를 시작하거나 중지하도록 허용합니다. 이 작업은 인스턴스의 리소스 태그와 보안 주체의 태그가 태그 키 `cost-center`와 동일한 값을 가질 경우에만 허용됩니다.이 정책을 사용하려면 정책 예제의 *#### ## # ## ###*를 본인의 정보로 대체하십시오.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/costcenter": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

태그 키를 기반으로 액세스 제어

IAM 정책에서 태그를 사용하여 리소스, 요청 또는 보안 주체에 특정 태그 키를 사용할 수 있는지 여부를 제어할 수 있습니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.를 사용하면 `temporary` 키가 있는 태그만 사용자로부터 제거할 수 있습니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "iam:UntagUser",
        "Resource": "*",
        "Condition": {"ForAllValues:StringEquals": {"aws:TagKeys": ["temporary"]}}
    }]
}
```

리소스 태그를 사용하여 AWS 리소스에 대한 액세스 제어

태그를 사용하여 태그 지정을 지원하는 AWS 리소스에 대한 액세스를 제어할 수 있습니다. IAM 사용자 및 역할을 태그 지정하여 액세스할 수 있는 권한을 제어할 수도 있습니다. IAM 사용자 및 역할을 태그 지정하는 방법을 알아보려면 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오. 보안 주체 태그가 있는 IAM 역할이 일치하는 태그가 있는 리소스에 액세스할 수 있도록 허용하는 정책을 만들고 테스트하는 자습서를 보려면 자습서: AWS에서 속성 기반 액세스 제어에 태그 사용 (p. 41) 단원을 참조하십시오. 다음 섹션의 정보를 사용하여 IAM 사용자 또는 역할을 태그 지정하지 않고 다른 AWS 서비스에 대한 액세스를 제어합니다.

태그를 사용하여 AWS 리소스에 대한 액세스를 제어하기 전에 AWS의 액세스 허용 방식을 이해해야 합니다. 또한 AWS는 리소스의 컬렉션으로 구성되어 있습니다. Amazon EC2 인스턴스도 리소스입니다. Amazon S3 버킷도 리소스입니다. AWS API, AWS CLI 또는 AWS Management 콘솔을 사용하여 작업(예: Amazon S3에서 버킷 생성)을 수행할 수 있습니다. 그렇게 하면 해당 작업에 대한 요청을 보냅니다. 이 요청은 작업, 리소스, 보안 주체 엔터티(사용자 또는 역할), 보안 주체 계정 및 필요한 요청 정보를 지정합니다. 이러한 모든 정보는 콘텍스트를 제공합니다.

그런 다음 AWS은 사용자(보안 주체 엔터티)가 지정된 리소스에 대해 지정된 작업을 수행할 수 있도록 인증(로그인) 및 권한 부여(권한 있음)되었는지 확인합니다. 권한을 부여하는 동안 AWS는 요청 콘텍스트에 적용되는 모든 정책을 확인합니다. 대부분의 정책은 AWS에 JSON 문서 (p. 354)로 저장되며 보안 주체 엔터티에 대한 권한을 지정합니다. 정책 유형 및 활용에 대한 자세한 내용은 정책 및 권한 (p. 349) 단원을 참조하십시오.

AWS는 정책이 요청의 각 부분을 허용한 경우에만 요청에 권한을 부여합니다. 다이어그램을 보고 IAM 인프라에 대해 자세히 알아보려면 IAM 작동 방식 이해 (p. 3) 단원을 참조하십시오. IAM가 요청이 허용되는지 여부를 결정하는 방법에 대한 자세한 내용은 정책 평가 로직 (p. 622) 단원을 참조하십시오.

태그로 인해 이 프로세스가 복잡해질 수 있는데, 리소스에 태그가 연결되거나 태그 지정을 지원하는 서비스에 대한 요청에 전달될 수 있기 때문입니다. 태그를 기반으로 액세스를 제어하려면 정책의 조건 요소 (p. 598)에 태그 정보를 제공하십시오. AWS 서비스에서 태그를 사용한 액세스 제어를 지원하는지 여부를 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하고, 태그 기반 권한 부여 열이 예인 서비스를 찾아보십시오. 서비스의 이름을 선택하여 해당 서비스에 대한 권한 부여 및 액세스 제어 문서를 봅니다.

그러면 리소스의 태그를 기반으로 리소스에 대한 액세스를 허용하거나 거부하는 IAM 정책을 생성할 수 있습니다. 해당 정책에서는 태그 조건 키를 사용하여 다음 중 하나에 대한 액세스를 제어할 수 있습니다.

- 리소스 (p. 385) – 리소스에 대한 태그를 기반으로 AWS 서비스 리소스에 대한 액세스를 제어합니다. 이를 수행하려면 ResourceTag/***key-name*** 조건 키를 사용하여 리소스에 연결된 태그를 기반으로 리소스에 대한 액세스를 허용할지 여부를 결정합니다.
- 요청 (p. 386) – 어떤 태그가 요청에 전달될 수 있는지 제어합니다. 이를 수행하려면 aws:RequestTag/***key-name*** 조건 키를 사용하여 AWS 리소스에 태그를 지정하거나 태그를 제거하는 요청에서 어떤 태그 키-값 페어를 전달할 수 있는지를 지정합니다.
- 권한 부여 프로세스의 일부 (p. 386) – aws:TagKeys 조건 키를 사용하여 특정 태그 키를 리소스 또는 요청에서 사용할 수 있는지 여부를 제어합니다.

JSON을 사용하거나 기존 관리형 정책을 가져와서 시각적으로 IAM 정책을 생성할 수 있습니다. 자세한 내용은 IAM 정책 만들기 (p. 435) 단원을 참조하십시오.

AWS 리소스에 대한 액세스 제어

IAM 정책의 조건을 사용하여 해당 리소스의 태그를 기반으로 AWS 리소스에 대한 액세스를 제어할 수 있습니다. 전역 `aws:ResourceTag/`*`tag-key`* 조건 키 또는 `iam:RequestTag/`*`tag-key`* 같은 서비스별 키를 사용하여 이 작업을 수행할 수 있습니다. IAM와 같은 일부 서비스는 이 키의 서비스별 버전만 지원하며 전역 버전은 지원하지 않습니다.

> **Note**
>
> `iam:PassRole` 작업을 포함하는 정책에는 `ResourceTag` 조건 키를 사용하지 마십시오. IAM 역할에서는 태그를 사용하여 누가 해당 역할을 전달할 수 있는지 액세스 권한을 제어할 수 없습니다. 서비스로 역할을 전달하는 데 필요한 권한에 대한 자세한 내용은 사용자에게 AWS 서비스에 역할을 전달할 권한 부여 (p. 254) 단원을 참조하십시오.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 Amazon EC2 인스턴스를 시작 또는 중지할 수 있도록 허용합니다. 이러한 작업은 인스턴스 태그 `Owner`가 사용자의 사용자 이름의 값과 같은 경우에만 허용됩니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringEquals": {"ec2:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
```

```
        }
    ]
}
```

이 정책을 계정의 IAM 사용자에게 연결할 수 있습니다. 이름이 `richard-roe`인 사용자가 Amazon EC2 인스턴스를 시작하려 하는 경우 인스턴스에 `Owner=richard-roe` 또는 `owner=richard-roe` 태그가 지정되어야 합니다. 그렇지 않은 경우 액세스가 거부됩니다. 태그 키 `Owner`는 `Owner` 및 `owner` 모두와 일치하는데, 조건 키가 대/소문자를 구분하지 않기 때문입니다. 자세한 내용은 IAM JSON 정책 요소: Condition (p. 598) 단원을 참조하십시오.

AWS 요청 중 액세스 제어

IAM 정책의 조건을 사용하여 AWS 리소스에 태그를 지정하는 요청에서 어떤 태그 키-값 페어를 전달할 수 있는지를 제어할 수 있습니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 Amazon EC2 `CreateTags` 작업을 사용하여 태그를 인스턴스에 연결할 수 있습니다. 태그에 `environment` 키 및 `preprod` 또는 `production` 값이 포함된 경우에만 태그를 연결할 수 있습니다. 원하는 경우 `ForAllValues` 변경자를 `aws:TagKeys` 조건 키와 함께 사용하여 요청에서 키 `environment`만 허용됨을 표시할 수 있습니다. 이를 통해 사용자가 `environment` 대신 `Environment`를 실수로 사용하는 것과 같이 다른 키를 포함시키는 것을 방지합니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "ec2:CreateTags",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

태그 키를 기반으로 액세스 제어

IAM 정책에서 조건을 사용하여 리소스 또는 요청에 특정 태그 키를 사용할 수 있는지 여부를 제어할 수 있습니다.

모범 사례로서 정책을 사용하여 태그를 사용한 액세스를 제어할 때 `aws:TagKeys` 조건 키 (p. 662)를 사용해야 합니다. 태그를 지원하는 AWS 서비스를 통해 대소문자만 다른 여러 키 이름을 생성할 수 있습니다(예: Amazon EC2 인스턴스에 `foo=bar1` 및 `Foo=bar2` 태그 지정). 정책 조건에서 키 이름은 대/소문자를 구분하지 않습니다. 따라서 정책의 조건 요소에서 `"ec2:ResourceTag:TagKey1": "Value1"` 지정을 완료한 경우 조건은 이름이 `TagKey1` 또는 `tagkey1`안 리소스 태그 키와 일치하지만 두 가지 모두와 일치하지는 않습니다. 대소문자만 다른 키를 포함한 중복 태그를 방지하려면 `aws:TagKeys` 조건을 사용하여 사용자가 적용할 수 있는 태그 키를 정의합니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.를 통해 Secrets Manager 비밀 생성 및 태그 지정이 가능하지만 태그 키 `environment` 또는 `cost-center`를 포함해야만 합니다.

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

```
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "secretsmanager:CreateSecret",
            "secretsmanager:TagResource"
        ],
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "environment",
                    "cost-center"
                ]
            }
        }
    }
}
```

IAM 자격 증명 기반 정책 예제

정책 (p. 349)은 자격 증명이나 리소스와 연결될 때 해당 권한을 정의하는 AWS의 객체입니다. AWS는 IAM 보안 주체(사용자 또는 역할)가 요청을 보낼 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지 여부를 결정합니다. 대부분의 정책은 IAM 자격 증명(사용자, 사용자 그룹 또는 역할)에 연결되는 JSON 문서로서 AWS에 저장됩니다. 자격 증명 기반 정책에는 AWS 관리형 정책, 고객 관리형 정책 및 인라인 정책이 포함됩니다. 이러한 예제 JSON 정책 문서를 사용하여 IAM 정책을 생성하는 방법에 대해 자세히 알아보려면 the section called “JSON 탭에서 정책 만들기” (p. 436) 단원을 참조하십시오.

기본적으로 모든 요청이 거부되기 때문에 ID가 액세스하려는 서비스, 작업 및 리소스에 대한 액세스 권한을 제공해야 합니다. 또한 IAM 콘솔에서 지정된 작업을 완료하기 위해 액세스를 허용하려면 추가 권한을 제공해야 합니다.

다음의 정책 라이브러리가 IAM ID에 대한 권한을 정의하는 데 도움이 될 수 있습니다. 필요로 하는 정책을 찾은 다음에 View this policy(이 정책 보기)를 선택하여 해당 정책의 JSON을 확인합니다. JSON 정책 문서를 자체 정책의 템플릿으로 활용할 수 있습니다.

> Note
>
> 이 참조 설명에 포함시킬 정책을 제출하고자 하는 경우 이 페이지의 하단에 있는 의견 버튼을 사용합니다.

정책 예제: AWS

- 특정 날짜 범위 동안 액세스를 허용합니다. (이 정책 보기 (p. 390).)
- AWS 리전 활성화 및 비활성화를 허용합니다. (이 정책 보기 (p. 390).)
- MFA 인증 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (이 정책 보기 (p. 391).)
- 특정 날짜 범위 동안 MFA를 사용하는 경우 특정 액세스를 허용합니다. (이 정책 보기 (p. 394).)
- 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (이 정책 보기 (p. 394).)
- 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 MFA 디바이스를 관리할 수 있도록 허용합니다. (이 정책 보기 (p. 396).)
- 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 암호를 관리할 수 있도록 허용합니다. (이 정책 보기 (p. 398).)
- 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 암호, 액세스 키 및 SSH 퍼블릭 키를 관리할 수 있도록 허용합니다. (이 정책 보기 (p. 399).)

- 요청된 리전에 따라 AWS에 대한 액세스를 거부합니다. (이 정책 보기 (p. 400).)
- 소스 IP 주소를 기반으로 AWS에 대한 액세스를 거부합니다. (이 정책 보기 (p. 401).)

정책 예제: AWS Data Pipeline

- 사용자가 생성하지 않은 파이프라인에 대한 액세스를 거부합니다. (이 정책 보기 (p. 402).)

정책 예제: Amazon DynamoDB

- 특정 Amazon DynamoDB 테이블에 대한 액세스를 허용합니다. (이 정책 보기 (p. 403).)
- 특정 Amazon DynamoDB 열에 대한 액세스를 허용합니다. (이 정책 보기 (p. 404).)
- Amazon Cognito ID를 기준으로 Amazon DynamoDB에 대한 행 수준 액세스를 허용합니다. (이 정책 보기 (p. 404).)

정책 예제: Amazon EC2

- Amazon EC2 인스턴스가 볼륨을 연결 또는 분리하도록 허용합니다. (이 정책 보기 (p. 405).)
- 태그를 기준으로 Amazon EBS 볼륨을 Amazon EC2 인스턴스에 연결 또는 분리하도록 허용합니다. (이 정책 보기 (p. 405).)
- 특정 서브넷에 있는 Amazon EC2 인스턴스를 프로그래밍 방식 및 콘솔에서 시작할 수 있도록 허용합니다. (이 정책 보기 (p. 406).)
- 특정 VPC와 관련된 Amazon EC2 보안 그룹을 프로그래밍 방식 및 콘솔에서 관리할 수 있도록 허용합니다. (이 정책 보기 (p. 407).)
- 사용자가 태그를 지정한 Amazon EC2 인스턴스를 프로그래밍 방식 및 콘솔에서 시작 또는 중지할 수 있도록 허용합니다. (이 정책 보기 (p. 407).)
- 리소스 및 보안 주체 태그 기반의 Amazon EC2 인스턴스를 프로그래밍 방식 및 콘솔에서 시작 또는 중지할 수 있도록 허용합니다. (이 정책 보기 (p. 408).)
- 리소스 및 주요 태그가 일치할 때 Amazon EC2 인스턴스를 시작 또는 중지할 수 있도록 허용합니다. (이 정책 보기 (p. 408).)
- 프로그래밍 방식 및 콘솔에서 특정 리전 내의 전체 Amazon EC2 액세스를 허용합니다. (이 정책 보기 (p. 409).)
- 프로그래밍 방식 및 콘솔에서 특정 Amazon EC2 인스턴스를 시작 또는 중지하고 특정 보안 그룹을 수정할 수 있도록 허용합니다. (이 정책 보기 (p. 409).)
- MFA 없이 특정 Amazon EC2 작업에 대한 액세스를 거부합니다. (이 정책 보기 (p. 410).)
- Amazon EC2 인스턴스 종료를 특정 IP 주소 범위로 제한합니다. (이 정책 보기 (p. 411).)

정책 예제: AWS Identity and Access Management(IAM)

- 정책 시뮬레이터 API에 대한 액세스를 허용합니다. (이 정책 보기 (p. 411).)
- 정책 시뮬레이터 콘솔에 대한 액세스를 허용합니다. (이 정책 보기 (p. 412).)
- 프로그래밍 방식 및 콘솔에서 특정 태그를 갖는 규칙을 수임하도록 허용합니다. (이 정책 보기 (p. 413).)
- 프로그래밍 방식 및 콘솔에서 여러 서비스에 대한 액세스를 허용 및 거부합니다. (이 정책 보기 (p. 413).)
- 프로그래밍 방식 및 콘솔에서 특정 태그가 있는 IAM 사용자에게 또 다른 특정 태그를 추가할 수 있도록 허용합니다. (이 정책 보기 (p. 414).)
- 프로그래밍 방식 및 콘솔에서 IAM 사용자 또는 역할에게 특정 태그를 추가할 수 있도록 허용합니다. (이 정책 보기 (p. 415).)

- 특정 태그가 있는 새 사용자만 만들 수 있도록 허용합니다. (이 정책 보기 (p. 416).)
- IAM 자격 증명 보고서 생성 및 검색을 허용합니다. (이 정책 보기 (p. 417).)
- 프로그래밍 방식 및 콘솔에서 그룹의 멤버십을 관리하도록 허용합니다. (이 정책 보기 (p. 417).)
- 특정 태그를 관리하도록 허용합니다. (이 정책 보기 (p. 418).)
- IAM 역할을 특정 서비스로 전달하도록 허용합니다. (이 정책 보기 (p. 419).)
- 보고 없이 IAM 콘솔에 대한 읽기 전용 액세스를 허용합니다. (이 정책 보기 (p. 419).)
- IAM 콘솔에 대한 읽기 전용 액세스를 허용합니다. (이 정책 보기 (p. 420).)
- 특정 사용자가 프로그래밍 방식 및 콘솔에서 그룹을 관리하도록 허용합니다. (이 정책 보기 (p. 420).)
- 프로그래밍 방식 및 콘솔에서 계정 암호 요구 사항을 설정하도록 허용합니다. (이 정책 보기 (p. 421).)
- 특정 경로를 지닌 사용자에 대해 정책 시뮬레이터 API의 사용을 허용합니다. (이 정책 보기 (p. 422).)
- 특정 경로를 지닌 사용자에 대해 정책 시뮬레이터 콘솔의 사용을 허용합니다. (이 정책 보기 (p. 422).)
- IAM 사용자가 MFA 디바이스를 자체적으로 관리할 수 있도록 허용합니다. (이 정책 보기 (p. 423).)
- 프로그래밍 방식으로 및 콘솔에서 IAM 사용자가 자신의 자격 증명을 교체할 수 있도록 허용합니다. (이 정책 보기 (p. 424).)
- IAM 콘솔에서 AWS Organizations 정책에 대해 서비스에서 마지막으로 액세스한 데이터를 보도록 허용합니다. (이 정책 보기 (p. 425).)
- IAM 사용자, 그룹 또는 역할에 적용할 수 있는 관리형 정책을 제한합니다(이 정책 보기 (p. 425)).

정책 예제: AWS Lambda

- AWS Lambda 함수가 Amazon DynamoDB 테이블에 액세스하도록 허용합니다. (이 정책 보기 (p. 426).)

정책 예제: Amazon RDS

- 특정 리전 내에서 모든 Amazon RDS 데이터베이스 액세스를 허용합니다. (이 정책 보기 (p. 427).)
- 프로그래밍 방식 및 콘솔에서 Amazon RDS 데이터베이스를 복원하도록 허용합니다. (이 정책 보기 (p. 427).)
- 태그 소유자가 자신이 태그를 지정한 Amazon RDS 리소스에 대한 모든 액세스 권한을 가지도록 허용합니다. (이 정책 보기 (p. 428).)

정책 예제: Amazon S3

- Amazon Cognito 사용자가 자신의 Amazon S3 버킷에 있는 객체에 액세스하도록 허용합니다. (이 정책 보기 (p. 429).)
- 연합된 사용자가 프로그래밍 방식 및 콘솔에서 Amazon S3에 있는 자신의 홈 디렉터리에 액세스하도록 허용합니다. (이 정책 보기 (p. 430).)
- 전체 S3 액세스를 허용하지만 관리자가 직전 30분 이내에 MFA를 사용하여 로그인하지 않은 경우 프로덕션 버킷에 대한 액세스를 명시적으로 거부합니다. (이 정책 보기 (p. 431).)
- IAM 사용자가 프로그래밍 방식 및 콘솔에서 Amazon S3에 있는 자신의 홈 디렉터리에 액세스하도록 허용합니다. (이 정책 보기 (p. 432).)
- 사용자가 하나의 Amazon S3 버킷을 관리하고 다른 모든 AWS 작업 및 리소스를 거부하도록 허용합니다. (이 정책 보기 (p. 433).)
- 특정 Amazon S3 버킷에 대한 `Read` 및 `Write` 액세스를 허용합니다. (이 정책 보기 (p. 433).)
- 프로그래밍 방식 및 콘솔에서 특정 Amazon S3 버킷에 대한 `Read` 및 `Write` 액세스를 허용합니다. (이 정책 보기 (p. 434).)

AWS: 특정 기간 동안 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.는 SERVICE-NAME라는 서비스의 ACTION-NAME 작업에 대한 액세스를 허용합니다. 액세스는 2017년 7월 1일과 2017년 12월 31일(UTC) 사이에 발생하는 작업으로 제한됩니다. 이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

IAM 정책의 Condition 블록 내에서 복수 조건을 사용하는 방법에 관한 자세한 내용은 다수의 조건 값 (p. 601) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "service-prefix:action-name",
        "Resource": "*",
        "Condition": {
            "DateGreaterThan": {"aws:CurrentTime": "2017-07-01T00:00:00Z"},
            "DateLessThan": {"aws:CurrentTime": "2017-12-31T23:59:59Z"}
        }
    }
}
```

AWS: AWS 리전 활성화 및 비활성화 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 관리자가 아시아 태평양(홍콩) 리전(ap-east-1)을 활성화 및 비활성화할 수 있도록 허용합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다. 이 설정은 AWS Management 콘솔의 계정 설정 페이지에 표시됩니다. 이 페이지에는 계정 관리자만이 보고 관리해야 하는 민감한 계정 수준 정보가 포함되어 있습니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

> **Important**
>
> 기본적으로 활성화되는 리전은 활성화하거나 비활성화할 수 없습니다. 기본적으로 비활성화되는 리전만 추가할 수 있습니다. 자세한 내용은 AWS General Reference에서 AWS 리전 관리 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableDisableHongKong",
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {"account:TargetRegion": "ap-east-1"}
            }
        },
        {
            "Sid": "ViewConsole",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewAccount",
                "account:ListRegions"
            ],
```

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

AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 Multi-Factor Authentication(MFA) (p. 119)을 사용하여 인증된 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. 이 AWS Management 콘솔 페이지에는 계정 ID 및 정식 사용자 ID와 같은 계정 정보가 표시됩니다. 또한 사용자는 자신의 암호, 액세스 키, MFA 디바이스, X.509 인증서, SSH 키 및 Git 자격 증명을 보고 편집할 수 있습니다. 이 예제 정책에는 페이지에 있는 모든 정보를 보고 편집하는 데 필요한 권한이 포함되어 있습니다. 또한 사용자가 AWS에서 다른 작업을 수행하기 전에 MFA 사용을 설정하고 인증해야 합니다. 사용자가 MFA를 사용하지 않고 자신의 자격 증명을 관리하도록 허용하려면 AWS: IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 394) 단원을 참조하십시오.

사용자가 My Security Credentials(내 보안 자격 증명) 페이지에 액세스할 수 있는 방법을 알아보려면 IAM 사용자가 자신의 암호를 변경하는 방법(콘솔) (p. 110) 단원을 참조하십시오.

> **Note**
>
> 이 정책 예제에서는 사용자가 로그인과 암호 재설정을 한 번에 할 수 없습니다. 새 사용자와 암호가 만료된 사용자는 이 작업을 시도할 수 있습니다. `iam:ChangePassword` 및 `iam:GetAccountPasswordPolicy`을 `DenyAllExceptListedIfNoMFA` 문에 추가하여 이를 허용할 수 있습니다. 그러나 IAM에서 이 방식은 권장하지 않습니다. 사용자가 MFA 없이 암호를 변경하도록 허용하면 보안 위험이 발생할 수 있습니다.

이 정책이 하는 일은 무엇입니까?

- `AllowViewAccountInfo` 문은 사용자가 계정 수준 정보를 볼 수 있도록 허용합니다. 이러한 권한은 리소스 ARN을 지원하지 않거나 리소스 ARN을 지정하는 데 필요하지 않기 때문에 자신의 문에 포함되어 있어야 합니다. 권한 대신 `"Resource" : "*"`를 지정합니다. 이 문에는 사용자가 특정 정보를 볼 수 있도록 허용하는 다음 작업이 포함되어 있습니다.
  - `GetAccountSummary` – 계정 ID 및 계정 정식 사용자 ID를 봅니다.
  - `GetAccountPasswordPolicy` – 자신의 IAM 사용자 암호를 변경하는 동안 계정 암호 요구 사항을 봅니다.
  - `ListVirtualMFADevices` – 사용자에 대해 활성화된 가상 MFA 디바이스에 대한 세부 정보를 봅니다.
- `AllowManageOwnPasswords` 문은 사용자가 자신의 암호를 변경할 수 있도록 허용합니다. 또한 이 문에는 My Security Credentials(내 보안 자격 증명) 페이지에 있는 대부분의 정보를 보는 데 필요한 `GetUser` 작업도 포함되어 있습니다.
- `AllowManageOwnAccessKeys` 문은 사용자가 자신의 액세스 키를 생성, 업데이트 및 삭제할 수 있도록 허용합니다.
- `AllowManageOwnSigningCertificates` 문은 사용자가 자신의 서명 인증서를 업로드, 업데이트 및 삭제할 수 있도록 허용합니다.
- `AllowManageOwnSSHPublicKeys` 문은 사용자가 CodeCommit에 대한 자신의 SSH 퍼블릭 키를 업로드, 업데이트 및 삭제할 수 있도록 허용합니다.
- `AllowManageOwnGitCredentials` 문은 사용자가 CodeCommit에 대한 자신의 Git 자격 증명을 생성, 업데이트 및 삭제할 수 있도록 허용합니다.
- `AllowManageOwnVirtualMFADevice` 문은 사용자가 에 대한 자신의 가상 MFA 디바이스를 생성하고 삭제할 수 있도록 허용합니다. 이 문의 리소스 ARN은 현재 로그인한 사용자와 동일한 이름의 MFA 디바이

스에만 액세스를 허용합니다. 사용자는 자신의 것이 아닌 다른 가상 MFA 디바이스를 생성하거나 삭제할 수 없습니다.

- `AllowManageOwnUserMFA` 문은 사용자가 자신의 사용자에 대해 가상, U2F 또는 하드웨어 MFA 디바이스를 보거나 관리할 수 있도록 허용합니다. 이 문의 리소스 ARN은 사용자 자신의 IAM 사용자에 대한 액세스만 허용합니다. 사용자는 다른 사용자의 MFA 디바이스를 보거나 관리할 수 없습니다.
- `DenyAllExceptListedIfNoMFA` 문은 사용자가 MFA를 사용하여 로그인하지 않은 경우에만 몇 가지 나열된 작업을 제외한 모든 AWS의 모든 작업에 대한 액세스를 거부합니다. 이 문은 `"Deny"` 및 `"NotAction"`의 조합을 사용하여 나열되지 않은 모든 작업에 대한 액세스를 명시적으로 거부합니다. 나열된 항목은 이 문에 따라 거부되거나 허용되지 않습니다. 하지만 정책의 다른 문에서 작업이 허용됩니다. 이 문의 로직에 대한 자세한 내용은 NotAction 및 Deny (p. 595) 단원을 참조하십시오. 사용자가 MFA를 사용하여 로그인한 경우 `Condition` 테스트가 실패하며 이 문은 어떠한 작업도 거부하지 않습니다. 이 경우 사용자에 대한 다른 정책 또는 문에 따라 사용자의 권한이 결정됩니다.

  이 문을 사용하면 MFA를 사용하여 로그인하지 않은 사용자는 나열된 작업만 수행할 수 있습니다. 또한 사용자는 다른 문 또는 정책이 해당 작업에 대한 액세스를 허용하는 경우에만 나열된 작업을 수행할 수 있습니다. MFA 권한 부여가 없으면 `iam:ChangePassword` 작업이 허용되지 않기 때문에 사용자는 로그인 시 암호를 생성할 수 없습니다.

  `...IfExists` 키를 분실했을 경우 `Bool` 연산자의 `aws:MultiFactorAuthPresent` 버전은 조건이 true로 반환됩니다. 즉, 액세스 키와 같은 장기 자격 증명으로 API를 액세스하는 사용자는 비 IAM API 작업에 대한 액세스가 거부됩니다.

이 정책은 사용자가 IAM 콘솔에서 Users(사용자) 페이지를 보거나 이 페이지를 사용하여 자신의 사용자 정보에 액세스할 수 있도록 허용합니다. 이 작업을 허용하려면 `iam:ListUsers` 작업을 `AllowViewAccountInfo` 문과 `DenyAllExceptListedIfNoMFA` 문에 추가합니다. 또한 이 문은 사용자가 자신의 사용자 페이지에서 암호를 변경하도록 허용하지 않습니다. 이 작업을 허용하려면 `iam:CreateLoginProfile`, `iam:DeleteLoginProfile`, `iam:GetLoginProfile` 및 `iam:UpdateLoginProfile` 작업을 `AllowManageOwnPasswords` 문에 추가합니다. 또한 사용자가 MFA를 사용하여 로그인하지 않고 자신의 사용자 페이지에서 자신의 암호를 변경할 수 있도록 허용하려면 `iam:CreateLoginProfile` 작업을 `DenyAllExceptListedIfNoMFA` 문에 추가합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowViewAccountInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:ListVirtualMFADevices"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowManageOwnPasswords",
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:GetUser"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:CreateAccessKey",
                "iam:DeleteAccessKey",
                "iam:ListAccessKeys",
```

```
            "iam:UpdateAccessKey"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnSigningCertificates",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteSigningCertificate",
            "iam:ListSigningCertificates",
            "iam:UpdateSigningCertificate",
            "iam:UploadSigningCertificate"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnSSHPublicKeys",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteSSHPublicKey",
            "iam:GetSSHPublicKey",
            "iam:ListSSHPublicKeys",
            "iam:UpdateSSHPublicKey",
            "iam:UploadSSHPublicKey"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnGitCredentials",
        "Effect": "Allow",
        "Action": [
            "iam:CreateServiceSpecificCredential",
            "iam:DeleteServiceSpecificCredential",
            "iam:ListServiceSpecificCredentials",
            "iam:ResetServiceSpecificCredential",
            "iam:UpdateServiceSpecificCredential"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnVirtualMFADevice",
        "Effect": "Allow",
        "Action": [
            "iam:CreateVirtualMFADevice",
            "iam:DeleteVirtualMFADevice"
        ],
        "Resource": "arn:aws:iam::*:mfa/${aws:username}"
    },
    {
        "Sid": "AllowManageOwnUserMFA",
        "Effect": "Allow",
        "Action": [
            "iam:DeactivateMFADevice",
            "iam:EnableMFADevice",
            "iam:ListMFADevices",
            "iam:ResyncMFADevice"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
        "Sid": "DenyAllExceptListedIfNoMFA",
        "Effect": "Deny",
        "NotAction": [
            "iam:CreateVirtualMFADevice",
            "iam:EnableMFADevice",
            "iam:GetUser",
```

```
                "iam:ListMFADevices",
                "iam:ListVirtualMFADevices",
                "iam:ResyncMFADevice",
                "sts:GetSessionToken"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

AWS: 지정 기간 동안 MFA를 사용한 특정 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 논리 AND를 사용하여 평가되는 여러 조건을 사용합니다. SERVICE-NAME-1으로 명명된 서비스에 대해 모든 액세스를 허용하고 ACTION-NAME-A로 명명된 서비스에서 ACTION-NAME-B 및 SERVICE-NAME-2 작업에 대한 액세스를 허용합니다. 이들 작업은 사용자가 멀티 팩터 인증(MFA)을 통해 인증된 경우에만 허용됩니다. 액세스는 2017년 7월 1일과 2017년 12월 31일(UTC) 사이에 발생하는 작업으로 제한됩니다. 이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ### ### ### ###*를 본인의 정보로 대체하십시오.

IAM 정책의 Condition 블록 내에서 복수 조건을 사용하는 방법에 관한 자세한 내용은 다수의 조건 값 (p. 601) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "service-prefix-1:*",
            "service-prefix-2:action-name-a",
            "service-prefix-2:action-name-b"
        ],
        "Resource": "*",
        "Condition": {
            "Bool": {"aws:MultiFactorAuthPresent": true},
            "DateGreaterThan": {"aws:CurrentTime": "2017-07-01T00:00:00Z"},
            "DateLessThan": {"aws:CurrentTime": "2017-12-31T23:59:59Z"}
        }
    }
}
```

AWS: IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.는 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 모든 자격 증명을 관리할 수 있도록 허용합니다. 이 AWS Management 콘솔 페이지에는 계정 ID 및 정식 사용자 ID와 같은 계정 정보가 표시됩니다. 또한 사용자는 자신의 암호, 액세스 키, X.509 인증서, SSH 키, Git 자격 증명을 보고 편집할 수 있습니다. 이 예제 정책에는 사용자의 MFA 디바이스를 제외하고 페이지에 있는 모든 정보를 보고 편집하는 데 필요한 권한이 포함되어 있습니다. 사용자가 MFA를 사용하여 자신의 자격 증명을 관리하도록 허용하려면 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391) 단원을 참조하십시오.

사용자가 My Security Credentials(내 보안 자격 증명) 페이지에 액세스할 수 있는 방법을 알아보려면 IAM 사용자가 자신의 암호를 변경하는 방법(콘솔) (p. 110) 단원을 참조하십시오.

이 정책이 하는 일은 무엇입니까?

- `AllowViewAccountInfo` 문은 사용자가 계정 수준 정보를 볼 수 있도록 허용합니다. 이러한 권한은 리소스 ARN을 지원하지 않거나 리소스 ARN을 지정하는 데 필요하지 않기 때문에 자신의 문에 포함되어 있어야 합니다. 권한 대신 `"Resource" : "*"`를 지정합니다. 이 문에는 사용자가 특정 정보를 볼 수 있도록 허용하는 다음 작업이 포함되어 있습니다.
  - `GetAccountPasswordPolicy` – 자신의 IAM 사용자 암호를 변경하는 동안 계정 암호 요구 사항을 봅니다.
  - `GetAccountSummary` – 계정 ID 및 계정 정식 사용자 ID를 봅니다.
- `AllowManageOwnPasswords` 문은 사용자가 자신의 암호를 변경할 수 있도록 허용합니다. 또한 이 문에는 My Security Credentials(내 보안 자격 증명) 페이지에 있는 대부분의 정보를 보는 데 필요한 `GetUser` 작업도 포함되어 있습니다.
- `AllowManageOwnAccessKeys` 문은 사용자가 자신의 액세스 키를 생성, 업데이트 및 삭제할 수 있도록 허용합니다.
- `AllowManageOwnSigningCertificates` 문은 사용자가 자신의 서명 인증서를 업로드, 업데이트 및 삭제할 수 있도록 허용합니다.
- `AllowManageOwnSSHPublicKeys` 문은 사용자가 CodeCommit에 대한 자신의 SSH 퍼블릭 키를 업로드, 업데이트 및 삭제할 수 있도록 허용합니다.
- `AllowManageOwnGitCredentials` 문을 사용하면 사용자가 CodeCommit에 대한 자신의 Git 자격 증명을 생성, 업데이트 및 삭제할 수 있습니다.

이 정책은 사용자가 자신의 MFA 디바이스를 보거나 관리하도록 허용하지 않습니다. 또한 사용자는 IAM 콘솔에서 Users(사용자) 페이지를 보거나 이 페이지를 사용하여 자신의 사용자 정보에 액세스할 수 없습니다. 이 작업을 허용하려면 `iam:ListUsers` 작업을 `AllowViewAccountInfo` 문에 추가합니다. 또한 이 문은 사용자가 자신의 사용자 페이지에서 암호를 변경하도록 허용하지 않습니다. 이 작업을 허용하려면 `iam:CreateLoginProfile`, `iam:DeleteLoginProfile`, `iam:GetLoginProfile` 및 `iam:UpdateLoginProfile` 작업을 `AllowManageOwnPasswords` 문에 추가합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowViewAccountInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowManageOwnPasswords",
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:GetUser"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:CreateAccessKey",
                "iam:DeleteAccessKey",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey"
            ],
```

```
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnSigningCertificates",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteSigningCertificate",
                "iam:ListSigningCertificates",
                "iam:UpdateSigningCertificate",
                "iam:UploadSigningCertificate"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnSSHPublicKeys",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteSSHPublicKey",
                "iam:GetSSHPublicKey",
                "iam:ListSSHPublicKeys",
                "iam:UpdateSSHPublicKey",
                "iam:UploadSSHPublicKey"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnGitCredentials",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceSpecificCredential",
                "iam:DeleteServiceSpecificCredential",
                "iam:ListServiceSpecificCredentials",
                "iam:ResetServiceSpecificCredential",
                "iam:UpdateServiceSpecificCredential"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        }
    ]
}
```

AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 MFA 디바이스를 관리할 수 있도록 허용합니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 Multi-Factor Authentication(MFA) (p. 119)을 통해 인증된 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 MFA 디바이스를 관리할 수 있도록 허용합니다. 이 AWS Management 콘솔 페이지에는 계정 및 사용자 정보가 표시되지만, 사용자는 자신의 MFA 디바이스만 보고 편집할 수 있습니다. 사용자가 MFA를 사용하여 자신의 모든 자격 증명을 관리하도록 허용하려면 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391) 단원을 참조하십시오.

Note

이 정책을 가진 IAM 사용자가 MFA 인증을 받지 않은 경우 이 정책은 MFA를 사용하여 인증하는 데 필요한 AWS 작업을 제외한 모든 해당 작업에 대한 액세스를 거부합니다. AWS CLI 및 AWS API를 사용하려면 IAM 사용자가 먼저 AWS STS GetSessionToken 작업을 사용하여 MFA 토큰을 검색한 다음 해당 토큰을 사용하여 원하는 작업을 인증해야 합니다. 리소스 기반 정책이나 기타 자격 증명 기반 정책 등의 기타 정책은 다른 서비스의 작업을 허용할 수 있습니다. 이 정책은 IAM 사용자가 MFA 인증되지 않은 경우 해당 액세스를 거부합니다.

사용자가 My Security Credentials(내 보안 자격 증명) 페이지에 액세스할 수 있는 방법을 알아보려면 IAM 사용자가 자신의 암호를 변경하는 방법(콘솔) (p. 110) 단원을 참조하십시오.

이 정책이 하는 일은 무엇입니까?

- `AllowViewAccountInfo` 문은 사용자가 사용자에 대해 활성화된 가상 MFA 디바이스에 대한 세부 정보를 볼 수 있도록 허용합니다. 이 권한은 리소스 ARN 지정을 지원하지 않으므로 자신의 문에 들어 있어야 합니다. 그 대신 `"Resource" : "*"`를 지정해야 합니다.
- `AllowManageOwnVirtualMFADevice` 문은 사용자가 에 대한 자신의 가상 MFA 디바이스를 생성하고 삭제할 수 있도록 허용합니다. 이 문의 리소스 ARN은 현재 로그인한 사용자와 동일한 이름의 MFA 디바이스에만 액세스를 허용합니다. 사용자는 자신의 것이 아닌 다른 가상 MFA 디바이스를 생성하거나 삭제할 수 없습니다.
- `AllowManageOwnUserMFA` 문은 사용자가 자신의 가상, U2F 또는 하드웨어 MFA 디바이스를 보거나 관리할 수 있도록 허용합니다. 이 문의 리소스 ARN은 사용자 자신의 IAM 사용자에 대한 액세스만 허용합니다. 사용자는 다른 사용자의 MFA 디바이스를 보거나 관리할 수 없습니다.
- `DenyAllExceptListedIfNoMFA` 문은 사용자가 MFA를 사용하여 로그인하지 않은 경우에만 몇 가지 나열된 작업을 제외한 모든 AWS의 모든 작업에 대한 액세스를 거부합니다. 이 문은 `"Deny"` 및 `"NotAction"`의 조합을 사용하여 나열되지 않은 모든 작업에 대한 액세스를 명시적으로 거부합니다. 나열된 항목은 이 문에 따라 거부되거나 허용되지 않습니다. 하지만 정책의 다른 문에서 작업이 허용됩니다. 이 문의 로직에 대한 자세한 내용은 NotAction 및 Deny (p. 595) 단원을 참조하십시오. 사용자가 MFA를 사용하여 로그인한 경우 `Condition` 테스트가 실패하며 이 문은 어떠한 작업도 거부하지 않습니다. 이 경우 사용자에 대한 다른 정책 또는 문에 따라 사용자의 권한이 결정됩니다.

  이 문을 사용하면 MFA를 사용하여 로그인하지 않은 사용자는 나열된 작업만 수행할 수 있습니다. 또한 사용자는 다른 문 또는 정책이 해당 작업에 대한 액세스를 허용하는 경우에만 나열된 작업을 수행할 수 있습니다.

  `...IfExists` 키를 분실했을 경우 `Bool` 연산자의 `aws:MultiFactorAuthPresent` 버전은 조건이 true로 반환됩니다. 따라서 액세스 키와 같은 장기 자격 증명을 사용하여 API 작업에 액세스하는 사용자는 비 IAM API 작업에 대한 액세스가 거부됩니다.

이 정책은 사용자가 IAM 콘솔에서 Users(사용자) 페이지를 보거나 이 페이지를 사용하여 자신의 사용자 정보에 액세스할 수 있도록 허용합니다. 이 작업을 허용하려면 `iam:ListUsers` 작업을 `AllowViewAccountInfo` 문과 `DenyAllExceptListedIfNoMFA` 문에 추가합니다.

> **Warning**
>
> MFA 인증 없이 MFA 디바이스를 삭제할 수 있는 권한 추가를 허용하지 마십시오. 이 정책을 보유한 사용자는 스스로를 MFA 디바이스로 지정하려 하고 `iam:DeleteVirtualMFADevice` 수행에 필요한 권한이 부여되지 않았다는 오류가 표시될 수 있습니다. 이 경우 `DenyAllExceptListedIfNoMFA` 문에 해당 권한을 추가하지 마십시오. MFA를 사용하여 인증되지 않은 사용자에게 MFA 디바이스 삭제를 허용해서는 안 됩니다. 이전에 사용자에게 가상 MFA 디바이스를 할당하기 시작하고 프로세스를 취소한 경우 이 오류가 표시될 수 있습니다. 이 문제를 해결하려면 사용자 또는 다른 관리자가 AWS CLI 또는 AWS API를 사용하여 사용자의 기존 MFA 디바이스를 삭제해야 합니다. 자세한 내용은 iam:DeleteVirtualMFADevice를 수행할 권한이 없음 (p. 536) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowViewAccountInfo",
            "Effect": "Allow",
            "Action": "iam:ListVirtualMFADevices",
            "Resource": "*"
        },
        {
            "Sid": "AllowManageOwnVirtualMFADevice",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice"
            ],
            "Resource": "arn:aws:iam::*:mfa/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnUserMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice",
                "iam:EnableMFADevice",
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "DenyAllExceptListedIfNoMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:CreateVirtualMFADevice",
                "iam:EnableMFADevice",
                "iam:GetUser",
                "iam:ListMFADevices",
                "iam:ListVirtualMFADevices",
                "iam:ResyncMFADevice",
                "sts:GetSessionToken"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": "false"}
            }
        }
    ]
}
```

AWS: IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 콘솔 암호를 변경할 수 있도록 허용합니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.는 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 AWS Management 콘솔 암호를 변경할 수 있도록 허용합니다. 이 AWS Management 콘솔 페이지에는 계정 및 사용자 정보가 표시되지만, 사용자는 자신의 암호에만 액세스할 수 있습니다. 사용자가 MFA를 사용하여 자신의 모든 자격 증명을 관리하도록 허용하려면 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391) 단원을 참조하십시오. 사용자가 MFA를 사용하지 않고 자신의 자격 증명을 관리하도록 허용하려면 AWS: IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 394) 단원을 참조하십시오.

사용자가 My Security Credentials(내 보안 자격 증명) 페이지에 액세스할 수 있는 방법을 알아보려면 IAM 사용자가 자신의 암호를 변경하는 방법(콘솔) (p. 110) 단원을 참조하십시오.

이 정책이 하는 일은 무엇입니까?

- `ViewAccountPasswordRequirements` 문은 사용자가 자신의 IAM 사용자 암호를 변경하는 동안 계정 암호 요구 사항을 볼 수 있도록 허용합니다.
- `ChangeOwnPassword` 문은 사용자가 자신의 암호를 변경할 수 있도록 허용합니다. 또한 이 문에는 My Security Credentials(내 보안 자격 증명) 페이지에 있는 대부분의 정보를 보는 데 필요한 `GetUser` 작업도 포함되어 있습니다.

이 정책은 사용자가 IAM 콘솔에서 Users(사용자) 페이지를 보거나 이 페이지를 사용하여 자신의 사용자 정보에 액세스할 수 있도록 허용합니다. 이 작업을 허용하려면 `iam:ListUsers` 작업을 `ViewAccountPasswordRequirements` 문에 추가합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewAccountPasswordRequirements",
            "Effect": "Allow",
            "Action": "iam:GetAccountPasswordPolicy",
            "Resource": "*"
        },
        {
            "Sid": "ChangeOwnPassword",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ChangePassword"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        }
    ]
}
```

AWS: IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 암호, 액세스 키 및 SSH 퍼블릭 키를 관리할 수 있도록 허용합니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.는 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 암호, 액세스 키 및 X.509 인증서를 관리할 수 있도록 허용합니다. 이 AWS Management 콘솔 페이지에는 계정 ID 및 정식 사용자 ID와 같은 계정 정보가 표시됩니다. 또한 사용자는 자신의 암호, 액세스 키, MFA 디바이스, X.509 인증서, SSH 키 및 Git 자격 증명을 보고 편집할 수 있습니다. 이 예제 정책에는 자신의 암호, 액세스 키 및 X.509 인증서만 보고 편집하는 데 필요한 권한이 포함되어 있습니다. 사용자가 MFA를 사용하여 자신의 모든 자격 증명을 관리하도록 허용하려면 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391) 단원을 참조하십시오. 사용자가 MFA를 사용하지 않고 자신의 자격 증명을 관리하도록 허용하려면 AWS: IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 394) 단원을 참조하십시오.

사용자가 My Security Credentials(내 보안 자격 증명) 페이지에 액세스할 수 있는 방법을 알아보려면 IAM 사용자가 자신의 암호를 변경하는 방법(콘솔) (p. 110) 단원을 참조하십시오.

이 정책이 하는 일은 무엇입니까?

- `AllowViewAccountInfo` 문은 사용자가 계정 수준 정보를 볼 수 있도록 허용합니다. 이러한 권한은 리소스 ARN을 지원하지 않거나 리소스 ARN을 지정하는 데 필요하지 않기 때문에 자신의 문에 포함되어 있어야 합니다. 권한 대신 `"Resource" : "*"`를 지정합니다. 이 문에는 사용자가 특정 정보를 볼 수 있도록 허용하는 다음 작업이 포함되어 있습니다.
  - `GetAccountPasswordPolicy` – 자신의 IAM 사용자 암호를 변경하는 동안 계정 암호 요구 사항을 봅니다.
  - `GetAccountSummary` – 계정 ID 및 계정 정식 사용자 ID를 봅니다.
- `AllowManageOwnPasswords` 문은 사용자가 자신의 암호를 변경할 수 있도록 허용합니다. 또한 이 문에는 My Security Credentials(내 보안 자격 증명) 페이지에 있는 대부분의 정보를 보는 데 필요한 `GetUser` 작업도 포함되어 있습니다.
- `AllowManageOwnAccessKeys` 문은 사용자가 자신의 액세스 키를 생성, 업데이트 및 삭제할 수 있도록 허용합니다.

- `AllowManageOwnSSHPublicKeys` 문은 사용자가 CodeCommit에 대한 자신의 SSH 퍼블릭 키를 업로드, 업데이트 및 삭제할 수 있도록 허용합니다.

이 정책은 사용자가 자신의 MFA 디바이스를 보거나 관리하도록 허용하지 않습니다. 또한 사용자는 IAM 콘솔에서 Users(사용자) 페이지를 보거나 이 페이지를 사용하여 자신의 사용자 정보에 액세스할 수 없습니다. 이 작업을 허용하려면 `iam:ListUsers` 작업을 `AllowViewAccountInfo` 문에 추가합니다. 또한 이 문은 사용자가 자신의 사용자 페이지에서 암호를 변경하도록 허용하지 않습니다. 이 작업을 허용하려면 `iam:CreateLoginProfile`, `iam:DeleteLoginProfile`, `iam:GetLoginProfile` 및 `iam:UpdateLoginProfile` 작업을 `AllowManageOwnPasswords` 문에 추가합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowViewAccountInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowManageOwnPasswords",
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:GetUser"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:CreateAccessKey",
                "iam:DeleteAccessKey",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowManageOwnSSHPublicKeys",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteSSHPublicKey",
                "iam:GetSSHPublicKey",
                "iam:ListSSHPublicKeys",
                "iam:UpdateSSHPublicKey",
                "iam:UploadSSHPublicKey"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        }
    ]
}
```

AWS: 요청된 리전에 따라 AWS에 대한 액세스를 거부

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.는 나열된 서비스의 작업을 제외하고 `eu-central-1` 및 `eu-west-1` 리전 외부의 작업에 대한 액세스를 거부합니다. 이 정책은 콘솔에서 이 작업

을 완료하는 데 필요한 권한도 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 정책은 `NotAction` 요소를 `Deny` 효과와 함께 사용하여 문에 나열되지 않은 모든 작업에 대한 액세스를 거부합니다. CloudFront, IAM, Route 53 및 AWS Support 서비스의 작업은 거부되어서는 안 되는데, 이는 이러한 서비스가 물리적으로 `us-east-1` 리전에 위치한 단일 엔드포인트가 포함된 유명한 AWS 전역 서비스이기 때문입니다. 이러한 서비스에 대한 모든 요청이 `us-east-1` 리전으로 전달되기 때문에 `NotAction` 요소 없이 요청은 거부됩니다. 이 요소를 편집하여 `budgets`, `globalaccelerator`, `importexport`, `organizations` 또는 `waf` 등과 같이 기타 AWS 전역 서비스에 대한 작업을 포함합니다. 전역 엔드포인트를 보유한 모든 서비스에 대해 알아보려면 AWS General Reference의 AWS 리전 및 엔드포인트를 참조하십시오. `Deny` 효과와 `NotAction` 요소의 사용에 대해 자세히 알아보려면 IAM JSON 정책 요소: NotAction (p. 595) 단원을 참조하십시오.

> **Important**
>
> 이 정책은 어떤 작업도 허용하지 않습니다. 이 정책을 특정 작업을 허용하는 다른 정책과 함께 사용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

AWS: 소스 IP를 바탕으로 AWS에 대한 액세스 거부

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 지정된 IP 범위를 벗어나는 보안 주체에서 요청이 오는 경우 계정의 모든 AWS 작업에 대한 액세스를 거부합니다. 이 정책은 회사의 IP 주소가 지정된 범위 내에 있는 경우에 유용합니다. 이 정책은 보안 주체의 자격 증명을 사용하여 AWS 서비스에 의해 수행된 요청을 거부하지 않습니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

`"Effect": "Deny"`와 동일한 정책 문에서 부정적인 조건을 사용해야 합니다. 이렇게 하면 정책 문에 지정된 작업이 지정된 조건을 제외한 모든 조건에서 명시적으로 거부됩니다.

또한 이 정책에는 논리적 `AND`를 초래하는 여러 조건 키 (p. 608)가 포함되어 있습니다. 이 정책에서는 AWS 서비스가 `not`호출을 할 때 소스 IP 주소가 지정된 범위 `AND`의 `not`이면 모든 AWS 작업이 거부됩니다.

> **Important**
>
> 이 정책은 어떤 작업도 허용하지 않습니다. 이 정책을 특정 작업을 허용하는 다른 정책과 함께 사용합니다.

다른 정책에서 작업을 허용하는 경우 보안 주체는 IP 주소 범위 내에서 요청을 할 수 있습니다. 또한 AWS 서비스는 보안 주체의 자격 증명을 사용하여 요청할 수도 있습니다. 보안 주체가 IP 범위 밖에서 요청을 하면 요청이 거부됩니다. 서비스가 서비스 역할 또는 서비스 연결 역할을 사용해 보안 주체를 대신하여 호출을 하는 경우에도 요청이 거부됩니다.

`aws:SourceIp` 및 `aws:ViaAWSService` 조건 키 사용에 관한 자세한 내용은 AWS 전역 조건 컨텍스트 키 (p. 650) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "aws:SourceIp": [
                    "192.0.2.0/24",
                    "203.0.113.0/24"
                ]
            },
            "Bool": {"aws:ViaAWSService": "false"}
        }
    }
}
```

AWS Data Pipeline: 사용자가 생성하지 않은 DataPipeline 파이프라인에 대한 액세스 거부

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.: 사용자가 생성하지 않은 파이프라인에 대한 액세스 거부 `PipelineCreator` 필드의 값이 IAM 사용자 이름과 일치하는 경우 지정된 작업이 거부되지 않습니다. 이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.

> **Important**
>
> 이 정책은 어떤 작업도 허용하지 않습니다. 이 정책을 특정 작업을 허용하는 다른 정책과 함께 사용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExplicitDenyIfNotTheOwner",
            "Effect": "Deny",
            "Action": [
                "datapipeline:ActivatePipeline",
                "datapipeline:AddTags",
                "datapipeline:DeactivatePipeline",
                "datapipeline:DeletePipeline",
                "datapipeline:DescribeObjects",
                "datapipeline:EvaluateExpression",
                "datapipeline:GetPipelineDefinition",
                "datapipeline:PollForTask",
                "datapipeline:PutPipelineDefinition",
                "datapipeline:QueryObjects",
                "datapipeline:RemoveTags",
                "datapipeline:ReportTaskProgress",
                "datapipeline:ReportTaskRunnerHeartbeat",
                "datapipeline:SetStatus",
                "datapipeline:SetTaskStatus",
```

```
                "datapipeline:ValidatePipelineDefinition"
            ],
            "Resource": ["*"],
            "Condition": {
                "StringNotEquals": {"datapipeline:PipelineCreator": "${aws:userid}"}
            }
        }
    ]
}
```

Amazon DynamoDB: 특정 테이블에 대한 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 `MyTable` DynamoDB 테이블에 대한 모든 액세스를 허용합니다. 이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

> **Important**
>
> 이 정책은 DynamoDB 테이블에서 수행 가능한 모든 작업을 허용합니다. 이들 작업을 검토하려면 Amazon DynamoDB 개발자 안내서의 DynamoDB API 권한: 작업, 리소스 및 조건 참조 단원을 참조하십시오. 개별 작업 각각을 등록하여 동일한 권한을 제공할 수 있습니다. 그러나 `"dynamodb:List*"`와 같이 `Action`에서 와일드카드(`*`)를 사용하는 경우, DynamoDB에서 새 목록 작업을 추가한다면 정책을 업데이트할 필요가 없습니다.

이 정책은 지정된 이름을 지닌 DynamoDB 테이블에 대해서만 작업을 허용합니다. DynamoDB에 있는 모든 것에 대한 `Read` 액세스 권한을 사용자에게 허용하려면 AmazonDynamoDBReadOnlyAccess AWS 관리형 정책을 연결할 수도 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListAndDescribe",
            "Effect": "Allow",
            "Action": [
                "dynamodb:List*",
                "dynamodb:DescribeReservedCapacity*",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTimeToLive"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SpecificTable",
            "Effect": "Allow",
            "Action": [
                "dynamodb:BatchGet*",
                "dynamodb:DescribeStream",
                "dynamodb:DescribeTable",
                "dynamodb:Get*",
                "dynamodb:Query",
                "dynamodb:Scan",
                "dynamodb:BatchWrite*",
                "dynamodb:CreateTable",
                "dynamodb:Delete*",
                "dynamodb:Update*",
                "dynamodb:PutItem"
            ],
            "Resource": "arn:aws:dynamodb:*:*:table/MyTable"
        }
    ]
```

```
}
```

Amazon DynamoDB: 특정 열에 대한 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.는 특정 DynamoDB 열에 대한 액세스를 허용합니다. 이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

`dynamodb:Select` 요건을 설정하면 API 작업이 인덱스 프로젝션 등의 방법으로 허용되지 않는 속성을 반환할 수 없게 됩니다. DynamoDB 조건 키에 대한 자세한 정보는 Amazon DynamoDB 개발자 안내서의 조건 지정: 조건 키 사용 단원을 참조하십시오. IAM 정책의 `Condition` 블록 내에서 복수 조건 또는 복수 조건 키를 사용하는 방법에 관한 자세한 내용은 다수의 조건 값 (p. 601) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:GetItem",
                "dynamodb:BatchGetItem",
                "dynamodb:Query",
                "dynamodb:PutItem",
                "dynamodb:UpdateItem",
                "dynamodb:DeleteItem",
                "dynamodb:BatchWriteItem"
            ],
            "Resource": ["arn:aws:dynamodb:*:*:table/table-name"],
            "Condition": {
                "ForAllValues:StringEquals": {
                    "dynamodb:Attributes": [
                        "column-name-1",
                        "column-name-2",
                        "column-name-3"
                    ]
                },
                "StringEqualsIfExists": {"dynamodb:Select": "SPECIFIC_ATTRIBUTES"}
            }
        }
    ]
}
```

Amazon DynamoDB: Amazon Cognito ID를 기준으로 DynamoDB에 대한 행 수준 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 Amazon Cognito ID에 따라 `MyTable` DynamoDB 테이블에 대한 행 수준 액세스를 허용합니다. 이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 정책을 사용하려면 Cognito 사용자 ID가 파티션 키가 되도록 DynamoDB 테이블을 구성해야 합니다. 자세한 정보는 Amazon DynamoDB 개발자 안내서의 테이블 생성 단원을 참조하십시오.

DynamoDB 조건 키에 대한 자세한 정보는 Amazon DynamoDB 개발자 안내서의 조건 지정: 조건 키 사용 단원을 참조하십시오.

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

```
            "Effect": "Allow",
            "Action": [
                "dynamodb:DeleteItem",
                "dynamodb:GetItem",
                "dynamodb:PutItem",
                "dynamodb:Query",
                "dynamodb:UpdateItem"
            ],
            "Resource": ["arn:aws:dynamodb:*:*:table/MyTable"],
            "Condition": {
                "ForAllValues:StringEquals": {
                    "dynamodb:LeadingKeys": ["${cognito-identity.amazonaws.com:sub}"]
                }
            }
        }
    ]
}
```

Amazon EC2: EC2 인스턴스가 볼륨을 연결 또는 분리하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 서비스 역할에 연결할 수 있습니다. 이 정책은 지정된 EC2 인스턴스가 볼륨을 연결 또는 분리하도록 허용합니다. 인스턴스는 `Condition` 요소에 ARN과 함께 지정됩니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

Amazon EC2 인스턴스는 인스턴스 프로파일에 연결되어 있는 EC2 인스턴스의 AWS 서비스 역할 (p. 175)에 의해 부여된 권한으로 AWS 명령을 실행할 수 있습니다. 이 정책을 역할에 연결하거나 이 명령문을 기존 정책에 추가할 수 있습니다. *INSTANCE-ID*에 의해 식별된 인스턴스만 해당 계정(자신의 계정 포함)의 인스턴스에 볼륨을 연결하거나 분리할 수 있습니다. 더 큰 정책에 존재할 수 있는 다른 명령문 요소는 이 '하나의 명령문' 제한에 의해 영향을 받지 않습니다. IAM 정책을 만들어 Amazon EC2 리소스에 대한 액세스를 제어하는 방법은 Linux 인스턴스용 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 대한 액세스 제어 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "ArnEquals": {"ec2:SourceInstanceARN": "arn:aws:ec2:*:*:instance/instance-
id"}
            }
        }
    ]
}
```

Amazon EC2: 태그를 기준으로 Amazon EBS 볼륨을 EC2 인스턴스에 연결 또는 분리

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 EBS 볼륨 소유자가 태그 `VolumeUser`를 사용하여 정의한 자신의 EBS 볼륨을 개발 인스턴스(`Department=Dev`)로 태그가 지정된 EC2 인스턴스에 연결하거나 분리할 수 있도록 허용합니다. 이 정책은 AWS API 또는 AWS CLI를 사용해서

만 이 작업을 완료할 수 있는 권한을 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringEquals": {"ec2:ResourceTag/Department": "Development"}
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "StringEquals": {"ec2:ResourceTag/VolumeUser": "${aws:username}"}
            }
        }
    ]
}
```

Amazon EC2: 특정 서브넷에 있는 EC2 인스턴스를 프로그래밍 방식으로 콘솔에서 시작할 수 있도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 모든 EC2 객체에 대한 정보의 열거와 특정 서브넷에서의 EC2 인스턴스 시작을 허용합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "ec2:GetConsole*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:subnet/subnet-subnet-id",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
```

```
        }
    ]
}
```

Amazon EC2: 특정 VPC와 연결된 EC2 보안 그룹을 콘솔에서 프로그래밍 방식으로 관리할 수 있도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 특정 가상 프라이빗 클라우드(VPC)와 관련된 Amazon EC2 보안 그룹을 관리할 수 있도록 합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:*:*:vpc/vpc-vpc-id"
                }
            }
        },
        {
            "Action": [
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Amazon EC2: 프로그래밍 방식으로 콘솔에서 사용자가 태그를 지정한 EC2 인스턴스를 시작 또는 중지할 수 있도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 IAM 사용자가 EC2 인스턴스를 시작 또는 중지할 수 있도록 허용하지만, 인스턴스 태그 `Owner`가 사용자의 사용자 이름의 값과 같은 경우로 제한합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
```

```
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Owner": "${aws:username}"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

EC2: 태그를 기반으로 인스턴스 시작 또는 중지

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 태그 키–값 페어 `Project = DataAnalytics`를 통한 인스턴스 시작 또는 중지를 허용하지만, 태그 키–값 페어 `Department = Data`가 있는 보안 주체만 가능합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

정책의 조건은 조건의 두 부분이 모두 true인 경우 true를 반환합니다. 인스턴스에 `Project=DataAnalytics` 태그가 있어야 합니다. 또한, 요청을 보내는 IAM 보안 주체(사용자나 역할)에 `Department=Data` 태그가 있어야 합니다.

> **Note**
>
> 가장 좋은 방법은 `aws:PrincipalTag` 조건 키가 있는 정책을 IAM 그룹에 연결하는 것입니다. 이 경우 일부 사용자는 지정된 태그가 있고 일부 사용자는 그렇지 않을 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StartStopIfTags",
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Project": "DataAnalytics",
                    "aws:PrincipalTag/Department": "Data"
                }
            }
        }
    ]
}
```

EC2: 일치하는 보안 주체 및 리소스 태그를 기반으로 인스턴스 시작 또는 중지

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.를 사용하면 인스턴스의 리소스 태그와 보안 주체 태그가 `CostCenter` 태그 키와 동일한 값을 가질 때 Amazon EC2 인스턴스를 시작하거나 중지할 수 있습니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

Note

가장 좋은 방법은 aws:PrincipalTag 조건 키가 있는 정책을 IAM 그룹에 연결하는 것입니다. 이 경우 일부 사용자는 지정된 태그가 있고 일부 사용자는 그렇지 않을 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"}}
    }
}
```

Amazon EC2: 특정 리전 내에서의 모든 EC2 액세스를 프로그래밍 방식으로 콘솔에서 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 특정 리전 내에서 모든 EC2 액세스를 허용합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:*",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "region"
                }
            }
        }
    ]
}
```

Amazon EC2: 프로그래밍 방식으로 콘솔에서 EC2 인스턴스를 시작 또는 중지하고 보안 그룹을 수정할 수 있도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 프로그래밍 방식으로 콘솔에서 특정 EC2 인스턴스를 시작 또는 중지하고 특정 보안 그룹을 수정할 수 있도록 허용합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupReferences",
```

```
                "ec2:DescribeStaleSecurityGroups"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/i-instance-id",
                "arn:aws:ec2:*:*:security-group/sg-security-group-id"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Amazon EC2: 특정 EC2 작업에 대해 MFA(GetSessionToken)를 요구

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.의 경우 Amazon EC2에서 모든 AWS API 작업에 대한 전체 액세스를 허용합니다. 하지만 사용자가 Multi-Factor Authentication(MFA) (p. 119)을 사용하여 인증되지 않은 경우 `StopInstances` 및 `TerminateInstances` API 작업에 대해 액세스는 명시적으로 거부됩니다. 이를 프로그래밍 방식으로 수행하려면 사용자가 `GetSessionToken` 작업을 호출하는 동안 선택 사항인 `SerialNumber` 및 `TokenCode` 값을 포함해야 합니다. 이 작업은 MFA를 사용하여 인증된 임시 자격 증명을 반환합니다. GetSessionToken에 대해 자세히 알아보려면 GetSessionToken—신뢰할 수 없는 환경에 있는 사용자를 위한 임시 자격 증명 (p. 310) 단원을 참조하십시오.

이 정책이 하는 일은 무엇입니까?

- `AllowAllActionsForEC2` 문은 모든 Amazon EC2 작업을 허용합니다.
- `DenyStopAndTerminateWhenMFAIsNotPresent` 문은 MFA 컨텍스트가 누락된 경우 `StopInstances` 및 `TerminateInstances` 작업을 거부합니다. 따라서 Multi-Factor Authentication(MFA) 컨텍스트가 누락된 경우(MFA가 사용되지 않은 경우) 작업이 거부됩니다. 거부는 허용을 무시합니다.

> **Note**
>
> MFA를 사용하지 않을 때는 키가 없어 키를 평가할 수 없기 때문에 `Deny` 문의 `MultiFactorAuthPresent`에 대한 조건 확인이 `{"Bool": {"aws:MultiFactorAuthPresent":false}}`이면 안 됩니다. 따라서 값을 확인하기 전에 `BoolIfExists`를 사용하여 키가 있는지 확인해야 합니다. 자세한 내용은 IfExists 조건 연산자 (p. 607) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllActionsForEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
```

```
        {
            "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

Amazon EC2: EC2 인스턴스 종료를 IP 주소 범위로 제한

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 작업을 허용하지만 요청이 지정된 IP 범위를 벗어나는 곳에서 오는 경우 액세스를 명시적으로 거부함으로써 EC2 인스턴스를 제한합니다. 이 정책은 회사의 IP 주소가 지정된 범위 내에 있는 경우에 유용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 정책을 `ec2:TerminateInstances` 작업을 허용하는 다른 정책(예: AmazonEC2FullAccess AWS 관리형 정책)과 조합하여 사용하는 경우 액세스가 거부됩니다. 이는 명시적 거부문이 허용문보다 우선 적용되기 때문입니다. 자세한 내용은 the section called “계정 내에서 요청 허용 여부 결정” (p. 625)를 참조하십시오.

> **Important**
>
> `aws:SourceIp` 조건 키는 여러분을 대신하여 호출하는 AWS CloudFormation과 같은AWS 서비스에 대한 액세스를 거부합니다. `aws:SourceIp` 조건 키 사용에 관한 자세한 내용은 AWS 전역 조건 컨텍스트 키 (p. 650) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ec2:TerminateInstances"],
            "Resource": ["*"]
        },
        {
            "Effect": "Deny",
            "Action": ["ec2:TerminateInstances"],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            },
            "Resource": ["*"]
        }
    ]
}
```

IAM: 정책 시뮬레이터 API에 액세스

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 현재 AWS 계정에서 사용자, 그룹 또는 역할에 연결되어 있는 정책에 대해 정책 시뮬레이터 API의 사용을 허용합니다. 또한 이 정책은

API에 문자열로 전달되는 덜 민감한 정책을 시뮬레이션할 수 있도록 액세스를 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetContextKeysForCustomPolicy",
                "iam:GetContextKeysForPrincipalPolicy",
                "iam:SimulateCustomPolicy",
                "iam:SimulatePrincipalPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Note

사용자가 정책 시뮬레이터 콘솔에 액세스하여 현재 AWS 계정의 사용자, 그룹 또는 역할에 연결된 정책을 시뮬레이션하도록 허용하는 방법은 IAM: 정책 시뮬레이터 콘솔 액세스 (p. 412) 단원을 참조하십시오.

IAM: 정책 시뮬레이터 콘솔 액세스

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 현재 AWS 계정에서 사용자, 그룹 또는 역할에 연결되어 있는 정책에 대해 정책 시뮬레이터 콘솔의 사용을 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.

다음 위치에서 IAM 정책 시뮬레이터 콘솔에 액세스할 수 있습니다. https://policysim.aws.amazon.com/

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetGroup",
                "iam:GetGroupPolicy",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListAttachedRolePolicies",
                "iam:ListAttachedUserPolicies",
                "iam:ListGroups",
                "iam:ListGroupPolicies",
                "iam:ListGroupsForUser",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:ListUserPolicies",
                "iam:ListUsers"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

IAM: 특정 태그가 있는 역할 수임

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서 IAM 사용자가 태그 키-값 페어가 `Project = ExampleCorpABC`인 역할을 수임하도록 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 태그가 포함된 역할이 사용자와 동일한 계정에 존재하는 경우 사용자는 해당 역할을 수임할 수 있습니다. 이 태그가 포함된 역할이 사용자가 아닌 다른 계정에 존재하는 경우 추가 권한이 필요합니다. 교차 계정 역할의 신뢰 정책에서 사용자 또는 사용자 계정의 모든 멤버가 역할을 수임하도록 허용해야 합니다. 교차 계정 액세스에 대한 역할 사용에 대한 자세한 정보는 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공 (p. 178) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:ResourceTag/Project": "ExampleCorpABC"}
            }
        }
    ]
}
```

IAM: 프로그래밍 방식에서, 그리고 콘솔에서 여러 서비스에 대한 액세스를 허용 및 거부

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다. 사용을 통해 IAM에서 여러 서비스에 대한 전체 액세스 및 제한적 자체 관리 액세스를 허용합니다. 또한 Amazon S3 `logs` 버킷 또는 Amazon EC2 `i-1234567890abcdef0` 인스턴스에 대한 액세스를 거부합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

> **Warning**
>
> 이 정책은 여러 서비스의 모든 작업 및 리소스에 대한 전체 액세스를 허용합니다. 이 정책은 신뢰할 수 있는 관리자에게만 적용되어야 합니다.

이 정책을 권한 경계로 사용하여 자격 증명 기반 정책이 IAM 사용자에게 부여할 수 있는 최대 권한을 정의할 수 있습니다. 자세한 내용은 권한 경계를 사용하여 다른 것에 책임 위임 (p. 367) 단원을 참조하십시오. 정책이 사용자에 대한 권한 경계로 사용되는 경우 문에서 다음 경계를 정의합니다.

- `AllowServices` 문은 지정된 AWS 서비스에 대한 완전한 액세스를 허용합니다. 이런 서비스의 사용자 작업이 사용자에 연결된 권한 정책에 따라서만 제한된다는 의미입니다.
- `AllowIAMConsoleForCredentials` 문에서 모든 IAM 사용자를 나열할 수 있는 액세스를 허용합니다. 이 액세스는 AWS Management 콘솔의 사용자 페이지를 탐색하는 데 필요합니다. 또한 계정의 암호 요구 사항을 확인하도록 허용합니다. 이 액세스는 사용자가 자신의 고유 암호를 변경할 때 필요합니다.
- `AllowManageOwnPasswordAndAccessKeys` 문은 사용자가 자신의 고유 콘솔 암호와 프로그래밍 방식의 액세스 키만 관리하도록 허용합니다. 이런 점은 중요합니다. 또 다른 정책에서 사용자에게 전체 IAM 액세스가 되는 권한 정책을 부여한다면 사용자 자신 또는 다른 사용자 권한을 변경할 수 있기 때문입니다. 이 설명문은 이런 상황을 방지할 수 있습니다.

- DenyS3Logs 설명문은 logs 버킷 액세스를 명시적으로 거부합니다. 이 정책은 사용자의 회사 제한을 적용합니다.
- DenyEC2Production 설명문은 i-1234567890abcdef0 인스턴스 액세스를 명시적으로 거부합니다.

이 정책은 다른 서비스 또는 작업에 대한 액세스를 허용하지 않습니다. 정책이 사용자에 대한 권한 경계로 사용되는 경우 사용자와 연결된 다른 정책에서 이러한 작업을 허용하더라도 AWS에서는 요청을 거부합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowServices",
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "cloudwatch:*",
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowIAMConsoleForCredentials",
            "Effect": "Allow",
            "Action": [
                "iam:ListUsers",
                "iam:GetAccountPasswordPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowManageOwnPasswordAndAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:*AccessKey*",
                "iam:ChangePassword",
                "iam:GetUser",
                "iam:*LoginProfile*"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "DenyS3Logs",
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::logs",
                "arn:aws:s3:::logs/*"
            ]
        },
        {
            "Sid": "DenyEC2Production",
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "arn:aws:ec2:*:*:instance/i-1234567890abcdef0"
        }
    ]
}
```

IAM: 특정 태그가 있는 사용자에게 특정 태그 추가

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 태그 값 Marketing, Development 또는 QualityAssurance가 지정된 태그 키 Department를 IAM 사용자에게 추가하도록

허용합니다. 사용자가 이미 태그 키–값 페어 `JobFunction = manager`를 포함해야 합니다. 이 정책을 사용하여 관리자가 세 부서 중 하나에 속하도록 요구할 수 있습니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

`ListTagsForAllUsers` 문을 사용하면 계정의 모든 사용자에 대한 태그를 볼 수 있습니다.

`TagManagerWithSpecificDepartment` 문의 첫 번째 조건에는 `StringEquals` 조건 연산자가 사용됩니다. 이 조건은 조건의 두 부분이 모두 true인 경우 true를 반환합니다. 태그 지정될 사용자에게 이미 `JobFunction=Manager` 태그가 있어야 합니다. 나열된 태그 값 중 하나가 지정된 `Department` 태그 키가 요청에 포함되어야 합니다.

두 번째 조건에는 `ForAllValues:StringEquals` 조건 연산자가 사용됩니다. 이 조건은 요청의 모든 태그 키가 정책의 키와 일치하는 경우 true를 반환합니다. 즉 `Department`가 요청의 유일한 태그 키여야 합니다. `ForAllValues` 사용에 관한 자세한 정보는 다수의 키 또는 값을 사용하는 조건 생성 (p. 608) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListTagsForAllUsers",
            "Effect": "Allow",
            "Action": [
                "iam:ListUserTags",
                "iam:ListUsers"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagManagerWithSpecificDepartment",
            "Effect": "Allow",
            "Action": "iam:TagUser",
            "Resource": "*",
            "Condition": {"StringEquals": {
                "iam:ResourceTag/JobFunction": "Manager",
                "aws:RequestTag/Department": [
                    "Marketing",
                    "Development",
                    "QualityAssurance"
                    ]
                },
                "ForAllValues:StringEquals": {"aws:TagKeys": "Department"}
            }
        }
    ]
}
```

IAM: 특정 값이 있는 특정 태그 추가

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.를 사용하면 모든 IAM 사용자 또는 역할에 태그 키 `CostCenter`와 태그 값 `A-123` 또는 태그 값 `B-456`만 추가할 수 있습니다. 이 정책을 사용하여 특정 태그 키 및 태그 값 세트로 태그 지정을 제한할 수 있습니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

`ConsoleDisplay` 문을 사용하면 계정의 모든 사용자 및 역할에 대한 태그를 볼 수 있습니다.

`AddTag` 문의 첫 번째 조건에는 `StringEquals` 조건 연산자가 사용됩니다. 이 조건은 나열된 태그 값 중 하나가 지정된 `CostCenter` 태그 키가 요청에 포함된 경우 true를 반환합니다.

두 번째 조건에는 `ForAllValues:StringEquals` 조건 연산자가 사용됩니다. 이 조건은 요청의 모든 태그 키가 정책의 키와 일치하는 경우 true를 반환합니다. 즉 `CostCenter`가 요청의 유일한 태그 키여야 합니다. `ForAllValues` 사용에 관한 자세한 정보는 다수의 키 또는 값을 사용하는 조건 생성 (p. 608) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListRoles",
                "iam:ListRoleTags",
                "iam:ListUsers",
                "iam:ListUserTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AddTag",
            "Effect": "Allow",
            "Action": [
                "iam:TagUser",
                "iam:TagRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/CostCenter": [
                        "A-123",
                        "B-456"
                    ]
                },
                "ForAllValues:StringEquals": {"aws:TagKeys": "CostCenter"}
            }
        }
    ]
}
```

IAM: 특정 태그가 있는 새 사용자만 생성

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 IAM 사용자 생성을 허용하지만 `Department` 및 `JobFunction` 태그 키 중 하나 또는 두 개 모두를 사용해야 합니다. `Department` 태그 키에는 `Development` 또는 `QualityAssurance` 태그 값이 지정되어야 합니다. `JobFunction` 태그 키에는 `Employee` 태그 값이 지정되어야 합니다. 새 사용자가 특정 업무 기능 및 부서를 갖도록 하려면 이 정책을 사용하십시오.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 설명문의 첫 번째 조건에는 `StringEqualsIfExists` 조건 연산자가 사용됩니다. 요청에 키가 `Department` 또는 `JobFunction`인 태그가 있는 경우 태그에 지정된 값이 있어야 합니다. 두 키가 모두 없으면 이 조건은 true로 평가됩니다. 조건이 false로 평가되는 유일한 경우는 지정된 조건 키 중 하나가 요청에 있지만 허용된 값이 아닌 다른 값이 지정된 경우뿐입니다. `IfExists` 사용에 관한 자세한 정보는 IfExists 조건 연산자 (p. 607) 단원을 참조하십시오.

두 번째 조건에는 `ForAllValues:StringEquals` 조건 연산자가 사용됩니다. 이 조건은 요청에 지정된 각각의 태그 키와 정책의 하나 이상의 값이 일치하는 경우 true를 반환합니다. 즉 요청의 모든 태그가 이 목록에 있어야 합니다. 하지만 요청은 목록에 있는 태그 중 하나만 포함할 수 있습니다. 예를 들면 `Department=QualityAssurance` 태그만 지정된 IAM 사용자를 생성할 수 있습니다. 하지만 `JobFunction=employee` 태그와 `Project=core` 태그가 지정된 IAM 사용자는 생성할 수 없습니다.

`ForAllValues` 사용에 관한 자세한 정보는 다수의 키 또는 값을 사용하는 조건 생성 (p. 608) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagUsersWithOnlyTheseTags",
            "Effect": "Allow",
            "Action": [
                "iam:CreateUser",
                "iam:TagUser"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIfExists": {
                    "aws:RequestTag/Department": [
                        "Development",
                        "QualityAssurance"
                    ],
                    "aws:RequestTag/JobFunction": "Employee"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "Department",
                        "JobFunction"
                    ]
                }
            }
        }
    ]
}
```

IAM: IAM 자격 증명 보고서 생성 및 검색

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서 사용자가 AWS 계정에 있는 모든 IAM 사용자를 나열한 보고서를 생성 및 다운로드하도록 허용합니다. 이 보고서에는 암호, 액세스 키, MFA 디바이스, 서명 인증서를 포함한 사용자 자격 증명의 상태가 포함됩니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.

자격 증명 보고서에 대한 자세한 내용은 AWS 계정의 자격 증명 보고서 가져오기 (p. 156) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:GenerateCredentialReport",
            "iam:GetCredentialReport"
        ],
        "Resource": "*"
    }
}
```

IAM: 프로그래밍 방식으로, 그리고 콘솔에서 그룹의 멤버십을 관리하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다. 사용을 통해 이름이 `MarketingTeam`인 그룹의 멤버십을 업데이트할 수 있습니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필

요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 정책이 하는 일은 무엇입니까?

- `ViewGroups` 문은 사용자가 AWS Management 콘솔의 모든 사용자 및 그룹을 나열하도록 허용합니다. 또한 사용자가 계정 내 사용자의 기본 정보를 볼 수 있도록 허용합니다. 이러한 권한은 리소스 ARN을 지원하지 않거나 리소스 ARN을 지정하는 데 필요하지 않기 때문에 자신의 문에 포함되어 있어야 합니다. 권한 대신 `"Resource" : "*"`를 지정합니다.
- `ViewEditThisGroup` 문은 사용자가 `MarketingTeam` 그룹에 대한 정보를 보고 해당 그룹에서 사용자를 제거할 수 있도록 허용합니다.

이 정책은 사용자가 사용자 또는 `MarketingTeam` 그룹의 권한을 보거나 편집하도록 허용하지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewGroups",
            "Effect": "Allow",
            "Action": [
                "iam:ListGroups",
                "iam:ListUsers",
                "iam:GetUser",
                "iam:ListGroupsForUser"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewEditThisGroup",
            "Effect": "Allow",
            "Action": [
                "iam:AddUserToGroup",
                "iam:RemoveUserFromGroup",
                "iam:GetGroup"
            ],
            "Resource": "arn:aws:iam::*:group/MarketingTeam"
        }
    ]
}
```

IAM: 특정 태그 관리

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.를 사용하면 태그 키 `Department`가 있는 IAM 태그를 추가 및 제거할 수 있습니다. 이 정책은 `Department` 태그의 가치를 제한하지 않습니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:TagUser",
            "iam:TagRole",
            "iam:UntagUser",
            "iam:UntagRole"
        ],
        "Resource": "*",
        "Condition": {"ForAllValues:StringEquals": {"aws:TagKeys": "Department"}}
```

```
    }
}
```

IAM: IAM 역할을 특정 AWS 서비스로 전달

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다. 사용을 통해 모든 IAM 서비스 역할 Amazon CloudWatch 서비스로 전달할 수 있습니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

서비스 역할은 AWS 서비스를 역할을 수임할 수 있는 보안 주체로 지정하는 IAM 역할입니다. 이를 사용하면 서비스는 역할을 수임하고 사용자를 대신해 다른 서비스의 리소스에 액세스할 수 있습니다. Amazon CloudWatch에서 전달한 역할을 수임하도록 허용하려면 `cloudwatch.amazonaws.com` 서비스 보안 주체를 역할의 신뢰 정책 내 보안 주체로 지정해야 합니다. 서비스 보안 주체는 서비스가 정의합니다. 서비스의 보안 주체를 확인하려면 해당 서비스의 설명서를 참조하십시오. 일부 서비스에 대해서는 IAM로 작업하는 AWS 서비스 (p. 573)을 참조하여 서비스 연결 역할 열에 예라고 표시된 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다. `amazonaws.com` 검색을 통해 서비스 보안 주체를 확인합니다.

서비스 역할을 서비스로 전달하는 것에 대해 자세히 알아보려면 사용자에게 AWS 서비스에 역할을 전달할 권한 부여 (p. 254) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:PassedToService": "cloudwatch.amazonaws.com"}
            }
        }
    ]
}
```

IAM: 보고 없이 IAM 콘솔에 대한 읽기 전용 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 IAM 사용자가 문자열 `Get`, `List`, `Generate`로 시작하는 모든 IAM 작업을 수행하도록 허용합니다. 사용자가 콘솔에서 작업할 경우 콘솔은 그룹, 사용자, 역할 및 정책 나열과 이러한 리소스에 대한 보고서 생성을 IAM에 요청합니다.

별표(*)는 와일드카드 역할을 합니다. 정책에서 `iam:Get*`을 사용할 때 결과 권한에는 `Get`으로 시작하는 모든 IAM 작업(예: `GetUser` 및 `GetRole`)이 포함됩니다. 와일드카드는 향후 새로운 유형의 엔터티가 IAM에 추가되는 경우 유용합니다. 이러한 경우 정책에서 부여한 권한은 자동으로 사용자가 새로운 엔터티에 대한 세부 정보를 나열하고 가져오도록 허용합니다.

이 정책은 보고 목적으로 사용될 수 없습니다.

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

```
    }
}
```

IAM: IAM 콘솔에 대한 읽기 전용 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 IAM 사용자가 문자열 `Get`, `List`, `Generate`로 시작하는 모든 IAM 작업을 수행하도록 허용합니다. 사용자가 IAM 콘솔에서 작업할 경우 콘솔은 그룹, 사용자, 역할 및 정책 나열과 이러한 리소스에 대한 보고서 생성을 요청합니다.

별표(*)는 와일드카드 역할을 합니다. 정책에서 `iam:Get*`을 사용할 때 결과 권한에는 `Get`으로 시작하는 모든 IAM 작업(예: `GetUser` 및 `GetRole`)이 포함됩니다. 향후 새로운 유형의 엔터티가 IAM에 추가되는 경우 와일드카드를 사용하는 것이 이롭습니다. 이러한 경우 정책에서 부여한 권한은 자동으로 사용자가 새로운 엔터티에 대한 세부 정보를 나열하고 가져오도록 허용합니다.

콘솔 액세스 또는 보고 목적으로 이 정책을 사용합니다.

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

IAM: 특정 IAM 사용자가 프로그래밍 방식으로, 그리고 콘솔에서 그룹을 관리하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 특정 IAM 사용자가 `AllUsers` 그룹을 관리하도록 허용합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *`#### ## ### ###`*를 본인의 정보로 대체하십시오.

이 정책이 하는 일은 무엇입니까?

- `AllowAllUsersToListAllGroups` 문은 모든 그룹의 표시를 허용합니다. 이는 콘솔 액세스에 대해 필수입니다. 이 권한은 리소스 ARN을 지원하지 않으므로 자신의 문에 들어 있어야 합니다. 권한 대신 `"Resource" : "*"`를 지정합니다.
- `AllowAllUsersToViewAndManageThisGroup` 문은 그룹 리소스 유형에서 수행할 수 있는 모든 그룹 작업을 허용합니다. 사용자 리소스 유형에서는 수행할 수 있지만 그룹 리소스 유형에서 수행할 수 없는 `ListGroupsForUser` 작업은 허용하지 않습니다. IAM 작업에 지정할 수 있는 리소스 유형에 대한 자세한 내용은 AWS Identity and Access Management에서 사용되는 작업, 리소스 및 조건 키를 참조하십시오.
- `LimitGroupManagementAccessToSpecificUsers` 문은 이름이 지정된 사용자의 쓰기 액세스와 그룹 작업 관리 권한을 거부합니다. 정책에 지정된 사용자가 그룹을 변경하려는 경우 문에서 이 요청을 거부합니다. 해당 요청은 `AllowAllUsersToViewAndManageThisGroup` 문에서 허용합니다. 다른 사용자가 이 작업을 수행하려는 경우 요청은 거부됩니다. IAM 콘솔에서 이 정책을 생성하는 동안 쓰기 또는 권한 관리로 정의된 IAM 작업을 볼 수 있습니다. 이를 수행하려면 JSON 탭에서 시각적 편집기 탭으로 전환합니다. 액세스 수준에 대한 자세한 내용은 AWS Identity and Access Management에서 사용되는 작업, 리소스 및 조건 키를 참조하십시오.

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

```
    "Statement": [
        {
            "Sid": "AllowAllUsersToListAllGroups",
            "Effect": "Allow",
            "Action": "iam:ListGroups",
            "Resource": "*"
        },
        {
            "Sid": "AllowAllUsersToViewAndManageThisGroup",
            "Effect": "Allow",
            "Action": "iam:*Group*",
            "Resource": "arn:aws:iam::*:group/AllUsers"
        },
        {
            "Sid": "LimitGroupManagementAccessToSpecificUsers",
            "Effect": "Deny",
            "Action": [
                "iam:AddUserToGroup",
                "iam:CreateGroup",
                "iam:RemoveUserFromGroup",
                "iam:DeleteGroup",
                "iam:AttachGroupPolicy",
                "iam:UpdateGroup",
                "iam:DetachGroupPolicy",
                "iam:DeleteGroupPolicy",
                "iam:PutGroupPolicy"
            ],
            "Resource": "arn:aws:iam::*:group/AllUsers",
            "Condition": {
                "StringNotEquals": {
                    "aws:username": [
                        "srodriguez",
                        "mjackson",
                        "adesai"
                    ]
                }
            }
        }
    ]
}
```

IAM: 프로그래밍 방식으로, 그리고 콘솔에서 계정 암호 요구 사항을 설정하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 사용자가 계정의 암호 요구 사항을 보고 업데이트하도록 허용합니다. 암호 요구 사항은 계정 멤버의 암호에 대한 복잡성 요구 사항 및 필수 교체 기산을 지정합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.

계정에 대해 암호 요구 사항 정책을 설정하는 방법을 알아보려면 IAM 사용자의 계정 암호 정책 설정 (p. 101) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:GetAccountPasswordPolicy",
            "iam:UpdateAccountPasswordPolicy"
        ],
        "Resource": "*"
    }
}
```

IAM: 사용자 경로를 바탕으로 정책 시뮬레이터 API 액세스

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 경로 `Department/Development`을 지닌 사용자에 대해서만 정책 시뮬레이터 API의 사용을 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetContextKeysForPrincipalPolicy",
                "iam:SimulatePrincipalPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:user/Department/Development/*"
        }
    ]
}
```

Note

경로 `Department/Development`을 지닌 사용자에 대해 정책 시뮬레이터 콘솔의 사용을 허용하는 정책을 생성하는 방법은 IAM: 사용자 경로를 바탕으로 정책 시뮬레이터 콘솔 액세스 (p. 422) 단원을 참조하십시오.

IAM: 사용자 경로를 바탕으로 정책 시뮬레이터 콘솔 액세스

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 경로 `Department/Development`을 지닌 사용자에 대해서만 정책 시뮬레이터 콘솔의 사용을 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

다음 위치에서 IAM 정책 시뮬레이터에 액세스할 수 있습니다. https://policysim.aws.amazon.com/

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetPolicy",
                "iam:GetUserPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:GetUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListGroupsForUser",
                "iam:ListUserPolicies",
                "iam:ListUsers"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:user/Department/Development/*"
        }
    ]
}
```

IAM: IAM 사용자가 MFA 디바이스를 스스로 관리하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 IAM 사용자가 자신의 Multi-Factor Authentication(MFA) (p. 119) 디바이스를 자체 관리할 수 있도록 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.

> **Note**
>
> AWS에 로그인되어 있는 사용자에게 이들 권한을 추가하는 경우 사용자가 로그아웃한 다음 변경을 확인해야 할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListActions",
            "Effect": "Allow",
            "Action": [
                "iam:ListUsers",
                "iam:ListVirtualMFADevices"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowIndividualUserToListOnlyTheirOwnMFA",
            "Effect": "Allow",
            "Action": [
                "iam:ListMFADevices"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/*",
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Sid": "AllowIndividualUserToManageTheirOwnMFA",
            "Effect": "Allow",
            "Action": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:EnableMFADevice",
                "iam:ResyncMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Sid": "AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ],
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        },
```

```
        {
            "Sid": "BlockMostAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:CreateVirtualMFADevice",
                "iam:EnableMFADevice",
                "iam:ListMFADevices",
                "iam:ListUsers",
                "iam:ListVirtualMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

IAM: 프로그램 방식으로 콘솔에서 IAM 사용자가 자신의 자격 증명을 교체하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 IAM 사용자가 자신의 액세스 키, 서명 인증서, 서비스별 자격 증명 및 암호를 교체하도록 허용합니다. 이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListUsers",
                "iam:GetAccountPasswordPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:*AccessKey*",
                "iam:ChangePassword",
                "iam:GetUser",
                "iam:*ServiceSpecificCredential*",
                "iam:*SigningCertificate*"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        }
    ]
}
```

사용자가 콘솔에서 자신의 암호를 변경하는 방법에 대해서는 the section called “IAM 사용자가 자신의 암호를 변경하는 방법” (p. 110) 단원을 참조하십시오.

IAM: 조직 정책에 대해 서비스에서 마지막으로 액세스한 데이터 보기

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.의 경우 특정 조직 정책에 대해 서비스에서 마지막으로 액세스한 데이터를 보도록 허용합니다. 이 정책은 `p-policy123` ID가 포함된 서비스 제어 정책(SCP)에 대한 데이터 검색을 허용합니다. 보고서를 생성하고 보는 사람은 AWS Organizations 마스터 계정 자격 증명을 사용하여 인증되어야 합니다. 이 정책은 요청자가 조직에 있는 조직 엔터티에 대한 데이터를 검색하도록 허용합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

필요 권한, 문제 해결, 지원되는 리전을 포함한 서비스에서 마지막으로 액세스한 데이터 대한 중요 정보는 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "AllowOrgsReadOnlyAndIamGetReport",
        "Effect": "Allow",
        "Action": [
            "iam:GetOrganizationsAccessReport",
            "organizations:Describe*",
            "organizations:List*"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowGenerateReportOnlyForThePolicy",
        "Effect": "Allow",
        "Action": "iam:GenerateOrganizationsAccessReport",
        "Resource": "*",
        "Condition": {
            "StringEquals": {"iam:OrganizationsPolicyId": "p-policy123"}
        }
    }
}
```

IAM: IAM 사용자, 그룹 또는 역할에 적용 가능한 관리형 정책을 제한

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 IAM 사용자, 그룹 또는 역할에 적용 가능한 고객 관리형 및 AWS 관리형 정책을 제한합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:AttachUserPolicy",
            "iam:DetachUserPolicy"
        ],
        "Resource": "*",
        "Condition": {
            "ArnEquals": {
                "iam:PolicyARN": [
                    "arn:aws:iam::*:policy/policy-name-1",
                    "arn:aws:iam::*:policy/policy-name-2"
                ]
```

```
            }
        }
    }
}
```

AWS Lambda: Lambda 함수의 Amazon DynamoDB 테이블 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 특정 Amazon DynamoDB 테이블에 대한 읽기 및 쓰기 액세스를 허용합니다. 이 정책은 또한 CloudWatch Logs에 대한 로그 파일 쓰기를 허용합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 정책을 사용하려면 정책을 Lambda 서비스 역할 (p. 233)에 연결합니다. 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하도록 계정에 생성한 역할입니다. 이 서비스 역할에는 AWS Lambda가 신뢰 정책의 보안 주체로 포함되어야 합니다. 이 정책을 사용하는 방법에 대한 자세한 내용은 AWS 보안 블로그의 AWS IAM 정책을 생성하여 Amazon DynamoDB 테이블에 대한 AWS Lambda 액세스를 허용하는 방법을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteTable",
            "Effect": "Allow",
            "Action": [
                "dynamodb:BatchGetItem",
                "dynamodb:GetItem",
                "dynamodb:Query",
                "dynamodb:Scan",
                "dynamodb:BatchWriteItem",
                "dynamodb:PutItem",
                "dynamodb:UpdateItem"
            ],
            "Resource": "arn:aws:dynamodb:*:*:table/SampleTable"
        },
        {
            "Sid": "GetStreamRecords",
            "Effect": "Allow",
            "Action": "dynamodb:GetRecords",
            "Resource": "arn:aws:dynamodb:*:*:table/SampleTable/stream/* "
        },
        {
            "Sid": "WriteLogStreamsAndGroups",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateLogGroup",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "*"
        }
    ]
}
```

Amazon RDS: 특정 리전에 있는 RDS 데이터베이스에 대한 완전한 액세스 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 RDS 데이터베이스에 대한 완전한 액세스를 허용합니다. 이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "rds:*",
            "Resource": ["arn:aws:rds:region:*:*"]
        },
        {
            "Effect": "Allow",
            "Action": ["rds:Describe*"],
            "Resource": ["*"]
        }
    ]
}
```

Amazon RDS: 프로그램 방식으로 콘솔에서 RDS 데이터베이스를 복원하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 RDS 데이터베이스 복원을 허용합니다. 이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "rds:CreateDBParameterGroup",
                "rds:CreateDBSnapshot",
                "rds:DeleteDBSnapshot",
                "rds:Describe*",
                "rds:DownloadDBLogFilePortion",
                "rds:List*",
                "rds:ModifyDBInstance",
                "rds:ModifyDBParameterGroup",
                "rds:ModifyOptionGroup",
                "rds:RebootDBInstance",
                "rds:RestoreDBInstanceFromDBSnapshot",
                "rds:RestoreDBInstanceToPointInTime"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon RDS: 태그 소유자가 자신이 태그를 지정한 RDS 리소스에 대한 모든 액세스 권한을 가지도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 태그 소유자가 자신이 태그를 지정한 RDS 리소스에 대한 모든 액세스 권한을 가지도록 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "rds:Describe*",
                "rds:List*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "rds:DeleteDBInstance",
                "rds:RebootDBInstance",
                "rds:ModifyDBInstance"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"rds:db-tag/Owner": "${aws:username}"}
            }
        },
        {
            "Action": [
                "rds:ModifyOptionGroup",
                "rds:DeleteOptionGroup"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"rds:og-tag/Owner": "${aws:username}"}
            }
        },
        {
            "Action": [
                "rds:ModifyDBParameterGroup",
                "rds:ResetDBParameterGroup"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"rds:pg-tag/Owner": "${aws:username}"}
            }
        },
        {
            "Action": [
                "rds:AuthorizeDBSecurityGroupIngress",
                "rds:RevokeDBSecurityGroupIngress",
                "rds:DeleteDBSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"rds:secgrp-tag/Owner": "${aws:username}"}
            }
```

```
        },
        {
            "Action": [
                "rds:DeleteDBSnapshot",
                "rds:RestoreDBInstanceFromDBSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"rds:snapshot-tag/Owner": "${aws:username}"}
            }
        },
        {
            "Action": [
                "rds:ModifyDBSubnetGroup",
                "rds:DeleteDBSubnetGroup"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"rds:subgrp-tag/Owner": "${aws:username}"}
            }
        },
        {
            "Action": [
                "rds:ModifyEventSubscription",
                "rds:AddSourceIdentifierToSubscription",
                "rds:RemoveSourceIdentifierFromSubscription",
                "rds:DeleteEventSubscription"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"rds:es-tag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Amazon S3: Amazon Cognito 사용자가 자신의 버킷에 있는 객체에 액세스할 수 있도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 Amazon Cognito 사용자가 특정 S3 버킷에 있는 객체에 액세스하도록 허용합니다. 이 정책은 ${cognito-identity.amazonaws.com:sub} 변수로 표현되는 cognito, 애플리케이션 이름 및 연동 사용자의 ID를 포함하는 이름을 통해 객체에 대한 액세스만을 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

> **Note**
>
> 객체 키에 사용된 '하위' 값은 사용자 풀의 사용자 하위 값이 아니라 자격 증명 풀의 사용자와 연결된 ID입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListYourObjects",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": ["arn:aws:s3:::bucket-name"],
            "Condition": {
                "StringLike": {
```

```
                    "s3:prefix": ["cognito/application-name/${cognito-
identity.amazonaws.com:sub}"]
                }
            }
        },
        {
            "Sid": "ReadWriteDeleteYourObjects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name/cognito/application-name/${cognito-
identity.amazonaws.com:sub}",
                "arn:aws:s3:::bucket-name/cognito/application-name/${cognito-
identity.amazonaws.com:sub}/*"
            ]
        }
    ]
}
```

Amazon Cognito는 웹 및 모바일 앱에 대한 인증, 권한 부여 및 사용자 관리를 제공합니다. 사용자는 사용자 이름과 암호를 사용하여 직접 로그인하거나 Facebook, Amazon, 또는 Google 같은 타사를 통해 로그인할 수 있습니다.

Amazon Cognito의 두 가지 주요 구성 요소는 사용자 풀과 자격 증명 풀입니다. 사용자 풀은 앱 사용자의 가입 및 로그인 옵션을 제공하는 사용자 디렉터리입니다. 자격 증명 풀을 통해 사용자에게 기타 AWS 서비스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자격 증명 풀과 사용자 풀을 별도로 또는 함께 사용할 수 있습니다.

Amazon Cognito에 대한 자세한 내용은 다음을 참조하십시오.

- Android용 AWS Mobile SDK Developer Guide의 Amazon Cognito 자격 증명
- AWS Mobile SDK for iOS Developer Guide의 Amazon Cognito 자격 증명

Amazon S3: 연합된 사용자가 프로그램 방식으로 콘솔에서 자신의 S3 홈 디렉터리에 액세스하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 연합된 사용자가 S3에 있는 자신의 홈 디렉터리 버킷 객체에 액세스하도록 허용합니다. 홈 디렉터리는 개별 연합된 사용자의 `home` 폴더를 포함하는 버킷입니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 정책의 `${aws:userid}` 변수가 `role-id:specified-name`로 변환됩니다. 연합된 사용자 ID의 `role-id` 부분은 생성 중에 연합된 사용자의 역할에 할당된 고유한 식별자입니다. 자세한 내용은 고유 식별자 (p. 567)를 참조하십시오. `specified-name`은 연합된 사용자가 자신의 역할을 맡을 때 `AssumeRoleWithWebIdentity` 요청에 전달된 RoleSessionName 파라미터입니다.

AWS CLI 명령 `aws iam get-role --role-name` *`specified-name`*.을 사용하여 역할 ID를 볼 수 있습니다. 예를 들어, 기억하기 쉬운 이름 `John`을 지정하고 CLI가 역할 ID `AROAXXT2NJT7D3SIQN7Z6`를 반환한다고 가정해 봅시다. 이 경우 연합된 사용자 ID는 `AROAXXT2NJT7D3SIQN7Z6:John`입니다. 그러면 이 정책에서 연합된 사용자 John이 접두사 `AROAXXT2NJT7D3SIQN7Z6:John`로 시작하는 Amazon S3 버킷에 액세스할 수 있도록 허용합니다.

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

```
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::bucket-name",
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "",
                        "home/",
                        "home/${aws:userid}/*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name/home/${aws:userid}",
                "arn:aws:s3:::bucket-name/home/${aws:userid}/*"
            ]
        }
    ]
}
```

Amazon S3: S3 버킷 액세스, 하지만 프로덕션 버킷은 최근 MFA 없이 거부

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서 Amazon S3 관리자가 객체 업데이트, 추가 및 삭제를 포함한 모든 버킷에 액세스하도록 허용합니다. 하지만 사용자가 지난 30분 내에 Multi-Factor Authentication(MFA) (p. 119)을 사용하여 로그인하지 않은 경우 `Production` 버킷에 대한 액세스가 명시적으로 거부됩니다. 이 정책은 콘솔에서 또는 프로그래밍 방식으로 AWS CLI 또는 AWS API를 사용하여 이 작업을 수행하는 데 필요한 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 정책은 장기 사용자 액세스 키를 사용한 `Production` 버킷에 대한 프로그래밍 방식 액세스를 허용하지 않습니다. 이 작업은 `NumericGreaterThanIfExists` 조건 연산자와 함께 `aws:MultiFactorAuthAge` 조건 키를 사용해 수행됩니다. 이 정책 조건은 MFA가 없거나 MFA 사용 기간이 30분 이상인 경우 `true`를 반환합니다. 이러한 상황에서는 액세스가 거부됩니다. 프로그래밍 방식으로 `Production` 버킷에 액세스하려면 S3 관리자는 GetSessionToken (p. 310) API 작업을 사용하여 지난 30분 동안 생성된 임시 자격 증명을 사용해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListAllS3Buckets",
            "Effect": "Allow",
            "Action": ["s3:ListAllMyBuckets"],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Sid": "AllowBucketLevelActions",
            "Effect": "Allow",
            "Action": [
```

```
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Sid": "AllowBucketObjectActions",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        },
        {
            "Sid": "RequireMFAForProductionBucket",
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::Production/*",
                "arn:aws:s3:::Production"
            ],
            "Condition": {
                "NumericGreaterThanIfExists": {"aws:MultiFactorAuthAge": "1800"}
            }
        }
    ]
}
```

Amazon S3: IAM 사용자가 프로그램 방식으로 콘솔에서 자신의 S3 홈 디렉터리에 액세스하도록 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 IAM 사용자가 S3에 있는 자신의 홈 디렉터리 버킷 객체에 액세스하도록 허용합니다. 홈 디렉터리는 개별 사용자의 home 폴더를 포함하는 버킷입니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::bucket-name",
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "",
                        "home/",
                        "home/${aws:username}/*"
                    ]
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name/home/${aws:username}",
                "arn:aws:s3:::bucket-name/home/${aws:username}/*"
            ]
        }
    ]
}
```

Amazon S3: 특정 S3 버킷으로 관리를 제한

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 특정 버킷에 대한 모든 S3 작업을 허용하지만 Amazon S3를 제외한 모든 AWS 서비스에 대한 액세스는 명시적으로 거부함으로써 S3 버킷의 관리를 제한합니다. 이 정책에서는 `s3:ListAllMyBuckets` 또는 `s3:GetObject`와 같이 S3 버킷에서 수행 불가능한 작업에 대한 액세스도 거부합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

이 정책을 이 정책에서 거부하는 작업을 허용하는 다른 정책(예: AmazonS3FullAccess 또는 AmazonEC2FullAccess AWS 관리형 정책)과 조합하여 사용하는 경우 액세스가 거부됩니다. 이는 명시적 거부문이 허용문보다 우선 적용되기 때문입니다. 자세한 내용은 the section called “계정 내에서 요청 허용 여부 결정” (p. 625) 단원을 참조하십시오.

> **Warning**
>
> `NotAction` (p. 595) 및 `NotResource` (p. 598)는 신중히 사용해야 하는 고급 정책 요소입니다. 이 정책에서는 Amazon S3를 제외한 모든 AWS 서비스에 대한 액세스를 거부합니다. 이 정책을 사용자에게 연결할 경우 다른 서비스에 대한 권한을 부여하는 다른 정책은 무시되거나 액세스가 거부됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        },
        {
            "Effect": "Deny",
            "NotAction": "s3:*",
            "NotResource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Amazon S3: S3 버킷에 있는 객체에 대한 읽기 및 쓰기 액세스 권한을 허용합니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 `Read` 및 `Write` 액세스 권한을 특정 S3 버킷에 있는 객체에 대해 허용합니다.이 정책은 AWS API 또는 AWS CLI를 사용해서만 이 작업

을 완료할 수 있는 권한을 부여합니다.이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

`s3:*Object` 작업에서는 와일드카드를 작업 이름의 일부로 사용합니다. `AllObjectActions` 문은 '객체' 단어로 끝나는 `GetObject`, `DeleteObject`, `PutObject` 및 기타 Amazon S3 작업을 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": ["arn:aws:s3:::bucket-name"]
        },
        {
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": ["arn:aws:s3:::bucket-name/*"]
        }
    ]
}
```

Note

Amazon S3 버킷에 있는 객체에 대한 `Read` 및 `Write` 액세스 권한을 허용하고 콘솔 액세스에 대한 추가 권한을 포함하려면 Amazon S3: S3 버킷에 있는 객체에 대한 읽기 및 쓰기 액세스 권한을 프로그래밍 방식으로 콘솔에서 허용 (p. 434) 단원을 참조하십시오.

Amazon S3: S3 버킷에 있는 객체에 대한 읽기 및 쓰기 액세스 권한을 프로그래밍 방식으로 콘솔에서 허용

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.에서는 `Read` 및 `Write` 액세스 권한을 특정 S3 버킷에 있는 객체에 대해 허용합니다. 이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다. 이 정책을 사용하려면 정책 예제의 *#### ## ### ###*를 본인의 정보로 대체하십시오.

`s3:*Object` 작업에서는 와일드카드를 작업 이름의 일부로 사용합니다. `AllObjectActions` 문은 '객체' 단어로 끝나는 `GetObject`, `DeleteObject`, `PutObject` 및 기타 Amazon S3 작업을 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": ["arn:aws:s3:::bucket-name"]
```

```
        },
        {
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": ["arn:aws:s3:::bucket-name/*"]
        }
    ]
}
```

IAM 정책 관리

IAM은 모든 유형의 IAM 정책(관리형 정책 및 인라인 정책)을 생성하고 관리하는 도구를 제공합니다. 권한을 IAM 자격 증명(IAM 사용자, 그룹 또는 역할)에 추가하려면 정책을 생성한 다음 자격 증명에 추가하면 됩니다. 다수의 정책을 자격 증명 하나에 연결하거나, 정책마다 다수의 권한이 포함될 수 있습니다.

자세한 내용은 다음 리소스를 참조하십시오.

- 다른 유형의 IAM 정책에 대한 자세한 내용은 정책 및 권한 (p. 349) 단원을 참조하십시오.
- IAM 내에서 정책 사용에 대한 일반적인 내용은 액세스 관리 (p. 348) 단원을 참조하십시오.
- 다수의 정책이 임의의 IAM 자격 증명 하나에게 적용되는 경우 권한 평가 방법에 대한 자세한 내용은 정책 평가 로직 (p. 622) 단원을 참조하십시오.
- 정책 크기 및 이름 지정 제한에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

주제

IAM 정책 만들기

정책 (p. 349)은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 개체입니다. AWS Management 콘솔, AWS CLI 또는 AWS API를 사용하여 IAM에서 고객 관리형 정책을 생성할 수 있습니다. 고객 관리형 정책은 자체 AWS 계정에서 관리하는 독립형 정책입니다. 그런 다음 정책을 AWS 계정의 자격 증명(사용자, 그룹 또는 역할)에 연결합니다.

IAM에서 자격 증명에 연결되는 정책을 자격 증명 기반 정책이라고 합니다. 자격 증명 기반 정책에는 AWS 관리형 정책, 고객 관리형 정책 및 인라인 정책이 포함될 수 있습니다. AWS 관리형 정책은 AWS에 의해 생성 및 관리됩니다. 사용자는 이러한 정책을 사용할 수 있지만 관리할 수 없습니다. 인라인 정책은 사용자가 생성한 정책으로 IAM 그룹, 사용자 또는 역할에 직접 삽입할 수 있습니다. 인라인 정책은 다른 자격 증명에서 재사용하거나 해당 자격 증명 외부에서 관리할 수 없습니다. 자세한 내용은 IAM 자격 증명 권한 추가 및 제거 (p. 450) 단원을 참조하십시오.

인라인 정책보다는 고객 관리형 정책을 사용 (p. 62)하는 것이 좋습니다. 또한 AWS 관리형 정책 대신 고객 관리형 정책을 사용하는 것이 가장 좋습니다. AWS 관리형 정책은 일반적으로 광범위한 관리 또는 읽기 전용 권한을 제공합니다. 보안을 극대화하려면 최소 권한을 부여합니다 (p. 61). 즉, 특정 작업을 수행하는 데 필요한 권한만 부여합니다.

AWS Management 콘솔, AWS CLI 또는 AWS API를 사용하여 IAM에서 고객 관리형 정책을 생성할 수 있습니다.

IAM 정책 만들기(콘솔)

정책 (p. 349)은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 개체입니다. AWS Management 콘솔을 사용하여 IAM에서 고객 관리형 정책을 생성할 수 있습니다. 고객 관리형 정책은 자체 AWS 계정에서 관리하는 독립형 정책입니다. 그런 다음 정책을 AWS 계정의 자격 증명(사용자, 그룹 또는 역할)에 연결합니다.

주제

IAM 정책 만들기(콘솔)

다음 방법 중 하나를 사용하여 AWS Management 콘솔에서 고객 관리형 정책을 생성할 수 있습니다.

- JSON (p. 436) — 게시된 예제 자격 증명 기반 정책 (p. 387)을 붙여넣고 사용자 지정합니다.
- 시각적 편집기 (p. 437) — 시각적 편집기에서 정책을 새로 생성합니다. 시각적 편집기를 사용할 경우 JSON 구문을 이해할 필요가 없습니다.
- 가져오기 (p. 438) — 계정 내에서 관리형 정책을 가져오고 사용자 지정합니다. 이전에 생성한 AWS 관리형 정책 또는 고객 관리형 정책을 가져올 수 있습니다.

정책 크기 제한 및 기타 할당량에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

JSON 탭에서 정책 만들기

JSON 탭을 선택하여 JSON에 정책을 입력하거나 붙여 넣을 수 있습니다. 이 방법은 계정에서 사용하기 위해 예제 정책 (p. 387)을 복사할 경우 유용합니다. 또는 JSON 편집기에 고유한 JSON 정책 문서를 입력할 수 있습니다. JSON 탭을 통해 시각적 편집기와 JSON 간에 전환하여 보기를 비교할 수도 있습니다.

JSON 정책 (p. 349) 문서는 하나 이상의 문으로 구성되어 있습니다. 각 문에는 동일한 효과(`Allow` 또는 `Deny`)를 공유하며 동일한 리소스와 조건을 지원하는 모든 작업이 포함되어야 합니다. 한 작업에서 모든 리소스를 지정(`"*"`)하도록 요구하고 다른 작업에서 특정 리소스의 Amazon 리소스 이름(ARN)을 지원하는 경우 이들은 두 개의 별개 JSON 문에 있어야 합니다. ARN 형식에 대한 자세한 내용은AWS General Reference 안내서의 Amazon 리소스 이름(ARN)을 참조하십시오. IAM 정책에 대한 일반적인 내용은 정책 및 권한 (p. 349) 단원을 참조하십시오. IAM 정책 언어에 대한 자세한 정보는 IAM JSON 정책 참조 (p. 586) 섹션을 참조하십시오.

JSON 정책 편집기를 사용하여 정책을 생성하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.
3. [Create policy]를 선택합니다.
4. [JSON] 탭을 선택합니다.
5. JSON 정책 문서를 입력하거나 붙여 넣습니다. IAM 정책 언어에 대한 자세한 정보는 IAM JSON 정책 참조 (p. 586) 섹션을 참조하십시오.
6. 작업이 완료되면 [Review policy]를 선택합니다. 정책 검사기 (p. 441)가 모든 구문 오류를 보고합니다.

Note

언제든지 Visual editor(시각적 편집기) 탭과 JSON 탭 간을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 정보는 정책 재구성 (p. 538) 단원을 참조하십시오.

7. 정책 검토 페이지에서 생성하는 정책에 대한 이름과 설명(선택 사항)을 입력합니다. 정책 요약을 검토하여 정책이 부여한 권한을 확인합니다. 그런 다음 [Create policy]를 선택하여 작업을 저장합니다.

정책을 생성한 후 그룹, 사용자 또는 역할에 연결할 수 있습니다. 자세한 정보는 IAM 자격 증명 권한 추가 및 제거 (p. 450) 단원을 참조하십시오.

시각적 편집기를 사용하여 정책 만들기

IAM 콘솔의 시각적 편집기는 JSON 구문을 작성하지 않고 정책을 생성하는 방법을 안내합니다. 시각적 편집기를 사용하여 정책을 생성하는 예제를 보려면 the section called “자격 증명에 대한 액세스 제어” (p. 376) 단원을 참조하십시오.

시각적 편집기를 사용하여 정책을 생성하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.
3. [Create policy]를 선택합니다.
4. Visual editor(시각적 편집기) 탭에서 Choose a service(서비스 선택)을 선택합니다. 그런 다음 정책에 추가할 AWS 제품을 선택합니다. 상단의 검색 상자를 사용하여 서비스 목록 결과를 제한할 수 있습니다. 시각적 편집기 권한 블록 내에서 하나의 서비스만 선택할 수 있습니다. 둘 이상의 서비스에 액세스 권한을 부여하려면 Add additional permissions(권한 추가)를 선택하여 여러 개의 권한 블록을 추가합니다.
5. Select actions(작업 선택)을 선택한 다음 정책에 추가할 작업을 선택합니다. 시각적 편집기에는 이전 단계에서 선택한 서비스에서 사용 가능한 작업이 표시됩니다.

   작업을 선택하는 방법은 다음과 같습니다.

   - 확인란을 사용하여 서비스에 대한 모든 작업을 선택하거나 사전 정의된 액세스 레벨 중 하나에서 모든 작업을 선택합니다.
   - 각 액세스 레벨 그룹을 확장하여 개별 작업을 선택합니다.
   - add actions(작업 추가)를 선택하여 특정 작업을 입력하거나 와일드카드(*)를 사용하여 여러 개의 작업을 지정합니다.

   기본적으로 생성되는 정책은 사용자가 선택하는 작업을 허용합니다. 대신 선택한 작업을 거부하려면 Switch to deny permissions(권한 거부로 전환)을 선택합니다. 기본적으로 IAM은 거부 (p. 622)하기 때문에, 보안 모범 사례로 사용자에게 필요한 작업과 리소스에만 권한을 허용하는 것이 좋습니다. 이것을 "화이트리스트"라고 부르기도 합니다. 다른 문이나 정책에서 허용되는 권한을 별도로 재정의하려는 경우에만 권한을 거부("블랙리스트")하기 위한 JSON 문을 생성해야 합니다. 권한 거부의 수가 늘어나면 권한 문제를 해결하기가 더 어려워질 수 있기 때문에 그 수를 최소한으로 제한하는 것이 좋습니다.
6. 이전 단계에서 선택한 서비스 및 작업이 특정 리소스 (p. 381) 선택을 지원하지 않는 경우 모든 리소스가 선택됩니다. 이러한 경우 이 섹션을 편집할 수 없습니다.

   리소스 수준 권한 (p. 381)을 지원하는 작업을 하나 이상 선택하면 시각적 편집기에 해당 리소스가 나열됩니다. 그러면 리소스를 선택하여 정책에 대한 리소스를 지정할 수 있습니다.

   리소스를 선택하는 방법은 다음과 같습니다.

   - Add ARN(ARN 추가)를 선택하여 리소스에 대한 세부 정보를 제공합니다. 값을 입력하는 대신 모두 선택을 선택하여 지정된 설정을 위한 값에 대한 권한을 제공할 수도 있습니다. 예를 들어, Amazon EC2

읽기 액세스 레벨 그룹을 선택하면 정책의 작업이 `instance` 리소스 유형을 지원합니다. 리소스에 대해 Region, Account 및 InstanceId 값을 제공해야 합니다. 계정 ID를 제공하지만 리전 및 인스턴스 ID에 대해 모두 선택을 선택한 경우 정책은 계정의 모든 인스턴스에 대해 권한을 부여합니다.

- Add ARN(ARN 추가)를 선택하여 Amazon 리소스 이름(ARN)별로 리소스를 지정합니다. ARN 필드에 와일드카드(*)를 사용할 수 있습니다(각 콜론 쌍 사이). ARN 형식에 대한 자세한 내용은AWS General Reference 안내서의 Amazon 리소스 이름(ARN)을 참조하십시오. 정책의 `Resource` 요소에 ARN을 사용하는 방법에 대한 자세한 내용은 IAM JSON 정책 요소: Resource (p. 597) 단원을 참조하십시오.
- 리소스 섹션의 오른쪽 맨 끝에서 모두 선택을 선택하여 특정 유형의 리소스에 대한 권한을 부여합니다.
- All resources(모든 리소스)를 선택하여 해당 서비스에 대한 모든 리소스를 선택합니다.

7. (선택 사항) Specify request conditions(optional)(요청 조건 지정(선택 사항))를 선택하여 생성하는 정책에 조건을 추가합니다. 조건은 JSON 정책 문의 효과를 제한합니다. 예를 들어 특정 시간 범위 내에 사용자의 요청이 발생하는 경우에만 사용자가 리소스에 대한 작업을 수행할 수 있도록 지정할 수 있습니다. 또한 일반적으로 사용되는 조건을 사용하여 사용자가 멀티 팩터 인증(MFA) 디바이스를 사용하여 인증받아야 하는지를 제한할 수 있습니다. 또는 요청이 특정 IP 주소 범위에서 발생하도록 요구할 수 있습니다. 정책 조건에서 사용할 수 있는 모든 콘텍스트 키 목록은 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

   조건을 선택하는 방법은 다음과 같습니다.

   - 확인란을 사용하여 일반적으로 사용되는 조건을 선택합니다.
   - 조건 추가를 선택하여 다른 조건을 지정합니다. 조건의 조건 키, 한정어, 연산자를 선택한 후 값을 입력합니다. 값을 두 개 이상 추가하려면 Add new value(새 값 추가)를 선택합니다. 해당 값이 논리적 "OR" 연산자로 연결되는 것으로 생각할 수 있습니다. 작업이 완료되면 추가를 선택합니다.

   조건을 두 개 이상 추가하려면 다시 조건 추가를 선택합니다. 필요에 따라 반복합니다. 각 조건은 이 시각적 편집기 권한 블록 하나에만 적용됩니다. 권한 블록이 일치하는 것으로 간주되려면 모든 조건이 true여야 합니다. 즉, 이들 조건이 논리적 "AND" 연산자로 연결되는 것으로 간주됩니다.

   조건 요소에 대한 자세한 정보는 IAM JSON 정책 참조 (p. 586)에서 IAM JSON 정책 요소: Condition (p. 598) 섹션을 참조하십시오.
8. 더 많은 권한 블록을 추가하려면 Add additional permissions(권한 추가)를 선택합니다. 각 블록에 대해 2~5단계를 반복합니다.
9. 작업이 완료되면 [Review policy]를 선택합니다.

   Note

   언제든지 Visual editor(시각적 편집기) 탭과 JSON 탭 간을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 정보는 정책 재구성 (p. 538) 단원을 참조하십시오.
10. 정책 검토 페이지에서 생성하는 정책에 대한 이름과 설명(선택 사항)을 입력합니다. 정책 요약을 검토하여 의도한 권한이 부여되었는지 확인한 다음 정책 생성을 선택하여 새 정책을 저장합니다.

정책을 생성한 후 그룹, 사용자 또는 역할에 연결할 수 있습니다. 자세한 내용은 IAM 자격 증명 권한 추가 및 제거 (p. 450) 단원을 참조하십시오.

기존 관리형 정책 가져오기

새 정책을 생성하는 쉬운 방법은 최소한으로 필요한 권한 중 일부가 이미 존재하는 계정으로 기존 관리형 정책을 가져오는 것입니다. 그런 다음, 새로운 요구 사항에 일치하도록 정책을 사용자 지정할 수 있습니다.

인라인 정책은 가져올 수 없습니다. 관리형 정책과 인라인 정책의 차이에 대해 자세히 알아보려면 관리형 정책과 인라인 정책 (p. 357) 단원을 참조하십시오.

시각적 편집기에서 기존 관리형 정책을 가져오려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.
3. [Create policy]를 선택합니다.
4. Visual editor(시각적 편집기) 탭을 선택한 다음 페이지 오른쪽에서 Import managed policy(관리형 정책 가져오기)를 선택합니다.
5. Import managed policies(관리형 정책 가져오기) 창에서 새 정책에 포함할 정책과 가장 근접한 관리형 정책을 선택합니다. 필터 메뉴를 사용하거나 상단의 검색 상자에 입력하여 정책 목록의 결과를 제한할 수 있습니다.
6. [Import]를 선택합니다.

   가져온 정책은 정책 하단의 새 권한 블록에 추가됩니다.
7. Visual editor(시각적 편집기)를 사용하거나 JSON을 선택하여 정책을 사용자 지정합니다. 그런 다음 정책 검토를 선택합니다.

   Note

   언제든지 Visual editor(시각적 편집기) 탭과 JSON 탭 간을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 정보는 정책 재구성 (p. 538) 단원을 참조하십시오.
8. 검토 페이지에서 생성하는 정책에 대한 이름과 설명(선택 사항)을 입력합니다. 이러한 설정은 나중에 편집할 수 없습니다. 정책 요약을 검토한 다음 정책 생성을 선택하여 작업을 저장합니다.

JSON 탭에서 기존 관리형 정책을 가져오려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.
3. [Create policy]를 선택합니다.
4. JSON 탭을 선택한 다음 페이지 오른쪽에서 Import managed policy(관리형 정책 가져오기)를 선택합니다.
5. Import managed policies(관리형 정책 가져오기) 창에서 새 정책에 포함할 정책과 가장 근접한 관리형 정책을 선택합니다. 필터 메뉴를 사용하거나 상단의 검색 상자에 입력하여 정책 목록의 결과를 제한할 수 있습니다.
6. [Import]를 선택합니다.

   가져온 정책의 문은 JSON 정책 하단에 추가됩니다.
7. 정책을 JSON으로 사용자 지정하거나 Visual editor(시각적 편집기)를 선택합니다. 그런 다음 정책 검토를 선택합니다.

   Note

   언제든지 Visual editor(시각적 편집기) 탭과 JSON 탭 간을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 정보는 정책 재구성 (p. 538) 단원을 참조하십시오.
8. 정책 검토 페이지에서 생성하는 정책에 대한 이름과 설명(선택 사항)을 입력합니다. 이러한 필드는 나중에 편집할 수 없습니다. 정책 요약을 검토한 다음 정책 생성을 선택하여 작업을 저장합니다.

정책을 생성한 후 그룹, 사용자 또는 역할에 연결할 수 있습니다. 자세한 내용은 IAM 자격 증명 권한 추가 및 제거 (p. 450) 단원을 참조하십시오.

IAM 정책 생성(AWS CLI)

정책 (p. 349)은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 개체입니다. AWS CLI을 사용하여 IAM에서 고객 관리형 정책을 생성할 수 있습니다. 고객 관리형 정책은 자체 AWS 계정에서 관리하는 독립형 정책입니다. 그런 다음 정책을 AWS 계정의 자격 증명(사용자, 그룹 또는 역할)에 연결합니다.

정책 크기 제한 및 기타 할당량에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

IAM 정책 생성(AWS CLI)

AWS Command Line Interface(AWS CLI)를 사용하여 IAM 고객 관리형 정책 또는 인라인 정책을 생성할 수 있습니다.

고객 관리형 정책을 만들려면(AWS CLI)

다음 명령을 사용합니다.

- create-policy

IAM 자격 증명(그룹, 사용자 또는 역할)에 대한 인라인 정책을 만들려면(AWS CLI)

다음 명령 중 하나를 사용합니다.

- put-group-policy
- put-role-policy
- put-user-policy

> **Note**
>
> IAM을 사용하여 service-linked role (p. 175)에 인라인 정책을 포함시킬 수 없습니다.

IAM 정책 생성(AWS API)

정책 (p. 349)은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 개체입니다. AWS API를 사용하여 IAM에서 고객 관리형 정책을 생성할 수 있습니다. 고객 관리형 정책은 자체 AWS 계정에서 관리하는 독립형 정책입니다. 그런 다음 정책을 AWS 계정의 자격 증명(사용자, 그룹 또는 역할)에 연결합니다.

정책 크기 제한 및 기타 할당량에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

IAM 정책 생성(AWS API)

AWS API를 사용하여 IAM 고객 관리형 정책 또는 인라인 정책을 생성할 수 있습니다.

고객 관리형 정책을 만들려면(AWS API)

다음 작업을 호출합니다.

- CreatePolicy

IAM 자격 증명(그룹, 사용자 또는 역할)에 대한 인라인 정책을 만들려면(AWS API)

다음 작업 중 하나를 호출합니다.

- PutGroupPolicy
- PutRolePolicy

- PutUserPolicy

  Note

  IAM을 사용하여 service-linked role (p. 175)에 인라인 정책을 포함시킬 수 없습니다.

JSON 정책 검증

정책 검사기는 신규 및 기존 IAM 액세스 제어 정책을 자동으로 검사하여 IAM 정책 문법의 준수 여부를 확인합니다. 여기에서 정책이란 IAM 정책 문법에 따라 작성된 JSON 문서를 말합니다. 정책을 연결할 AWS 사용자, 그룹 또는 역할의 액세스 권한을 정의합니다. 정책 검사기에서 정책 문법을 준수하지 않은 정책을 발견하면 해당 정책을 수정하라는 메시지가 표시됩니다. 정책이 문법을 준수하지 않는 경우에는 정책 검사기만 사용할 수 있습니다.

다음 방법을 사용하여 정책 검사기에 액세스할 수도 있습니다.

1. JSON 정책 생성 – 정책 검토를 선택하면 새 JSON 정책을 생성할 때 정책 검사기가 자동으로 실행됩니다. 정책이 유효하지 않으면 알림이 표시되고 계속 진행하기 전에 문제를 해결해야 합니다.
2. JSON 정책 편집 – 정책 검토를 선택하면 기존 JSON 정책을 편집할 때 정책 검사기가 자동으로 실행됩니다. 정책이 유효하지 않으면 알림이 표시되고 계속 진행하기 전에 문제를 해결해야 합니다. 정책 검사기를 도입하기 전에 설정된 기존 정책에 오류가 있어도 그대로 실행됩니다. 그러나 정책 구문 오류를 수정하지 않으면 해당 정책을 편집 및 저장할 수 없습니다.

   Note

   정책 검사기는 JSON 정책 구문 및 문법만 검사합니다. ARN, 작업 이름 또는 조건 키가 올바른지는 검사하지 않습니다.

IAM 정책 시뮬레이터로 IAM 정책 테스트하기

IAM 정책의 사용 방식과 이유에 대한 자세한 정보는 정책 및 권한 (p. 349) 단원을 참조하십시오.

다음 위치에서 IAM 정책 시뮬레이터 콘솔에 액세스할 수 있습니다. https://policysim.aws.amazon.com/

IAM 정책 시뮬레이터 시작하기

IAM 정책 시뮬레이터를 사용하면 자격 증명 기반 정책, IAM 권한 경계, 조직 서비스 제어 정책 및 리소스 기반 정책을 테스트하고 문제를 해결할 수 있습니다. 다음은 정책 시뮬레이터로 수행할 수 있는 몇 가지 일반적인 사항입니다.

- AWS 계정의 IAM 사용자, 그룹 또는 역할에 연결된 정책을 테스트합니다. 사용자, 그룹 또는 역할에 추가된 정책이 다수일 때는 모든 정책을 테스트하거나, 테스트할 정책만 따로 선택할 수 있습니다. 특정 리소스에 대해 선택한 정책에서 어떤 작업을 허용하거나 거부하는지 테스트할 수 있습니다.
- IAM 엔터티에 대한 권한 경계 (p. 363)의 효과를 테스트하고 문제를 해결합니다. 참고: 한 번에 하나의 권한 경계만 시뮬레이션할 수 있습니다.
- Amazon S3 버킷, Amazon SQS 대기열, Amazon SNS 주제, Amazon S3 Glacier 볼트 등과 같은 AWS 리소스에 연결된 정책을 테스트합니다.
- AWS 계정이 AWS Organizations의 조직에 속한 경우, 서비스 제어 정책(SCP)이 IAM 정책 및 리소스 정책에 미치는 영향을 테스트할 수 있습니다.
- 사용자, 그룹 또는 역할에 아직 추가되지 않은 새로운 정책을 시뮬레이터에 입력 또는 복사하여 테스트합니다. 이는 시뮬레이션에서만 사용되며 저장되지 않습니다. 참고: 리소스 기반 정책을 시뮬레이터에 입력하거나 복사하지 마십시오. 시뮬레이터에서 리소스 기반 정책을 사용하려면 시뮬레이션에 리소스를 포함해야 합니다. 또한 해당 리소스의 정책을 시뮬레이션에 포함하려면 확인란을 선택해야 합니다.

- 선택한 서비스, 작업 및 리소스에 대한 정책을 테스트합니다. 예를 들어 정책이 특정 버킷의 Amazon S3 서비스에서 주체가 `ListAllMyBuckets`, `CreateBucket` 및 `DeleteBucket` 작업을 수행할 수 있도록 허용하는지 확인하기 위해 테스트할 수 있습니다.
- 테스트할 정책에서 키가 지정되어 있는 경우에는 테스트할 정책의 `Condition` 요소에 포함된 IP 주소나 날짜 같은 콘텍스트 키를 제공하여 실제 시나리오를 시뮬레이션합니다.
- 어떤 정책 문이 특정 리소스 또는 작업에 대한 액세스를 허용하거나 거부하는지 식별합니다.

주제

IAM 정책 시뮬레이터의 원리

시뮬레이터는 선택한 정책을 평가한 후 지정 작업 각각에 대해 유효한 권한을 결정합니다. 정책 평가 엔진으로는 실제로 AWS 서비스를 요청할 때와 동일한 엔진을 사용하지만 다음과 같은 방식에서 실시간 AWS 환경과는 차이가 있습니다.

- 시뮬레이터는 실제로 AWS 서비스를 요청하는 것은 아니기 때문에 실행 중인 AWS 환경을 변경하지 않고 요청을 안전하게 테스트할 수 있습니다.
- 시뮬레이터는 선택한 작업 중 실행 중인 작업은 시뮬레이션하지 않기 때문에 시뮬레이션된 요청에 대한 응답을 보고하지 않습니다. 요청된 작업이 허용되는지 아니면 거부되는지 여부만 결과로 반환됩니다.
- 시뮬레이터에서 정책을 편집할 경우 이러한 변경은 시뮬레이터에만 영향을 줍니다. AWS 계정의 해당 정책은 변함없이 그대로 유지됩니다.

IAM 정책 시뮬레이터를 사용하는 데 필요한 권한

정책 시뮬레이터 콘솔 또는 정책 시뮬레이터 API를 사용하여 정책을 테스트할 수 있습니다. 기본적으로 콘솔 사용자는 사용자, 그룹 또는 역할에 아직 연결되지 않은 정책을 시뮬레이터에 입력하거나 복사하여 테스트할 수 있습니다. 이러한 정책은 시뮬레이션에만 사용되며 민감한 정보를 공개하지 않습니다. API 사용자가 연결되지 않은 정책을 테스트하려면 권한이 있어야 합니다. 콘솔 또는 API 사용자가 AWS 계정의 IAM 사용자, 그룹 또는 역할에 연결된 정책을 테스트하도록 허용할 수 있습니다. 이렇게 하려면 해당 정책을 검색할 수 있는 권한을 제공해야 합니다. 리소스 기반 정책을 테스트하려면 사용자가 리소스의 정책을 검색할 수 있는 권한을 보유해야 합니다.

사용자가 시뮬레이션할 수 있는 콘솔 및 API 정책의 예시는 the section called “정책 예제: AWS Identity and Access Management(IAM)” (p. 388) 단원을 참조하십시오.

정책 시뮬레이터 콘솔을 사용하는 데 필요한 권한

사용자가 AWS 계정의 IAM 사용자, 그룹 또는 역할에 연결된 정책을 테스트하도록 허용할 수 있습니다. 이렇게 하려면 사용자에게 해당 정책을 검색할 수 있는 권한을 제공해야 합니다. 리소스 기반 정책을 테스트하려면 사용자가 리소스의 정책을 검색할 수 있는 권한을 보유해야 합니다.

사용자, 그룹 또는 역할에 연결된 정책에 대해 정책 시뮬레이터 콘솔의 사용을 허용하는 정책의 예시는 IAM: 정책 시뮬레이터 콘솔 액세스 (p. 412) 단원을 참조하십시오.

특정 경로를 지닌 사용자에 대해서만 정책 시뮬레이터 콘솔의 사용을 허용하는 정책의 예시는 IAM: 사용자 경로를 바탕으로 정책 시뮬레이터 콘솔 액세스 (p. 422) 단원을 참조하십시오.

한 가지 유형의 엔터티에 대해서만 정책 시뮬레이터 콘솔의 사용을 허용하는 정책을 만들려면 다음의 절차에 따릅니다.

콘솔 사용자가 사용자를 위한 정책을 시뮬레이션하도록 허용하는 방법

정책에 다음의 작업을 포함시킵니다.

- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAttachedUserPolicies
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:ListUserPolicies
- iam:ListUsers

콘솔 사용자가 그룹을 위한 정책을 시뮬레이션하도록 허용하는 방법

정책에 다음의 작업을 포함시킵니다.

- iam:GetGroup
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:ListAttachedGroupPolicies
- iam:ListGroupPolicies
- iam:ListGroups

콘솔 사용자가 역할에 대한 정책을 시뮬레이션하도록 허용하는 방법

정책에 다음의 작업을 포함시킵니다.

- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRole
- iam:GetRolePolicy
- iam:ListAttachedRolePolicies
- iam:ListRolePolicies
- iam:ListRoles

리소스 기반 정책을 테스트하려면 사용자가 리소스의 정책을 검색할 수 있는 권한을 보유해야 합니다.

콘솔 사용자가 Amazon S3 버킷에서 리소스 기반 정책을 테스트하도록 허용하는 방법

정책에 다음의 작업을 포함시킵니다.

- s3:GetBucketPolicy

예를 들어, 다음 정책에서 이 작업을 사용하여 특정 Amazon S3 버킷에서 콘솔 사용자가 리소스 기반 정책을 시뮬레이션하도록 허용합니다.

```
{
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "s3:GetBucketPolicy",
            "Resource":"arn:aws:s3:::bucket-name/*"
          }
        ]
      }
```

콘솔 사용자가 AWS Organizations를 위한 정책을 테스트하도록 허용하는 방법

정책에 다음의 작업을 포함시킵니다.

- `organizations:DescribePolicy`
- `organizations:ListPolicies`
- `organizations:ListPoliciesForTarget`
- `organizations:ListTargetsForPolicy`

API 정책 시뮬레이터를 사용하는 데 필요한 권한

정책 시뮬레이터 API 작업 GetContextKeyForCustomPolicy 및 SimulateCustomPolicy는 아직 사용자, 그룹 또는 역할에 연결되지 않은 정책을 테스트하도록 허용합니다. 이러한 정책을 테스트하려면 정책을 문자열로 API에 전달합니다. 이러한 정책은 시뮬레이션에만 사용되며 민감한 정보를 공개하지 않습니다. API를 사용하여 AWS 계정의 IAM 사용자, 그룹 또는 역할에 연결된 정책을 테스트할 수도 있습니다. 이렇게 하려면 사용자에게 GetContextKeyForPrincipalPolicy 및 SimulatePrincipalPolicy를 호출할 수 있는 권한을 제공해야 합니다.

현재 AWS 계정에 연결된 정책 및 연결되지 않은 정책에 대해 정책 시뮬레이터 API를 사용하도록 허용하는 예제 정책을 보려면 IAM: 정책 시뮬레이터 API에 액세스 (p. 411) 단원을 참조하십시오.

한 가지 유형의 정책에 대해서만 정책 시뮬레이터 API의 사용을 허용하는 정책을 만들려면 다음의 절차에 따릅니다.

API 사용자가 API에 문자열로 직접 전달되는 정책을 시뮬레이션하도록 허용하는 방법

정책에 다음의 작업을 포함시킵니다.

- `iam:GetContextKeysForCustomPolicy`
- `iam:SimulateCustomPolicy`

API 사용자로 하여금 IAM 사용자, 그룹 또는 역할에 연결된 정책을 시뮬레이션하도록 하는 방법

정책에 다음의 작업을 포함시킵니다.

- `iam:GetContextKeysForPrincipalPolicy`
- `iam:SimulatePrincipalPolicy`

예를 들어, Alice라는 사용자에게 할당된 정책을 시뮬레이션할 수 있는 권한을 Bob이라는 사용자에게 부여하려면, Bob에게 `arn:aws:iam::777788889999:user/alice`라는 리소스에 액세스할 수 있는 권한을 부여해야 합니다.

특정 경로를 지닌 사용자에 대해서만 정책 시뮬레이터 API의 사용을 허용하는 정책의 예시는 IAM: 사용자 경로를 바탕으로 정책 시뮬레이터 API 액세스 (p. 422) 단원을 참조하십시오.

IAM 정책 시뮬레이터 사용(콘솔)

기본적으로 사용자는 사용자, 그룹 또는 역할에 아직 연결되지 않은 정책을 정책 시뮬레이터 콘솔에 입력하거나 복사하여 테스트할 수 있습니다. 이러한 정책은 시뮬레이션에만 사용되며 민감한 정보를 공개하지 않습니다.

사용자, 그룹 또는 역할에 연결되지 않은 정책을 테스트하려면(콘솔)

1. https://policysim.aws.amazon.com/에서 IAM 정책 시뮬레이터 콘솔을 엽니다.
2. 페이지의 상단에 있는 Mode:(모드:) 메뉴에서 New Policy(새 정책)을 선택합니다.
3. Policy Sandbox(정책 샌드박스)에서 새 정책 생성을 선택합니다.
4. 시뮬레이터에 입력하거나 복사하여 붙여 넣고, 다음 단계의 설명에 따라 시뮬레이터를 사용합니다.

IAM 정책 시뮬레이터 콘솔을 사용할 권한이 있으면 시뮬레이터를 사용하여 IAM 사용자, 그룹, 역할 또는 리소스 정책을 테스트할 수 있습니다.

사용자, 그룹 또는 역할에 연결된 정책을 테스트하려면(콘솔)

1. https://policysim.aws.amazon.com/에서 IAM 정책 시뮬레이터 콘솔을 엽니다.

   Note

   IAM 사용자로 정책 시뮬레이터에 로그인하려면 고유의 로그인 URL을 사용하여 AWS Management 콘솔에 로그인합니다. 그런 다음 https://policysim.aws.amazon.com/으로 이동합니다. IAM 사용자 권한의 로그인에 대한 자세한 정보는 IAM 사용자가 AWS에 로그인하는 방법 (p. 91)를 참조하십시오.

   시뮬레이터가 Existing Policies(기존 정책) 모드로 열리며 Users, Groups, and Roles(사용자, 그룹 및 역할) 아래 계정에 속한 IAM 사용자가 표시됩니다.
2. 작업에 적합한 옵션을 선택합니다.

테스트 대상	수행할 작업:
사용자에게 연결된 정책	Users, Groups, and Roles(사용자, 그룹 및 역할) 목록에서 사용자를 선택합니다. 그런 다음 사용자를 선택합니다.
그룹에 연결된 정책	Users, Groups, and Roles(사용자, 그룹 및 역할) 목록에서 그룹을 선택합니다. 그런 다음 그룹을 선택합니다.
역할에 연결된 정책	Users, Groups, and Roles(사용자, 그룹 및 역할) 목록에서 역할을 선택합니다. 그런 다음 역할을 선택합니다.
리소스에 연결된 정책	Step 9 단원을 참조하십시오.
사용자, 그룹 또는 역할에 대한 사용자 지정 정책	새 정책 생성을 선택합니다. 새 정책 창에 정책을 입력하거나 붙여넣은 후 적용을 선택합니다.

도움말

그룹에 연결된 정책을 테스트하려면 IAM 정책 시뮬레이터를 IAM 콘솔에서 직접 실행한 후 탐색 창에서 그룹을 선택합니다. 정책을 테스트하려는 그룹 이름을 선택한 후 권한 탭을 선택합니다. Inline Policies(인라인 정책) 또는 Managed Policies(관리형 정책) 섹션에서 테스트하려는 정책을 찾습니다. 해당 정책의 작업 열에서 Simulate Policy(정책 시뮬레이션)을 선택합니다. 사용자에게 연결된 고객 관리형 정책을 테스트하려면 탐색 창에서 사용자를 선택합니다. 정책을 테스트하고자 하는 사용자의 이름을 선택합니다. 그런 다음 권한 탭을 선택하고 테스트할 정

책을 확장합니다. 오른쪽 맨 끝에서 Simulate Policy(정책 시뮬레이션)를 선택합니다. IAM 정책 시뮬레이터가 새 창으로 열리면서 선택한 정책을 정책 창에 표시합니다.

3. (선택 사항) 계정이 AWS Organizations의 조직에 속한 경우, 시뮬레이션된 사용자의 계정에 영향을 미치는 서비스 제어 정책(SCP)이 정책 창에 표시됩니다. 정책 창에는 IAM 정책, 리소스 정책 및 권한 경계 정책도 표시됩니다. SCP는 조직 또는 조직 단위(OU)에 최대 권한을 지정하는 JSON 정책입니다. SCP는 멤버 계정의 엔터티에 대한 권한을 제한합니다. SCP가 서비스 또는 작업을 차단하는 경우 해당 계정에 있는 어떤 엔터티도 해당 서비스에 액세스하거나 해당 작업을 수행할 수 없습니다. 이는 관리자가 IAM 또는 리소스 정책을 통해 해당 서비스 또는 작업에 명시적으로 권한을 부여하는 경우에도 해당합니다. 시뮬레이션에서 SCP를 제거하려면 SCP 이름 옆의 확인란에서 선택을 취소하면 됩니다. SCP 콘텐츠를 보려면 해당 SCP 이름을 선택합니다.

   계정이 조직에 속하지 않은 경우, 시뮬레이션할 SCP가 없습니다.
4. (선택 사항) 그룹이 아닌 IAM 엔터티(사용자 또는 역할)에 대해 권한 경계 (p. 363)로 설정된 정책을 테스트할 수 있습니다. 현재 엔터티에 대해 권한 경계 정책이 설정되어 있는 경우 정책 창에 표시됩니다. 한 엔터티에 대해 권한 경계 하나만 설정할 수 있습니다. 다른 권한 경계를 테스트하려면 사용자 지정 권한 경계를 만들면 됩니다. 이렇게 하려면 새 정책 생성을 선택합니다. 새 정책 창이 열립니다. 메뉴에서 사용자 지정 IAM 권한 경계 정책을 선택합니다. 새 정책의 이름을 입력하고 아래 공백에 정책을 입력하거나 복사합니다. 적용을 선택하여 정책을 저장합니다. 그런 다음 뒤로를 선택하여 원래 정책 창으로 돌아갑니다. 시뮬레이션에 사용할 권한 경계 옆의 확인란을 선택합니다.
5. (선택 사항) 사용자, 그룹 또는 역할에 연결된 정책의 하위 집합만 테스트할 수 있습니다. 이렇게 하려면 정책 창에서 제외할 각 정책 옆에 있는 확인란의 선택을 취소합니다.
6. Policy Simulator(정책 시뮬레이터)에서 Select service(서비스 선택)를 선택한 후 테스트할 서비스를 선택합니다. 그런 다음 Select actions(작업 선택)을 선택하고 테스트할 작업을 한 개 이상 선택합니다. 메뉴에는 한 번에 한 서비스에 대해 가능한 선택만 표시되지만 선택한 모든 서비스와 작업이 Action Settings and Results(작업 설정 및 결과)에 나타납니다.
7. (선택 사항) Step 2 및 Step 5에서 선택하는 정책 중 하나라도 AWS 글로벌 조건 키 (p. 650)를 지닌 조건을 포함하는 경우, 해당 키에 대한 값을 제공합니다. 글로벌 설정 섹션을 확장하고 표시된 키 이름의 값을 입력하여 키에 대한 값을 제공할 수 있습니다.

   Warning

   조건 키의 값을 비워 놓으면 해당 키가 시뮬레이션 중에 무시됩니다. 이로 인해 오류가 발생하고 시뮬레이션이 실행되지 않는 경우가 있습니다. 또한 시뮬레이션은 실행되지만 결과를 신뢰할 수 없는 경우도 있습니다. 이 경우 조건 키에 대한 값이나 변수를 포함하는 실제 조건과 시뮬레이션이 일치하지 않습니다.
8. (선택 사항) 선택한 각 작업은 Action Settings and Results(작업 설정 및 결과) 목록에 표시되고 실제로 시뮬레이션을 실행할 때까지는 권한 열에 Not simulated(시뮬레이션되지 않음)이라고 표시됩니다. 시뮬레이션을 실행하기 전에 리소스를 포함하는 각 작업을 구성할 수 있습니다. 특정 시나리오에 맞게 개별 작업을 구성하려면 화살표를 선택하여 작업 행을 확장합니다. 작업이 리소스 수준 권한을 지원할 경우 액세스를 테스트하려는 특정 리소스의 Amazon 리소스 이름(ARN) (p. 564)을 입력할 수 있습니다. 기본적으로 각 리소스는 와일드카드(*)로 설정됩니다. 또한 임의의 조건 콘텍스트 키 (p. 673)에 대한 값을 지정할 수 있습니다. 앞에서도 설명했듯이 값이 비어 있는 키는 무시되며, 이로 인해 시뮬레이션이 실패하거나 신뢰할 수 없는 결과가 반환될 수 있습니다.

   a. 작업 이름 옆에 있는 화살표를 선택하여 각 행을 확장하고 해당 시나리오에 맞게 작업을 정확하게 시뮬레이션하는 데 필요한 추가 정보를 구성합니다. 작업에 리소스 수준 권한이 필요할 경우 액세스를 시뮬레이션하려는 특정 리소스의 Amazon 리소스 이름(ARN) (p. 564)을 입력할 수 있습니다. 기본적으로 각 리소스는 와일드카드(*)로 설정됩니다.
   b. 작업이 리소스 수준 권한을 지원하지만 그러한 권한이 필요하지 않을 경우 리소스 추가를 선택하여 시뮬레이션에 추가하려는 리소스 유형을 선택합니다.
   c. 선택한 정책이 해당 작업의 서비스에 대한 콘텍스트 키를 참조하는 `Condition` 요소를 포함할 경우 해당 키 이름이 작업 아래에 표시됩니다. 지정한 리소스에 대한 해당 작업의 시뮬레이션 중에 사용할 값을 지정할 수 있습니다.

   여러 리소스 유형 그룹이 필요한 작업

일부 작업은 서로 다른 환경에서 여러 리소스 유형이 필요합니다. 리소스 유형의 각 그룹은 시나리오와 관련이 있습니다. 이 중 하나가 시뮬레이션에 적용될 경우 리소스를 선택하면 시뮬레이터가 해당 시나리오에 적합한 리소스 유형을 필요로 합니다. 다음 목록에는 지원되는 각 시나리오 옵션과 시뮬레이션을 실행하기 위해 정의해야 하는 리소스가 나와 있습니다.

다음의 Amazon EC2 시나리오 각각에 대해 `instance`, `image`, `security-group` 리소스를 지정해야 합니다. 시나리오에 EBS 볼륨이 포함될 경우에는 해당 `volume`을 리소스로 지정해야 합니다. Amazon EC2 시나리오에 가상 프라이빗 클라우드(VPC)가 포함될 경우에는 `network-interface` 리소스를 제공해야 합니다. IP 서브넷이 포함될 경우에는 `subnet` 리소스를 지정해야 합니다. Amazon EC2 시나리오 옵션에 대한 자세한 정보는 Amazon EC2 사용 설명서의 지원되는 플랫폼을 참조하십시오.

- EC2-Classic-InstanceStore

  인스턴스, 이미지, 보안 그룹
- EC2-Classic-EBS

  인스턴스, 이미지, 보안 그룹, 볼륨
- EC2-VPC-InstanceStore

  인스턴스, 이미지, 보안 그룹, 네트워크 인터페이스
- EC2-VPC-InstanceStore-Subnet

  인스턴스, 이미지, 보안 그룹, 네트워크 인터페이스, 서브넷
- EC2-VPC-EBS

  인스턴스, 이미지, 보안 그룹, 네트워크 인터페이스, 볼륨
- EC2-VPC-EBS-Subnet

  인스턴스, 이미지, 보안 그룹, 네트워크 인터페이스, 서브넷, 볼륨

9. (선택 사항) 시뮬레이션에 리소스 기반 정책을 포함하려면 먼저 해당 리소스에 대해 시뮬레이션하려는 작업을 Step 6에서 선택해야 합니다. 선택한 작업의 행을 확장하고 시뮬레이션하려는 정책을 포함하는 리소스의 ARN을 입력합니다. 그런 다음 ARN 텍스트 상자 옆의 리소스 정책 포함(Include Resource Policy)을 선택합니다. IAM 정책 시뮬레이터는 현재, Amazon S3(리소스 기반 정책만 해당. ACL은 현재 지원되지 않음), Amazon SQS, Amazon SNS 및 잠겨 있지 않은 S3 Glacier 볼트(잠겨 있는 볼트는 현재 지원되지 않음) 서비스의 리소스 기반 정책만 지원합니다.
10. 상단 오른쪽 모서리 부분에서 Run Simulation(시뮬레이션 실행)을 선택합니다.

    Action Settings and Results(작업 설정 및 결과)의 각 행에 있는 권한 열에 지정된 리소스에 대한 해당 작업의 시뮬레이션 결과가 표시됩니다.
11. 상단 오른쪽 모서리 부분에서 Run Simulation(시뮬레이션 실행)을 선택합니다.

    Action Settings and Results(작업 설정 및 결과)의 각 행에 있는 권한 열에 지정된 리소스에 대한 해당 작업의 시뮬레이션 결과가 표시됩니다.
12. 정책의 어떤 문이 작업을 허용하거나 거부하는지 확인하려면 권한 열에서 ***N*** matching statement(s)(일치하는 문 N개) 링크를 선택하여 행을 확장한 후 Show statement(문 표시) 링크를 선택합니다. 정책 창에 해당 정책이 표시되고 시뮬레이션 결과에 영향을 준 문이 강조 표시됩니다.

    Note

    작업이 암묵적으로 거부된 경우, 즉 명시적으로 허용되지 않아 작업이 거부된 경우에만 목록 및 Show statement(문 표시) 옵션이 표시되지 않습니다.

IAM 정책 시뮬레이터 콘솔 메시지 문제 해결

다음 표에는 IAM 정책 시뮬레이터 사용 시 나타날 수 있는 정보 메시지와 경고 메시지가 나와 있습니다. 그 밖에 문제 해결에 필요한 단계도 나와 있습니다.

Message	문제 해결 단계
This policy has been edited. Changes will not be saved to your account.	작업이 필요하지 않음 이것은 정보 메시지입니다. IAM 정책 시뮬레이터에서 기존 정책을 편집하더라도 AWS 계정에서는 변경 사항이 적용되지 않습니다. 시뮬레이터에서는 테스트 목적으로만 정책을 변경할 수 있습니다.
Cannot get the resource policy. 사유: ## ## ###	요청된 리소스 기반 정책에 시뮬레이터가 액세스할 수 없습니다. 지정된 리소스 ARN이 정확하며, 시뮬레이션을 실행하는 사용자가 리소스의 정책을 읽을 수 있는 권한이 있는지 확인하십시오.
One or more policies require values in the simulation settings. The simulation might fail without these values.	이 메시지는 테스트하려는 정책에 포함되어 있는 조건 키 또는 변수 값을 Simulation Settings(시뮬레이션 설정)에 입력하지 않은 경우 나타납니다. 이 메시지를 닫으려면 Simulation Settings(시뮬레이션 설정)를 선택한 다음 각 조건 키 또는 변수에 대한 값을 입력합니다.
You have changed policies. These results are no longer valid.	이 메시지는 결과가 Results 창에 표시되는 중에 선택한 정책을 변경하였을 때 나타납니다. Results 창에 표시되는 결과는 동적으로 업데이트되지 않습니다. 이 메시지를 닫으려면 정책 창의 변경에 따라 다시 Run Simulation(시뮬레이션 실행)을 선택하여 새로운 시뮬레이션 결과를 표시합니다.
The resource you typed for this simulation does not match this service.	이 메시지는 현재 시뮬레이션에서 선택한 서비스와 일치하지 않는 Amazon 리소스 이름(ARN)을 Simulation Settings(시뮬레이션 설정) 창에 입력했을 때 나타납니다. 예를 들어, Amazon DynamoDB 리소스의 ARN을 지정하고 시뮬레이션할 서비스로 Amazon Redshift를 선택하면 이 메시지가 나타납니다. 이 메시지를 닫으려면 다음 중 한 가지를 실행합니다. • Simulation Settings(시뮬레이션 설정) 창의 상자에서 ARN을 삭제합니다. • Simulation Settings(시뮬레이션 설정)에서 지정한 ARN과 일치하는 서비스를 선택합니다.
이 작업은 Amazon S3 ACL 또는 S3 Glacier 볼트 잠금 정책 같은 리소스 기반 정책 외에 특수 액세스 제어 방식을 지원하는 서비스에 속합니다. The policy simulator does not support these mechanisms, so the results can differ from your production environment.	작업이 필요하지 않음 이것은 정보 메시지입니다. 현재 버전에서 시뮬레이터는 사용자와 그룹에 연결된 정책을 평가하며, Amazon S3, Amazon SQS, Amazon SNS, S3 Glacier에 대한 리소스 기반 정책을 평가할 수 있습니다. 정책 시뮬레이터가 다른 AWS 서비스에서 지

Message	문제 해결 단계
	원하는 액세스 제어 방식을 모두 지원하는 것은 아닙니다.
DynamoDB FGAC is currently not supported.	작업이 필요하지 않음 이 정보 메시지는 세분화된 액세스 제어를 가리킵니다. 세분화된 액세스 제어는 IAM 정책 조건을 사용하여 DynamoDB 테이블 및 인덱스의 개별 데이터 항목과 속성에 액세스할 수 있는 사용자를 결정하는 기능입니다. 또한 이러한 테이블 및 인덱스에서 수행할 수 있는 작업을 나타내기도 합니다. 현재 버전의 IAM 정책 시뮬레이터는 이 유형의 정책 조건을 지원하지 않습니다. DynamoDB FGAC에 대한 자세한 정보는 DynamoDB에 대한 세분화된 액세스 제어를 참조하십시오.
You have policies that do not comply with the policy syntax. You can use the Policy Validator to review and accept the recommended updates to your policies.	이 메시지는 IAM 정책 문법을 위반하는 정책이 있는 경우 정책 목록 상단에 나타납니다. 이러한 정책은 JSON 정책 검증 (p. 441)의 지침에 따른 시뮬레이션을 통해 식별하여 위반 문제를 해결해야 합니다.
This policy must be updated to comply with the latest policy syntax rules.	이 메시지는 IAM 정책 문법을 위반하는 정책이 있는 경우에 표시됩니다. 이러한 정책은 JSON 정책 검증 (p. 441)의 지침에 따른 시뮬레이션을 통해 식별하여 위반 문제를 해결해야 합니다.

IAM 정책 시뮬레이터의 사용(AWS CLI 및 AWS API)

정책 시뮬레이터 명령어는 다음의 2가지 작업을 수행하는 데 일반적으로 API 작업 호출이 필요합니다.

1. 정책을 평가하고 정책이 참조하는 콘텍스트 키 목록을 반환합니다. 어떤 콘텍스트 키가 참조되는지 알아야 다음 단계에서 콘텍스트 키에 값을 제공할 수 있습니다.
2. 시뮬레이션 중에 사용되는 작업, 리소스, 콘텍스트 키의 목록을 제공하여 정책을 시뮬레이션합니다.

보안 상의 이유로 API 작업은 2개의 그룹으로 나뉘어 있습니다.

- API에 직접 문자열로 전달되는 정책만을 시뮬레이션하는 API 작업. 이 세트에는 GetContextKeysForCustomPolicy 및 SimulateCustomPolicy가 포함됩니다.
- 지정된 IAM 사용자, 그룹, 역할 또는 리소스에 연결된 정책을 시뮬레이션하는 API 작업. 이러한 API 작업은 다른 IAM 주체에 할당된 권한의 세부 정보를 알려주기 때문에 이 API 작업에 대한 액세스 제한을 고려해 보아야 합니다. 이 세트에는 GetContextKeysForPrincipalPolicy 및 SimulatePrincipalPolicy가 포함됩니다. API 작업 액세스 제한에 대한 자세한 정보는 정책 예제: AWS Identity and Access Management(IAM) (p. 388) 단원을 참조하십시오.

두 경우 모두 API 작업은 1개 이상의 정책들이 작업 및 리소스 목록에 미치는 영향을 시뮬레이션합니다. 각 작업은 각 리소스와 짝을 이루고, 시뮬레이션은 정책이 리소스에 대한 작업을 허용 또는 거부하는지 여부를 결정합니다. 또한, 정책이 참조하는 모든 콘텍스트 키에 대한 값을 제공할 수 있습니다. 정책이 참조하는 콘텍스트 키 목록은 `GetContextKeysForCustomPolicy` 또는 `GetContextKeysForPrincipalPolicy`를 호출하여 확인할 수 있습니다. 콘텍스트 키에 대한 값을 제공하지 않는다 해도 시뮬레이션은 여전히 실행되고 있지만, 시뮬레이터가 평가 시에 콘텍스트 키를 포함할 수 없기 때문에 그 결과를 신뢰하지 못할 수 있습니다.

조건 키 목록을 확인하려면(AWS CLI, AWS API)

다음을 사용하여 정책 목록을 평가하고, 정책에 사용된 콘텍스트 키 목록을 반환합니다.

- AWS CLI, `aws iam get-context-keys-for-custom-policy` 및 `aws iam get-context-keys-for-principal-policy`
- AWS API: `GetContextKeysForCustomPolicy` 및 `GetContextKeysForPrincipalPolicy`

IAM 정책을 시뮬레이션하려면(AWS CLI, AWS API)

다음을 통해 IAM 정책을 시뮬레이션하여 사용자의 유효 권한을 확인합니다.

- AWS CLI, `aws iam simulate-custom-policy` 및 `aws iam simulate-principal-policy`
- AWS API: `SimulateCustomPolicy` 및 `SimulatePrincipalPolicy`

IAM 자격 증명 권한 추가 및 제거

정책을 사용하여 자격 증명(사용자, 그룹 또는 역할)에 대한 권한을 정의합니다. AWS Management 콘솔, AWS Command Line Interface(AWS CLI) 또는 AWS API를 사용하여 자격 증명에 대한 IAM 정책을 첨부 및 분리하여 사용 권한을 추가 및 제거할 수 있습니다. 정책을 사용하여 동일한 방법으로 엔터티(사용자 또는 역할)에 대한 권한 경계 (p. 363)만 설정할 수 있습니다. 권한 경계는 엔터티가 가질 수 있는 최대 권한을 제어하는 고급 AWS 기능입니다.

주제

용어

권한 정책을 자격 증명(사용자, 그룹, 역할)과 연결할 때, 관리형 정책을 사용하는지 아니면 인라인 정책을 사용하는지에 따라 용어와 절차가 달라집니다.

- 연결 – 관리형 정책에 사용됩니다. 자격 증명(사용자, 그룹 또는 역할)에 관리형 정책을 연결합니다. 정책을 연결하면 정책의 해당 권한이 자격 증명에 적용됩니다.
- 분리 – 관리형 정책에 사용됩니다. IAM 자격 증명(사용자, 그룹, 역할)에서 관리형 정책을 분리합니다. 정책을 분리하면 자격 증명에서 해당 권한이 제거됩니다.
- 포함 – 인라인 정책에 사용됩니다. 자격 증명(사용자, 그룹 또는 역할)에 인라인 정책을 포함시킵니다. 정책을 포함하면 정책의 해당 권한이 자격 증명에 적용됩니다. 인라인 정책은 자격 증명에 저장되므로 결과는 비슷하지만 연결되지 않고 포함됩니다.

  Note

  역할에 따라 달라지는 서비스에만 서비스 연결 역할 (p. 175)에 대한 인라인 정책을 포함할 수 있습니다. 서비스가 이 기능을 지원하는지 여부를 확인하려면 서비스에 대한 AWS 설명서를 참조하십시오.
- 삭제 – 인라인 정책에 사용됩니다. IAM 자격 증명(사용자, 그룹, 역할)에서 인라인 정책을 삭제합니다. 정책을 삭제하면 자격 증명에서 해당 권한이 제거됩니다.

Note

역할에 따른 서비스에서만 서비스 연결 역할 (p. 175)의 인라인 정책을 삭제할 수 있습니다. 서비스가 이 기능을 지원하는지 여부를 확인하려면 서비스에 대한 AWS 설명서를 참조하십시오.

콘솔, AWS CLI 또는 AWS API를 사용하여 다음과 같은 작업을 수행할 수 있습니다.

추가 정보

- 관리형 정책과 인라인 정책의 차이점에 대한 자세한 정보는 관리형 정책과 인라인 정책 (p. 357) 단원을 참조하십시오.
- 권한 경계에 대한 자세한 정보는 IAM 엔터티에 대한 권한 경계 (p. 363) 단원을 참조하십시오.
- IAM 정책에 대한 일반적인 내용은 정책 및 권한 (p. 349) 단원을 참조하십시오.
- 정책 크기 제한에 대한 자세한 정보는 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

자격 증명 작업 보기

자격 증명(사용자, 그룹 또는 역할)에 대한 사용 권한을 변경하기 전에 최근 서비스 수준 활동을 검토해야 합니다. 이 기능은 사용 중인 보안 주체(사람 또는 애플리케이션)의 액세스 권한을 제거하지 않으려는 경우 중요합니다. 서비스에서 마지막으로 액세스한 데이터 보기에 대한 자세한 정보는 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

IAM 자격 증명 권한 추가(콘솔)

AWS Management 콘솔을 사용하여 자격 증명(사용자, 그룹 또는 역할)에 권한을 추가할 수 있습니다. 이렇게 하려면 권한을 제어하는 관리형 정책을 연결하거나 권한 경계 (p. 363) 역할을 하는 정책을 지정하십시오. 인라인 정책을 포함할 수도 있습니다.

자격 증명에 대한 권한 정책으로서 관리형 정책을 사용하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 연결할 정책 이름 옆의 확인란을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. [Policy actions]를 선택한 후 [Attach]를 선택합니다.
5. 정책을 연결할 자격 증명을 하나 이상 선택합니다. [Filter] 메뉴와 검색 상자를 사용하면 보안 주체 개체 목록을 필터링할 수 있습니다. 자격 증명을 선택한 후 정책 연결을 선택합니다.

보안 경계(콘솔)를 설정하기 위해서 관리형 정책을 사용하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 설정할 정책 이름을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. 정책 요약 페이지에서 Policy usage tab(정책 활용 탭)을 선택하고 필요하다면 Permissions boundaries(권한 경계) 섹션에서 Set boundary(경계 설정)을 선택합니다.
5. 권한 경계에 대한 정책이 사용될 하나 이상의 사용자 또는 역할을 선택하십시오. [Filter] 메뉴와 검색 상자를 사용하면 보안 주체 개체 목록을 필터링할 수 있습니다. 보안 주체를 선택한 후 Set boundaries(경계 설정)을 선택합니다.

사용자 또는 역할의 인라인 정책을 포함하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자 또는 역할을 선택합니다.
3. 목록에서 정책을 삽입할 그룹, 사용자 또는 역할 이름을 선택합니다.
4. Permissions 탭을 선택합니다.
5. 페이지의 하단으로 스크롤하고 Add inline policy(인라인 정책 추가)를 선택합니다.

   Note

   IAM에서 service-linked role (p. 175)에 인라인 정책을 포함시킬 수 없습니다. 링크된 서비스가 역할 권한을 수정할 수 있는지 여부를 결정하기 때문에 서비스 콘솔이나 API 또는 AWS CLI에서 정책을 추가할 수 있습니다. 서비스에 대한 서비스 연결 역할 설명서를 보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하고, 해당 서비스의 Service-Linked Role(서비스 연결 역할) 열에서 예를 선택합니다.
6. 다음 방법 중에서 선택하여 정책을 생성하는 데 필요한 단계를 볼 수 있습니다.

   - 기존 관리형 정책 가져오기 (p. 438) – 계정으로 관리형 정책을 가져온 다음 정책을 편집하여 특정 요구 사항에 맞게 사용자 지정할 수 있습니다. 관리형 정책은 사용자가 이전에 생성한 고객 관리형 정책이거나 AWS 관리형 정책일 수 있습니다.
   - 시각적 편집기를 사용하여 정책 만들기 (p. 437) – 시각적 편집기에서 정책을 새로 생성할 수 있습니다. 시각적 편집기를 사용할 경우 JSON 구문을 이해할 필요가 없습니다.
   - JSON 탭에서 정책 만들기 (p. 436) – JSON 탭에서 JSON 구문을 사용하여 정책을 생성할 수 있습니다. 새 JSON 정책 문서를 입력하거나 예제 정책 (p. 387)을 붙여 넣을 수 있습니다.
7. 인라인 정책을 생성하고 나면 이 정책이 사용자나 역할에 자동으로 포함됩니다.

그룹의 인라인 정책을 포함하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 [Groups]를 선택합니다.
3. 목록에서 정책을 삽입할 그룹 이름을 선택합니다.
4. 권한 탭을 선택하고 필요할 경우 Inline Policies(인라인 정책) 섹션을 확장합니다.
5. Create Group Policy(그룹 정책 생성)을 선택합니다. 그룹에 기존 정책이 없는 경우 여기를 클릭하십시오를 선택하여 첫 번째 인라인 정책을 만듭니다.
6. 정책 생성기 또는 사용자 지정 정책과 선택을 차례대로 선택합니다.
7. 다음 중 하나를 수행하십시오.

   - 사용자 지정 정책을 선택한 경우에는 정책 이름을 지정한 후 정책 문서를 생성합니다. 정책 검사기 (p. 441)가 모든 구문 오류를 보고합니다.
   - 정책 생성기를 사용하여 정책을 생성한 경우에는 효과, AWS 서비스 및 작업 옵션을 선택합니다. Amazon 리소스 이름(ARN)(해당하는 경우)을 입력하고 포함하려는 조건을 추가합니다. 그런 다음 설명문 추가를 선택합니다. 문은 원하는 만큼 정책에 추가할 수 있습니다. 문 추가를 마치면 다음 단계를 선택합니다.
8. 정책에 아무런 문제가 없으면 [Apply Policy]를 선택합니다.

하나 이상의 엔터티에 대한 권한 경계 설정을 변경하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.

2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 설정할 정책 이름을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. 정책 요약 페이지에서 Policy usage tab(정책 활용 탭)을 선택하고 필요하다면 Permissions boundaries(권한 경계) 섹션을 엽니다. 변경할 경계의 사용자 또는 역할 옆에 있는 확인란을 선택한 후 Change boundary(경계 변경)을 선택합니다.
5. 새로운 정책을 선택하여 권한 경계를 사용하십시오. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다. 정책을 선택한 후 Change boundary(경계 변경)을 선택합니다.

IAM 자격 증명 권한 제거(콘솔)

AWS Management 콘솔을 사용하여 자격 증명(사용자, 그룹 또는 역할)에서 권한을 제거할 수 있습니다. 이렇게 하려면 권한을 제어하는 관리형 정책을 분리하거나 권한 경계 (p. 363) 역할을 하는 정책을 제거하십시오. 인라인 정책을 삭제할 수도 있습니다.

권한 정책(콘솔)으로서 사용된 관리형 정책을 분리하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 분리할 정책 이름 옆의 확인란을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. Policy actions(정책 작업)을 선택한 후 분리를 선택합니다.
5. 정책을 분리할 자격 증명을 선택합니다. 필터 메뉴와 검색 상자를 사용하여 자격 증명 목록을 필터링할 수 있습니다. 자격 증명을 선택한 후 Detach policy(정책 분리)를 선택합니다.

권한 경계(콘솔)를 제거하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 설정할 정책 이름을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. 정책 요약 페이지에서 Policy usage tab(정책 활용 탭)을 선택하고 필요하다면 Permissions boundaries(권한 경계) 섹션에서 Remove boundary(경계 제거)를 선택합니다.
5. 제거를 선택하여 경계를 제거합니다.

인라인 정책을 삭제하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 그룹, 사용자 또는 역할을 선택합니다.
3. 목록에서 제거할 정책이 있는 그룹, 사용자 또는 역할 이름을 선택합니다.
4. Permissions 탭을 선택합니다. 그룹을 선택한 경우 필요에 따라 Inline Policies(인라인 정책) 섹션을 확장합니다.
5. 그룹에서는 Remove Policy(정책 제거)를 선택합니다. 사용자 또는 역할에서는 X를 선택합니다.

IAM 정책 추가(AWS CLI)

AWS CLI을 사용하여 자격 증명(사용자, 그룹 또는 역할)에 권한을 추가할 수 있습니다. 이렇게 하려면 권한을 제어하는 관리형 정책을 연결하거나 권한 경계 (p. 363) 역할을 하는 정책을 지정하십시오. 인라인 정책을 포함할 수도 있습니다.

엔터티에 대한 권한 정책으로서 관리형 정책을 사용하려면(AWS CLI)

1. (선택 사항) 관리형 정책에 대한 정보를 보려면 다음 명령을 실행합니다.
   - 관리형 정책의 목록 보기: aws iam list-policies
   - 관리형 정책에 대한 세부 정보 가져오기: get-policy
2. 관리형 정책을 자격 증명(사용자, 그룹 또는 역할)에 연결하려면 다음 명령 중 하나를 사용합니다.
   - aws iam attach-user-policy
   - aws iam attach-group-policy
   - aws iam attach-role-policy

보안 경계(AWS CLI)를 설정하기 위해서 관리형 정책을 사용하려면

1. (선택 사항) 관리형 정책에 대한 정보를 보려면 다음 명령을 실행합니다.
   - 관리형 정책의 목록 보기: aws iam list-policies
   - 관리형 정책에 대한 세부 정보 가져오기: aws iam get-policy
2. 관리형 정책을 사용하여 엔터티(사용자 또는 역할)에 대한 권한 경계를 설정하려면 다음 명령 중 하나를 사용합니다.
   - aws iam put-user-permissions-boundary
   - aws iam put-role-permissions-boundary

인라인 정책을 포함시키려면(AWS CLI)

인라인 정책을 자격 증명(사용자, 그룹 또는 서비스 연결 역할 (p. 175)이 아닌 역할)에 포함시키려면 다음 명령 중 하나를 사용합니다.

- aws iam put-user-policy
- aws iam put-group-policy
- aws iam put-role-policy

IAM 정책 제거(AWS CLI)

AWS CLI를 사용하여 권한을 제어하는 관리형 정책을 분리하거나 권한 경계 (p. 363) 역할을 하는 정책을 제거할 수 있습니다. 인라인 정책을 삭제할 수도 있습니다.

권한 정책(AWS CLI)으로서 사용된 관리형 정책을 분리하려면

1. (선택 사항)정책에 대한 정보를 보려면 다음 명령을 실행합니다.
   - 관리형 정책의 목록 보기: aws iam list-policies
   - 관리형 정책에 대한 세부 정보 가져오기: aws iam get-policy
2. (선택 사항) 정책과 자격 증명 간의 관계에 대해 확인하려면 다음 명령을 실행합니다.
   - 관리형 정책이 연결된 자격 증명(사용자, 그룹 및 역할)의 목록을 보려면 다음과 같이 합니다.

    - aws iam list-entities-for-policy
  - 자격 증명(사용자, 그룹 또는 역할)에 연결된 관리형 정책의 목록을 보려면 다음 명령 중 하나를 사용합니다.
    - aws iam list-attached-user-policies
    - aws iam list-attached-group-policies
    - aws iam list-attached-role-policies
3. 관리형 정책을 자격 증명(사용자, 그룹 또는 역할)에서 분리하려면 다음 명령 중 하나를 사용합니다.
   - aws iam detach-user-policy
   - aws iam detach-group-policy
   - aws iam detach-role-policy

권한 경계(AWS CLI)를 제거하려면

1. (선택 사항) 현재 어떤 관리형 정책을 사용하여 사용자 또는 역할에 대한 권한 경계를 설정하는지 보려면 다음 명령을 실행하십시오.
   - aws iam get-user
   - aws iam get-role
2. (선택 사항) 현재 어떤 관리형 정책의 사용자 또는 역할이 권한 경계로 사용되는지 보려면 다음 명령을 실행하십시오.
   - aws iam list-entities-for-policy
3. (선택 사항) 관리형 정책에 대한 정보를 보려면 다음 명령을 실행합니다.
   - 관리형 정책의 목록 보기: aws iam list-policies
   - 관리형 정책에 대한 세부 정보 가져오기: aws iam get-policy
4. 사용자 또는 역할에서 권한 경계를 제거하려면 다음 명령 중 하나를 사용합니다.
   - aws iam delete-user-permissions-boundary
   - aws iam delete-role-permissions-boundary

인라인 정책을 삭제하려면(AWS CLI)

1. (선택 사항) 자격 증명(사용자, 그룹 또는 역할)에 연결된 모든 인라인 정책의 목록을 보려면 다음 명령 중 하나를 사용합니다.
   - aws iam list-user-policies
   - aws iam list-group-policies
   - aws iam list-role-policies
2. (선택 사항) 자격 증명(사용자, 그룹 또는 역할)에 포함된 인라인 정책 문서를 가져오려면 다음 명령 중 하나를 사용합니다.
   - aws iam get-user-policy
   - aws iam get-group-policy
   - aws iam get-role-policy
3. 자격 증명(사용자, 그룹 또는 서비스 연결 역할 (p. 175)이 아닌 역할)에서 인라인 정책을 삭제하려면 다음 명령 중 하나를 사용합니다.
   - aws iam delete-user-policy
   - aws iam delete-group-policy
   - aws iam delete-role-policy

IAM 정책 추가(AWS API)

AWS API를 사용하여 권한을 제어하는 관리형 정책을 연결하거나 권한 경계 (p. 363) 역할을 하는 정책을 지정할 수 있습니다. 인라인 정책을 포함할 수도 있습니다.

엔터티에 대한 권한 정책으로서 관리형 정책을 사용하려면(AWS API)

1. (선택 사항)정책에 대한 정보를 보려면 다음 작업을 호출합니다.
   - 관리형 정책의 목록 보기: ListPolicies
   - 관리형 정책에 대한 세부 정보 가져오기: GetPolicy
2. 관리형 정책을 자격 증명(사용자, 그룹 또는 역할)에 연결하려면 다음 작업 중 하나를 호출합니다.
   - AttachUserPolicy
   - AttachGroupPolicy
   - AttachRolePolicy

보안 경계(AWS API)를 설정하기 위해서 관리형 정책을 사용하려면

1. (선택 사항) 관리형 정책에 대한 정보를 보려면 다음 작업을 호출합니다.
   - 관리형 정책의 목록 보기: ListPolicies
   - 관리형 정책에 대한 세부 정보 가져오기: GetPolicy
2. 관리형 정책을 사용하여 엔터티(사용자 또는 역할)에 대한 권한 경계를 설정하려면 다음 작업 중 하나를 호출합니다.
   - PutUserPermissionsBoundary
   - PutRolePermissionsBoundary

인라인 정책을 포함시키려면(AWS API)

인라인 정책을 자격 증명(사용자, 그룹 또는 서비스 연결 역할 (p. 175)이 아닌 역할)에 포함시키려면 다음 작업 중 하나를 호출합니다.

- PutUserPolicy
- PutGroupPolicy
- PutRolePolicy

IAM 정책 제거(AWS API)

AWS API를 사용하여 권한을 제어하는 관리형 정책을 분리하거나 권한 경계 (p. 363) 역할을 하는 정책을 제거할 수 있습니다. 인라인 정책을 삭제할 수도 있습니다.

권한 정책(AWS API)으로서 사용된 관리형 정책을 분리하려면

1. (선택 사항)정책에 대한 정보를 보려면 다음 작업을 호출합니다.
   - 관리형 정책의 목록 보기: ListPolicies
   - 관리형 정책에 대한 세부 정보 가져오기: GetPolicy
2. (선택 사항) 정책과 자격 증명 간의 관계에 대해 확인하려면 다음 작업을 호출합니다.
   - 관리형 정책이 연결된 자격 증명(사용자, 그룹 및 역할)의 목록을 보려면 다음과 같이 합니다.

    - ListEntitiesForPolicy
  - 자격 증명(사용자, 그룹 또는 역할)에 연결된 관리형 정책의 목록을 보려면 다음 작업 중 하나를 호출합니다.
    - ListAttachedUserPolicies
    - ListAttachedGroupPolicies
    - ListAttachedRolePolicies
3. 관리형 정책을 자격 증명(사용자, 그룹 또는 역할)에서 분리하려면 다음 작업 중 하나를 호출합니다.

   - DetachUserPolicy
   - DetachGroupPolicy
   - DetachRolePolicy

권한 경계(AWS API)를 제거하려면

1. (선택 사항) 현재 어떤 관리형 정책을 사용하여 사용자 또는 역할에 대한 권한 경계를 설정하는지 보려면 다음 작업을 호출하십시오.

   - GetUser
   - GetRole
2. (선택 사항) 현재 어떤 관리형 정책의 사용자 또는 역할이 권한 경계로 사용되는지 보려면 다음 작업을 호출하십시오.

   - ListEntitiesForPolicy
3. (선택 사항) 관리형 정책에 대한 정보를 보려면 다음 작업을 호출합니다.

   - 관리형 정책의 목록 보기: ListPolicies
   - 관리형 정책에 대한 세부 정보 가져오기: GetPolicy
4. 사용자 또는 역할에서 권한 경계를 제거하려면 다음 작업 중 하나를 호출합니다.

   - DeleteUserPermissionsBoundary
   - DeleteRolePermissionsBoundary

인라인 정책을 삭제하려면(AWS API)

1. (선택 사항) 자격 증명(사용자, 그룹 또는 역할)에 연결된 모든 인라인 정책의 목록을 보려면 다음 작업 중 하나를 호출합니다.

   - ListUserPolicies
   - ListGroupPolicies
   - ListRolePolicies
2. (선택 사항) 자격 증명(사용자, 그룹 또는 역할)에 포함된 인라인 정책 문서를 가져오려면 다음 작업 중 하나를 호출합니다.

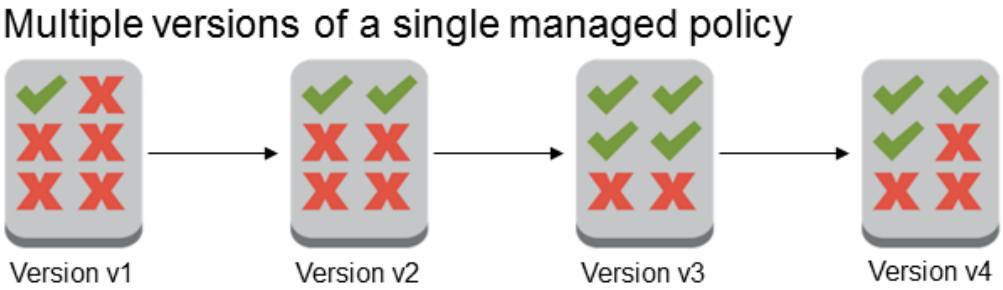
   - GetUserPolicy
   - GetGroupPolicy
   - GetRolePolicy
3. 인라인 정책을 자격 증명(사용자, 그룹 또는 서비스 연결 역할 (p. 175)이 아닌 역할)에서 삭제하려면 다음 작업 중 하나를 호출합니다.

   - DeleteUserPolicy
   - DeleteGroupPolicy
   - DeleteRolePolicy

IAM 정책 버전 관리

IAM 고객 관리형 정책을 변경할 때, 그리고 AWS에서 AWS 관리형 정책을 변경할 때 변경된 정책은 기존 정책을 덮어쓰지 않습니다. 대신 IAM은 관리형 정책의 새 버전을 만듭니다. IAM은 고객 관리 정책을 최대 5개 버전까지 저장합니다. IAM은 인라인 정책의 버전 관리를 지원하지 않습니다.

다음은 고객 관리형 정책의 버전 관리를 나타낸 다이어그램입니다.



정책 버전은 `Version` 정책 요소와 다릅니다. `Version` 정책 요소는 정책 내에서 사용되며 정책 언어의 버전을 정의합니다. `Version` 정책 요소에 대한 자세한 내용은 IAM JSON 정책 요소: Version (p. 587)을 참조하십시오.

버전을 사용하여 관리형 정책에 대한 변경 사항을 추적할 수 있습니다. 예를 들어 관리형 정책을 변경한 다음 해당 변경 사항으로 인해 의도하지 않은 결과가 발생한 사실을 발견할 수 있습니다. 이 경우 이전 버전을 기본 버전으로 설정하여 관리형 정책의 이전 버전으로 롤백할 수 있습니다.

다음 섹션에서는 관리형 정책에 버전 관리를 사용할 수 있는 방법에 대해 설명합니다.

주제

정책의 기본 버전을 설정할 수 있는 권한

정책의 기본 버전을 설정하는 데 필요한 권한은 작업에 대한 AWS API 작업에 해당합니다. `CreatePolicyVersion` 또는 `SetDefaultPolicyVersion` API 작업을 사용하여 정책의 기본 버전을 설정할 수 있습니다. 어떤 사람이 기존 정책의 기본 정책 버전을 설정할 수 있게 허용하려면 `iam:CreatePolicyVersion` 작업 또는 `iam:SetDefaultPolicyVersion` 작업에 대한 액세스 권한을 허용하면 됩니다. 그러면 `iam:CreatePolicyVersion` 작업을 이용해 새 버전의 정책을 생성하고 이 버전을 기본으로 설정할 수 있습니다. 또한 `iam:SetDefaultPolicyVersion` 작업을 통해서는 기존 버전의 정책을 기본으로 설정할 수 있습니다.

> **Important**
>
> 사용자의 정책에서 `iam:SetDefaultPolicyVersion` 작업을 거부해도 사용자가 새 정책 버전을 생성하고 이 버전을 기본으로 설정하는 작업을 하지 못하게 할 수는 없습니다.

다음 정책을 사용하면 사용자가 기존 고객 관리형 정책을 변경하기 위해 액세스하는 것을 거부할 수 있습니다.

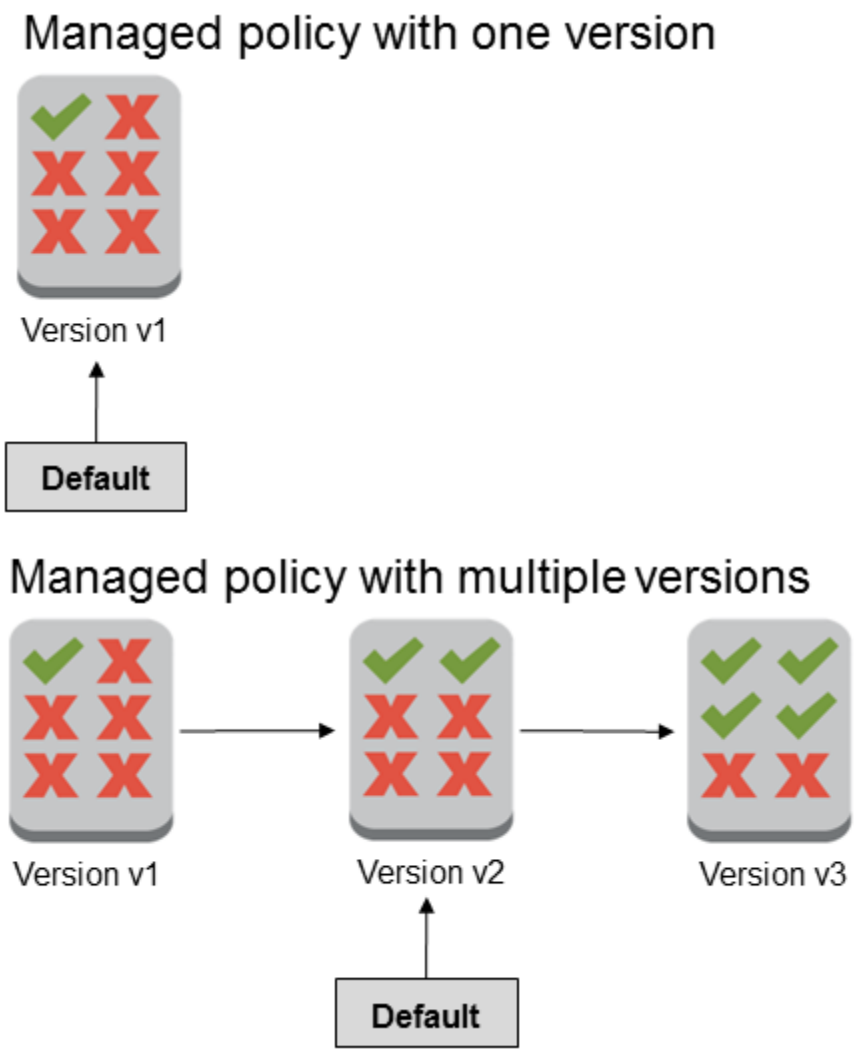
```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "iam:CreatePolicyVersion",
                "iam:SetDefaultPolicyVersion"
            ],
            "Resource": "arn:aws:iam::*:policy/POLICY-NAME"
        }
    ]
}
```

고객 관리형 정책의 기본 버전 설정

관리형 정책의 버전 중 하나가 기본 버전으로 설정됩니다. 정책의 기본 버전은 유효한 버전입니다. 즉, 기본 버전은 관리형 정책이 연결된 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에 적용되는 버전입니다.

고객 관리형 정책을 만들 때 정책은 v1로 식별되는 단일 버전으로 시작합니다. 버전이 하나뿐인 관리형 정책의 경우 해당 버전이 기본값으로 자동 설정됩니다. 버전이 둘 이상인 고객 관리형 정책의 경우에는 기본값으로 설정할 버전을 선택해야 합니다. AWS 관리형 정책의 경우 기본 버전은 AWS에서 설정됩니다. 다음 다이어그램에서는 이 개념을 보여 줍니다.



고객 관리형 정책의 기본 버전이 정책이 연결되는 모든 IAM 개체(사용자, 그룹 및 역할)에 적용되도록 해당 버전을 설정할 수 있습니다. 단, AWS 관리형 정책 또는 인라인 정책에는 기본 버전을 설정할 수 없습니다.

고객 관리형 정책의 기본 버전을 설정하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 기본 버전을 설정할 정책 이름을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. Policy versions(정책 버전) 탭을 선택합니다. 기본 버전으로 설정할 버전 옆의 확인란을 선택한 후 기본값으로 설정을 선택합니다.

AWS Command Line Interface 또는 AWS API에서 고객 관리형 정책을 기본 버전으로 설정하는 방법을 알아보려면 고객 관리형 정책 편집(AWS CLI) (p. 463) 단원을 참조하십시오.

버전을 사용하여 변경 사항 롤백

변경 사항을 롤백하도록 고객 관리형 정책의 기본 버전을 설정할 수 있습니다. 예를 들어 다음 시나리오를 고려해 보십시오:

사용자가 AWS Management 콘솔을 사용하여 특정 Amazon S3 버킷을 관리할 수 있도록 허용하는 고객 관리형 정책을 만듭니다. 생성 시 고객 관리형 정책의 버전은 v1로 식별되는 한 버전뿐이어서 이 버전이 기본값으로 자동 설정됩니다. 정책이 의도대로 적용됩니다.

나중에 두 번째 Amazon S3 버킷을 관리하기 위한 권한을 추가하기 위해 정책을 업데이트합니다. IAM에서 변경 사항을 포함하고 v2로 식별되는 정책의 새 버전을 만듭니다. v2 버전을 기본값으로 설정하고 얼마 지나지 않아 사용자들이 Amazon S3 콘솔을 사용할 수 있는 권한이 없다고 보고합니다. 이 경우 의도대로 적용되는 정책의 v1 버전으로 롤백할 수 있습니다. 이렇게 하기 위해 v1 버전을 기본 버전으로 설정합니다. 이제 사용자들이 Amazon S3 콘솔을 사용하여 원래 버킷을 관리할 수 있습니다.

나중에 정책의 v2 버전에 있는 오류를 해결한 후 두 번째 Amazon S3 버킷을 관리하기 위한 권한을 추가하기 위해 다시 정책을 업데이트합니다. IAM에서 v3으로 식별되는 정책의 새 버전을 하나 더 만듭니다. v3 버전을 기본값으로 설정합니다. 이 버전이 의도대로 적용됩니다. 이 시점에서 정책의 v2 버전을 삭제합니다.

버전 제한

관리형 정책에는 최대 5개의 버전이 있을 수 있습니다. 5개 버전을 만든 후에도 관리형 정책을 변경해야 할 경우 AWS Command Line Interface 또는 AWS API에서 먼저 기존 버전을 하나 이상 삭제해야 합니다. AWS Management 콘솔을 사용할 경우에는 정책을 편집하기 전에 버전을 삭제할 필요가 없습니다. 6번째 버전을 저장할 경우 정책의 기본 버전이 아닌 버전을 한 개 이상 삭제하라는 메시지가 표시된 대화 상자가 나타납니다. 결정을 위해 각 버전의 JSON 정책 문서를 볼 수 있습니다. 이 대화 상자에 대한 자세한 내용은 the section called “IAM 정책 편집” (p. 460) 단원을 참조하십시오.

기본 버전을 제외하고 원하는 모든 관리형 정책 버전을 삭제할 수 있습니다. 버전을 삭제할 때 나머지 버전의 버전 식별자는 변경되지 않습니다. 따라서 버전 식별자가 순차적이지 않을 수 있습니다. 예를 들어 관리형 정책의 v2 및 v4 버전을 삭제하고 새 버전을 2개 추가하면 나머지 버전 식별자가 v1, v3, v5, v6 및 v7이 될 수 있습니다.

IAM 정책 편집

정책 (p. 349)은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 개체입니다. 정책은 JSON 문서로 AWS에 저장되며 IAM에서 자격 증명 기반 정책으로 보안 주체에 연결됩니다. 자격 증명 기반 정책을 IAM 그룹, 사용자 또는 역할과 같은 보안 주체(또는 자격 증명)에 연결할 수 있습니다. 자격 증명 기반 정책에는

AWS 관리형 정책, 고객 관리형 정책 및 인라인 정책 (p. 357)이 포함됩니다. IAM에서 고객 관리형 정책 및 인라인 정책을 편집할 수 있습니다. AWS 관리형 정책은 편집할 수 없습니다. 정책 크기 제한 및 기타 할당량에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

주제

정책 액세스 보기

정책에 대한 권한을 변경하기 전에 최근 서비스 수준 활동을 검토해야 합니다. 이 기능은 사용 중인 보안 주체(사람 또는 애플리케이션)의 액세스 권한을 제거하지 않으려는 경우 중요합니다. 서비스에서 마지막으로 액세스한 데이터 보기에 대한 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

고객 관리형 정책 편집(콘솔)

고객 관리형 정책을 편집하여 정책에 정의된 권한을 변경할 수 있습니다. 고객 관리형 정책에 최대 5개의 버전을 사용할 수 있습니다. 이는 관리형 정책을 변경하여 버전이 5개 넘게 생성될 경우 AWS Management 콘솔에서 어느 버전을 삭제할 것이지 결정하라는 메시지가 표시되므로 중요합니다. 메시지가 표시되지 않도록 편집하기 전에 기본 버전을 변경하거나 정책 버전을 삭제할 수도 있습니다. 버전에 대한 자세한 내용은 IAM 정책 버전 관리 (p. 458) 단원을 참조하십시오.

고객 관리형 정책을 편집하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 편집할 정책 이름을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. 권한 탭을 선택한 다음 정책 편집을 선택합니다.
5. 다음 중 하나를 수행하십시오.
   - Visual editor(시각적 편집기) 탭을 선택하면 JSON 구문을 이해하지 않아도 정책을 변경할 수 있습니다. 정책의 각 권한 블록에 대한 서비스, 작업, 리소스 또는 조건(선택 사항)을 변경할 수 있습니다. 정책을 가져와 추가 권한을 정책 하단에 추가할 수도 있습니다. 변경이 완료되면 정책 검토를 선택하여 계속 진행합니다.
   - JSON 탭을 선택하고 JSON 텍스트 상자에 입력하거나 붙여 넣어 정책을 수정합니다. 정책을 가져와 추가 권한을 정책 하단에 추가할 수도 있습니다. 변경이 완료되면 정책 검토를 선택하여 계속 진행합니다. 정책 검사기 (p. 441)가 모든 구문 오류를 보고합니다.

     Note

     언제든지 Visual editor(시각적 편집기) 및 JSON 탭을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 정책 재구성 (p. 538) 단원을 참조하십시오.
6. 검토 페이지에서 정책 요약을 검토하고 나서 변경 사항 저장을 선택하여 작업을 저장합니다.
7. 관리형 정책 버전이 이미 최댓값인 5개가 있을 경우 저장을 선택하면 대화 상자가 나타납니다. 새 버전을 저장하려면 이전 버전을 한 개 이상 삭제해야 합니다. 기본 버전은 삭제할 수 없습니다. 다음 옵션 중 하나를 선택합니다.

- Remove oldest non-default policy version(version v# - created # days ago)(기본 정책을 제외하고 가장 오래된 정책 버전 제거(버전 v# - #일 전에 생성됨)) – 어느 버전이 삭제될 것이고 언제 삭제되었는지 보려면 이 옵션을 사용합니다. 두 번째 옵션인 Select versions to remove(제거할 버전 선택)을 선택하면 기본 버전 외 다른 버전 모두에 대한 JSON 정책 문서를 볼 수 있습니다.
- Select versions to remove(제거할 버전 선택) – JSON 정책 문서를 보고 한 개 이상을 선택하여 삭제하려면 이 옵션을 사용합니다.

삭제할 버전을 선택한 후 Delete version and save(버전 삭제 및 저장)을 선택하여 새 정책 버전을 저장합니다.

고객 관리형 정책의 기본 버전을 설정하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 기본 버전을 설정할 정책 이름을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. Policy versions(정책 버전) 탭을 선택합니다. 기본 버전으로 설정할 버전 옆의 확인란을 선택한 후 기본 값으로 설정을 선택합니다.

고객 관리형 정책의 버전을 삭제하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 버전을 삭제하려는 고객 관리형 정책의 이름을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. Policy versions(정책 버전) 탭을 선택합니다. 삭제하려는 버전 옆의 확인란을 선택합니다. 그런 다음 [Delete]를 선택합니다.
5. 버전을 정말로 삭제할 것인지 다시 한 번 묻는 메시지가 나오면 확인 후 삭제를 선택합니다.

인라인 정책 편집(콘솔)

AWS Management 콘솔에서 인라인 정책을 편집할 수 있습니다.

그룹, 사용자 또는 역할의 인라인 정책을 편집하려면(콘솔)

1. 탐색 창에서 사용자 또는 역할을 선택합니다.
2. 정책을 변경하려는 사용자 또는 역할 이름을 선택합니다. 그런 다음 권한 탭을 선택하고 정책을 확장합니다.
3. 인라인 정책을 편집하려면 정책 편집을 선택합니다.
4. 다음 중 하나를 수행하십시오.

   - Visual editor(시각적 편집기) 탭을 선택하면 JSON 구문을 이해하지 않아도 정책을 변경할 수 있습니다. 정책의 각 권한 블록에 대한 서비스, 작업, 리소스 또는 조건(선택 사항)을 변경할 수 있습니다. 정책을 가져와 추가 권한을 정책 하단에 추가할 수도 있습니다. 변경이 완료되면 정책 검토를 선택하여 계속 진행합니다.
   - JSON 탭을 선택하고 JSON 텍스트 상자에 입력하거나 붙여 넣어 정책을 수정합니다. 정책을 가져와 추가 권한을 정책 하단에 추가할 수도 있습니다. 변경이 완료되면 정책 검토를 선택하여 계속 진행합니다. 정책 검사기 (p. 441)가 모든 구문 오류를 보고합니다. 현재 추가된 주체에 아무런 영향을 주지

않고 변경 사항만 저장하려면 Save as default version(기본 버전으로 저장) 확인란의 선택을 해제합니다.

Note

언제든지 Visual editor(시각적 편집기) 및 JSON 탭을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 정책 재구성 (p. 538) 단원을 참조하십시오.

5. 검토 페이지에서 정책 요약을 검토하고 나서 변경 사항 저장을 선택하여 작업을 저장합니다.

그룹의 인라인 정책을 편집하려면

1. 탐색 창에서 [Groups]를 선택합니다.
2. 정책을 변경하려는 그룹 이름을 선택합니다. 그런 다음 권한 탭을 선택합니다.
3. 인라인 정책을 편집하려면 정책 편집을 선택합니다.
4. JSON 정책을 수정한 후 저장을 선택하여 변경 사항을 저장합니다.

고객 관리형 정책 편집(AWS CLI)

AWS Command Line Interface에서 고객 관리형 정책을 편집할 수 있습니다(AWS CLI).

Note

관리형 정책에는 최대 5개의 버전이 있을 수 있습니다. 5개 버전을 만든 후에도 고객 관리형 정책을 변경해야 할 경우 먼저 기존 버전을 1개 이상 삭제해야 합니다.

고객 관리형 정책을 편집하려면(AWS CLI)

1. (선택 사항)정책에 대한 정보를 보려면 다음 명령을 실행합니다.
   - 관리형 정책의 목록 보기: list-policies
   - 관리형 정책에 대한 세부 정보 가져오기: get-policy
2. (선택 사항) 정책과 자격 증명 간의 관계에 대해 확인하려면 다음 명령을 실행합니다.
   - 관리형 정책이 연결된 자격 증명(사용자, 그룹 및 역할)의 목록을 보려면 다음과 같이 합니다.
     - list-entities-for-policy
   - 자격 증명(사용자, 그룹 또는 역할)에 연결된 관리형 정책의 목록을 보려면
     - list-attached-user-policies
     - list-attached-group-policies
     - list-attached-role-policies
3. 고객 관리형 정책을 편집하려면 다음 명령을 실행합니다.
   - create-policy-version

고객 관리형 정책의 기본 버전을 설정하려면(AWS CLI)

1. (선택 사항) 관리형 정책 목록을 보려면 다음 명령을 실행합니다.
   - list-policies
2. 고객 관리형 정책의 기본 버전을 설정하려면 다음 명령을 실행합니다.

- set-default-policy-version

고객 관리형 정책의 한 버전을 삭제하려면(AWS CLI)

1. (선택 사항) 관리형 정책 목록을 보려면 다음 명령을 실행합니다.
   - list-policies
2. 고객 관리형 정책을 삭제하려면 다음 명령을 실행합니다.
   - delete-policy-version

고객 관리형 정책 편집(AWS API)

AWS API를 사용하여 고객 관리형 정책을 편집할 수 있습니다.

> Note
>
> 관리형 정책에는 최대 5개의 버전이 있을 수 있습니다. 5개 버전을 만든 후에도 고객 관리형 정책을 변경해야 할 경우 먼저 기존 버전을 1개 이상 삭제해야 합니다.

고객 관리형 정책을 편집하려면(AWS API)

1. (선택 사항)정책에 대한 정보를 보려면 다음 작업을 호출합니다.
   - 관리형 정책의 목록 보기: ListPolicies
   - 관리형 정책에 대한 세부 정보 가져오기: GetPolicy
2. (선택 사항) 정책과 자격 증명 간의 관계에 대해 확인하려면 다음 작업을 호출합니다.
   - 관리형 정책이 연결된 자격 증명(사용자, 그룹 및 역할)의 목록을 보려면 다음과 같이 합니다.
     - ListEntitiesForPolicy
   - 자격 증명(사용자, 그룹 또는 역할)에 연결된 관리형 정책의 목록을 보려면
     - ListAttachedUserPolicies
     - ListAttachedGroupPolicies
     - ListAttachedRolePolicies
3. 고객 관리형 정책을 편집하려면 다음 작업을 호출합니다.
   - CreatePolicyVersion

고객 관리형 정책의 기본 버전을 설정하려면(AWS API)

1. (선택 사항) 관리형 정책 목록을 보려면 다음 작업을 호출합니다.
   - ListPolicies
2. 고객 관리형 정책의 기본 버전을 설정하려면 다음 작업을 호출합니다.
   - SetDefaultPolicyVersion

고객 관리형 정책의 한 버전을 삭제하려면(AWS API)

1. (선택 사항) 관리형 정책 목록을 보려면 다음 작업을 호출합니다.
   - ListPolicies

2. 고객 관리형 정책을 삭제하려면 다음 작업을 호출합니다.

   - DeletePolicyVersion

IAM 정책 삭제

AWS Management 콘솔, AWS Command Line Interface(AWS CLI) 또는 IAM API를 사용하여 IAM 정책을 삭제할 수 있습니다.

관리형 정책과 인라인 정책의 차이점에 대한 자세한 내용은 관리형 정책과 인라인 정책 (p. 357) 단원을 참조하십시오.

IAM 정책에 대한 일반적인 내용은 정책 및 권한 (p. 349) 단원을 참조하십시오.

정책 크기 제한 및 기타 할당량에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

주제

정책 액세스 보기

정책을 삭제하기 전에 최근 서비스 수준 활동을 검토해야 합니다. 이 기능은 사용 중인 보안 주체(사람 또는 애플리케이션)의 액세스 권한을 제거하지 않으려는 경우 중요합니다. 서비스에서 마지막으로 액세스한 데이터 보기에 대한 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

IAM 정책 삭제(콘솔)

고객 관리형 정책은 삭제하여 AWS 계정에서 제거할 수 있습니다. 단, AWS 관리형 정책은 삭제할 수 없습니다.

고객 관리형 정책을 삭제하려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 삭제할 고객 관리형 정책 옆의 확인란을 선택합니다. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. Policy actions(정책 작업)을 선택한 후 삭제를 선택합니다.
5. 정책을 정말로 삭제할 것인지 다시 한 번 묻는 메시지가 나오면 확인 후 삭제를 선택합니다.

그룹, 사용자 또는 역할의 인라인 정책을 삭제하려면(콘솔)

1. 탐색 창에서 그룹, 사용자 또는 역할을 선택합니다.
2. 정책을 삭제하려는 그룹, 사용자 또는 역할 이름을 선택합니다. 그런 다음 권한 탭을 선택합니다. 사용자 또는 역할을 선택한 경우 정책을 확장합니다.
3. 그룹에서 인라인 정책을 삭제하려면 Remove Policy(정책 제거)를 선택합니다. 사용자 또는 역할에서 인라인 정책을 삭제하려면 X를 선택합니다.

IAM 정책 삭제(AWS CLI)

AWS Command Line Interface에서 고객 관리형 정책을 삭제할 수 있습니다.

고객 관리형 정책을 삭제하려면(AWS CLI)

1. (선택 사항)정책에 대한 정보를 보려면 다음 명령을 실행합니다.
   - 관리형 정책의 목록 보기: list-policies
   - 관리형 정책에 대한 세부 정보 가져오기: get-policy
2. (선택 사항) 정책과 자격 증명 간의 관계에 대해 확인하려면 다음 명령을 실행합니다.
   - 관리형 정책이 연결된 자격 증명(사용자, 그룹 및 역할)의 목록을 보려면 다음 명령을 실행합니다.
     - list-entities-for-policy
   - 자격 증명(사용자, 그룹 또는 역할)에 연결된 관리형 정책의 목록을 보려면 다음 명령 중 하나를 실행합니다.
     - list-attached-user-policies
     - list-attached-group-policies
     - list-attached-role-policies
3. 고객 관리형 정책을 삭제하려면 다음 명령을 실행합니다.
   - delete-policy

인라인 정책을 삭제하려면(AWS CLI)

1. (선택 사항) 자격 증명(사용자, 그룹 또는 역할)에 연결된 모든 인라인 정책의 목록을 보려면 다음 명령 중 하나를 사용합니다.
   - aws iam list-user-policies
   - aws iam list-group-policies
   - aws iam list-role-policies
2. (선택 사항) 자격 증명(사용자, 그룹 또는 역할)에 포함된 인라인 정책 문서를 가져오려면 다음 명령 중 하나를 사용합니다.
   - aws iam get-user-policy
   - aws iam get-group-policy
   - aws iam get-role-policy
3. 자격 증명(사용자, 그룹 또는 서비스 연결 역할 (p. 175)이 아닌 역할)에서 인라인 정책을 삭제하려면 다음 명령 중 하나를 사용합니다.
   - aws iam delete-user-policy
   - aws iam delete-group-policy
   - aws iam delete-role-policy

IAM 정책 삭제(AWS API)

AWS API를 사용하여 고객 관리형 정책을 삭제할 수 있습니다.

고객 관리형 정책을 삭제하려면(AWS API)

1. (선택 사항)정책에 대한 정보를 보려면 다음 작업을 호출합니다.
   - 관리형 정책의 목록 보기: ListPolicies

- 관리형 정책에 대한 세부 정보 가져오기: GetPolicy

2. (선택 사항) 정책과 자격 증명 간의 관계에 대해 확인하려면 다음 작업을 호출합니다.
   - 관리형 정책이 연결된 자격 증명(사용자, 그룹 및 역할)의 목록을 보려면 다음 작업을 호출합니다.
     - ListEntitiesForPolicy
   - 자격 증명(사용자, 그룹 또는 역할)에 연결된 관리형 정책의 목록을 보려면 다음 작업 중 하나를 호출합니다.
     - ListAttachedUserPolicies
     - ListAttachedGroupPolicies
     - ListAttachedRolePolicies
3. 고객 관리형 정책을 삭제하려면 다음 작업을 호출합니다.
   - DeletePolicy

인라인 정책을 삭제하려면(AWS API)

1. (선택 사항) 자격 증명(사용자, 그룹 또는 역할)에 연결된 모든 인라인 정책의 목록을 보려면 다음 작업 중 하나를 호출합니다.
   - ListUserPolicies
   - ListGroupPolicies
   - ListRolePolicies
2. (선택 사항) 자격 증명(사용자, 그룹 또는 역할)에 포함된 인라인 정책 문서를 가져오려면 다음 작업 중 하나를 호출합니다.
   - GetUserPolicy
   - GetGroupPolicy
   - GetRolePolicy
3. 인라인 정책을 자격 증명(사용자, 그룹 또는 서비스 연결 역할 (p. 175)이 아닌 역할)에서 삭제하려면 다음 작업 중 하나를 호출합니다.
   - DeleteUserPolicy
   - DeleteGroupPolicy
   - DeleteRolePolicy

서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화

IAM 또는 AWS Organizations의 엔터티 또는 정책에 대해 서비스에서 마지막으로 액세스한 데이터를 볼 수 있습니다. 이 데이터는 계정의 IAM 정책 또는 엔터티(사용자 또는 역할)에 대해 제공됩니다. IAM 데이터는 IAM 엔터티가 마지막으로 액세스를 시도한 허용된 서비스 및 그 시간에 대한 정보를 포함합니다. IAM에 대해 서비스에서 마지막으로 액세스한 데이터를 보는 방법 및 보고서에 대해 자세히 알아보려면 IAM에 대해 서비스에서 마지막으로 액세스한 데이터 보기 (p. 472) 단원을 참조하십시오.

마스터 계정 자격 증명을 사용하여 로그인할 경우 AWS Organizations 엔터티 또는 정책에 대해 서비스에서 마지막으로 액세스한 데이터를 볼 수도 있습니다. AWS Organizations 엔터티는 조직 루트, 조직 단위(OU) 또는 계정을 포함합니다. 조직 서비스에서 마지막으로 액세스한 데이터에는 조직 계정의 보안 주체가 마지막으로 액세스를 시도한 허용된 서비스 및 그 시간에 대한 정보가 포함됩니다. AWS Organizations에 대해 서비스에서 마지막으로 액세스한 데이터를 보는 방법 및 보고서에 대해 자세히 알아보려면 조직에 대해 서비스에서 마지막으로 액세스한 데이터 보기 (p. 474) 단원을 참조하십시오.

서비스에서 마지막으로 액세스한 데이터를 사용하여 정책을 세분화하고 엔터티가 사용하는 서비스에 대해서만 액세스를 허용할 수 있습니다. 그러면 최소 권한 (p. 61) 모범 사례를 더 효과적으로 준수할 수 있습니다.

서비스에서 마지막으로 액세스한 데이터를 사용하여 IAM 엔터티 또는 조직 엔터티에 부여할 권한을 결정하는 데 대한 예제 시나리오는 서비스에서 마지막으로 액세스한 데이터를 사용하는 예제 시나리오 (p. 478) 단원을 참조하십시오.

주제

알아야 할 것들

서비스에서 마지막으로 액세스한 보고서의 데이터를 사용하여 IAM 엔터티 또는 조직 엔터티의 권한을 변경하려면 먼저 데이터에 대한 다음 세부 정보를 검토하십시오.

- 보고 기간 – 최근 활동은 IAM 콘솔에서 일반적으로 4시간 이내에 나타납니다. IAM은 지난 365일 동안의 활동을 보고합니다. 단, 해당 지역에서 이 기능을 지원한 지 1년 미만인 경우 더 적을 수 있습니다. 자세한 내용은 데이터가 추적되는 리전 (p. 471) 단원을 참조하십시오.
- 보고서 소유자 – 보고서를 생성하는 보안 주체만 보고서 세부 정보를 볼 수 있습니다. 즉 AWS Management 콘솔에서 데이터를 볼 때 데이터가 생성 및 로드될 때까지 기다려야 할 수 있습니다. AWS CLI 또는 AWS API를 사용하여 보고서 세부 정보를 가져오는 경우 자격 증명이 보고서를 생성한 보안 주체의 자격 증명과 일치해야 합니다. 역할 또는 연동 사용자에 대해 임시 자격 증명을 사용하는 경우 동일한 세션 중에 보고서를 생성하고 검색해야 합니다. 위임된 역할 세션 보안 주체에 대한 자세한 내용은 AWS JSON 정책 요소: Principal (p. 589) 단원을 참조하십시오.
- PassRole – `iam:PassRole` 작업이 추적되지 않습니다.
- 인증된 IAM 엔터티 – IAM 데이터에는 계정의 인증된 IAM 엔터티(사용자 또는 역할)만 포함됩니다. 조직 데이터에는 지정된 조직 엔터티의 인증된 보안 주체(IAM 사용자, IAM 역할 또는 AWS 계정 루트 사용자)만 포함됩니다. 인증되지 않은 시도는 데이터에 포함되지 않습니다.
- IAM 정책 유형 – IAM 데이터에는 IAM 엔터티의 정책이 허용하는 서비스가 포함됩니다. 이러한 정책은 역할에 연결되거나 사용자에게 직접 또는 그룹을 통해 연결됩니다. 다른 정책 유형에서 허용하는 액세스는 보고서에 포함되어 있지 않습니다. 제외된 정책 유형에는 리소스 기반 정책, 액세스 제어 목록, AWS Organizations SCP, IAM 권한 경계 및 세션 정책이 있습니다. 다른 정책 유형이 액세스를 허용하거나 거부하는 방법을 알아보려면 정책 평가 로직 (p. 622) 단원을 참조하십시오.
- 조직 정책 유형 – AWS Organizations 데이터에는 조직 엔터티의 상속된 서비스 제어 정책(SCP)이 허용하는 서비스만 포함됩니다. SCP는 루트, OU 또는 계정에 연결된 정책입니다. 다른 정책 유형에서 허용하는 액세스는 보고서에 포함되어 있지 않습니다. 제외된 정책 유형에는 자격 증명 기반 정책, 리소스 기반 정책, 액세스 제어 목록, IAM 권한 경계 및 세션 정책이 있습니다. 다른 정책 유형이 액세스를 허용하거나 거부하는 방법을 알아보려면 정책 평가 로직 (p. 622) 단원을 참조하십시오.
- 정책 ID 지정 – AWS CLI 또는 AWS API를 사용하여 조직에서 서비스에서 마지막으로 액세스한 데이터에 대한 보고서를 생성할 때 선택적으로 정책 ID를 지정할 수 있습니다. 그러면 생성되는 보고서는 해당 정책이 허용하는 서비스에 대한 데이터만 포함합니다. 이 데이터에는 지정된 조직 엔터티 또는 엔터티 하위의 가장 최근 계정 활동이 포함됩니다. 자세한 내용은 aws iam generate-organizations-access-report 또는 GenerateOrganizationsAccessReport를 참조하십시오.
- 조직 마스터 계정 – 서비스에서 마지막으로 액세스한 데이터를 보려면 조직의 마스터 계정 자격 증명을 사용하여 로그인해야 합니다. IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 마스터 계정에 대한 데이터를 보도록 선택할 수 있습니다. 마스터 계정은 SCP에 의해 제한을 받지 않으므로 생성되는 보고서에는 모든

AWS 서비스가 나열됩니다. CLI 또는 API에 정책 ID를 지정할 경우 해당 정책이 무시됩니다. 각 서비스에 대해, 보고서가 마스터 계정에 대한 보고서만 포함합니다. 그러나 다른 조직 개체에 대한 보고서는 마스터 계정의 활동에 대한 데이터를 반환하지 않습니다.

- 조직 설정 – 관리자는 조직에 대한 데이터를 생성하려면 조직 루트에서 SCP를 활성화해야 합니다.

필요한 권한

AWS Management 콘솔을 사용하여 서비스에서 마지막으로 액세스한 데이터를 보려면 필요한 권한을 부여하는 정책이 있어야 합니다.

IAM 데이터에 대한 권한

IAM 콘솔을 사용하여 IAM 사용자, 역할 또는 정책에 대해 서비스에서 마지막으로 액세스한 데이터를 보려면 다음 작업을 포함하는 정책이 있어야 합니다.

- `iam:GenerateServiceLastAccessedDetails`
- `iam:Get*`
- `iam:List*`

이러한 권한을 사용하면 사용자가 다음을 확인할 수 있습니다.

- 관리형 정책에 연결된 사용자, 그룹 또는 역할
- 사용자 또는 역할이 액세스할 수 있는 서비스
- 서비스에 마지막으로 액세스한 시간

AWS CLI 또는 AWS API를 사용하여 IAM에 대해 서비스에서 마지막으로 액세스한 데이터를 보려면 사용하려는 작업과 일치하는 권한이 있어야 합니다.

- `iam:GenerateServiceLastAccessedDetails`
- `iam:GetServiceLastAccessedDetails`
- `iam:GetServiceLastAccessedDetailsWithEntities`
- `iam:ListPoliciesGrantingServiceAccess`

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.은 IAM 서비스에서 마지막으로 액세스한 데이터 보기를 허용합니다. 또한 모든 IAM에 대한 읽기 전용 액세스를 허용합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.

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

AWS Organizations 데이터에 대한 권한

IAM 콘솔을 사용하여 조직의 루트, OU 또는 계정 엔터티에 대한 보고서를 보려면 다음 작업을 포함하는 정책이 있어야 합니다.

- iam:GenerateOrganizationsAccessReport
- iam:GetOrganizationsAccessReport
- organizations:DescribeAccount
- organizations:DescribeOrganization
- organizations:DescribeOrganizationalUnit
- organizations:DescribePolicy
- organizations:ListChildren
- organizations:ListParents
- organizations:ListPoliciesForTarget
- organizations:ListRoots
- organizations:ListTargetsForPolicy

AWS CLI 또는 AWS API를 사용하여 조직에 대해 서비스에서 마지막으로 액세스한 데이터를 보려면 다음 작업을 포함하는 정책이 있어야 합니다.

- iam:GenerateOrganizationsAccessReport
- iam:GetOrganizationsAccessReport
- organizations:DescribePolicy
- organizations:ListChildren
- organizations:ListParents
- organizations:ListPoliciesForTarget
- organizations:ListRoots
- organizations:ListTargetsForPolicy

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.는 조직에 대한 마지막으로 액세스한 데이터 보기를 허용합니다. 또한 모든 조직에 대한 읽기 전용 액세스를 허용합니다.이 정책은 콘솔에서 이 작업을 완료하는 데 필요한 권한도 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:GenerateOrganizationsAccessReport",
            "iam:GetOrganizationsAccessReport",
            "organizations:Describe*",
            "organizations:List*"
        ],
        "Resource": "*"
    }
}
```

iam:OrganizationsPolicyId (p. 665) 조건 키를 사용하여 특정 조직 정책에 대해서만 보고서 생성을 허용할 수도 있습니다. 정책에 대한 예는 IAM: 조직 정책에 대해 서비스에서 마지막으로 액세스한 데이터 보기 (p. 425)을 참조하십시오.

IAM 및 조직 엔터티 작업 문제 해결

일부의 경우, AWS Management 콘솔 서비스에서 마지막으로 액세스한 데이터 테이블이 비어 있을 수 있습니다. 혹은 AWS CLI 또는 AWS API 요청이 빈 데이터 세트 또는 null 필드를 반환할 수 있습니다. 이러한 경우 다음 문제를 검토하십시오.

- IAM 사용자의 경우 사용자가 직접 또는 그룹 멤버십을 통해 인라인 또는 관리형 정책이 하나 이상 연결되어 있는지 확인합니다.
- IAM 그룹의 경우 그룹에 인라인 또는 관리형 정책이 하나 이상 연결되어 있는지 확인합니다.
- IAM 그룹의 경우 보고서는 그룹 정책을 사용하여 서비스에 액세스한 멤버에 대해서만 서비스에서 마지막으로 액세스한 데이터를 반환합니다. 멤버가 다른 정책을 사용했는지 여부를 확인하려면 해당 사용자에 대해 서비스에서 마지막으로 액세스한 데이터를 검토하십시오.
- IAM 역할의 경우 역할에 인라인 또는 관리형 정책이 하나 이상 연결되어 있는지 확인합니다.
- IAM 엔터티(사용자 또는 역할)의 경우 해당 엔터티의 사용 권한에 영향을 줄 수 있는 다른 정책 유형을 검토합니다. 여기에는 리소스 기반 정책, 액세스 제어 목록, AWS Organizations 정책, IAM 권한 경계 또는 세션 정책이 있습니다. 자세한 정보는 정책 유형 (p. 349) 또는 단일 계정 내에서 정책 평가 (p. 623) 단원을 참조하십시오.
- IAM 정책의 경우 지정된 관리형 정책이 하나 이상의 사용자, 멤버가 있는 그룹 또는 역할에 연결되어 있는지 확인합니다.
- 조직 엔터티(루트, OU 또는 계정)의 경우 조직 마스터 계정 자격 증명을 사용하여 로그인되어 있는지 확인합니다.
- 조직 루트에서 SCP가 활성화되어 있는지 확인합니다.

변경을 수행할 때 IAM 콘솔 보고서에 작업이 나타날 때까지 최소 4시간을 기다리십시오. AWS CLI 또는 AWS API를 사용하는 경우 업데이트된 데이터를 표시하려면 새 보고서를 생성해야 합니다.

데이터가 추적되는 리전

AWS는 대부분의 리전에서 서비스에서 마지막으로 액세스한 데이터를 수집합니다. 데이터는 최대 365일 동안 저장됩니다. AWS에서 리전을 추가하면 AWS에서 각 리전의 데이터 추적을 시작한 날짜와 함께 해당 리전이 다음 표에 추가됩니다.

리전 이름	Region	추적 시작 날짜
미국 동부(오하이오)	us-east-2	2017년 10월 27일
미국 동부(버지니아 북부)	us-east-1	2015년 10월 1일
미국 서부(캘리포니아 북부 지역)	us-west-1	2015년 10월 1일
미국 서부(오레곤)	us-west-2	2015년 10월 1일
아시아 태평양(도쿄)	ap-northeast-1	2015년 10월 1일
아시아 태평양(서울)	ap-northeast-2	2016년 1월 6일
아시아 태평양(싱가포르)	ap-southeast-1	2015년 10월 1일
아시아 태평양(시드니)	ap-southeast-2	2015년 10월 1일
아시아 태평양(뭄바이)	ap-south-1	2016년 6월 27일
아시아 태평양(홍콩)	ap-east-1	2019년 4월 24일
중동(바레인)	me-south-1	2019년 7월 29일
캐나다(중부)	ca-central-1	2017년 10월 28일
유럽(프랑크푸르트)	eu-central-1	2015년 10월 1일
유럽(스톡홀름)	eu-north-1	2018년 12월 12일
유럽(아일랜드)	eu-west-1	2015년 10월 1일

리전 이름	Region	추적 시작 날짜
유럽(런던)	eu-west-2	2017년 10월 28일
유럽(파리)	eu-west-3	2017년 12월 18일
남아메리카(상파울루)	sa-east-1	2015년 12월 11일

앞의 표에 나와 있지 않은 리전은 서비스에서 마지막으로 액세스한 데이터를 아직 제공하지 않습니다.

IAM에 대해 서비스에서 마지막으로 액세스한 데이터 보기

IAM, AWS Management 콘솔, AWS CLI 또는 AWS API를 사용하여 서비스에서 마지막으로 액세스한 데이터를 볼 수 있습니다. 서비스에서 마지막으로 액세스한 데이터에 대한 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

IAM에서 각 리소스 유형에 대한 데이터를 볼 수 있습니다. 각각의 경우 데이터는 지정된 보고 기간 동안 허용된 서비스를 포함합니다.

- 사용자 – 사용자가 허용된 각 서비스에 액세스하려고 시도한 마지막 시간을 표시합니다.
- 그룹 – 그룹 멤버가 허용된 각 서비스에 액세스하려고 시도한 마지막 시간에 대한 정보를 표시합니다. 또한 이 보고서에는 액세스를 시도한 총 멤버 수가 포함됩니다.
- 역할 – 해당 역할이 허용된 각 서비스에 액세스하려고 시도한 마지막 시간을 표시합니다.
- 정책 – 사용자 또는 역할이 허용된 각 서비스에 액세스하려고 시도한 마지막 시간에 대한 정보를 표시합니다. 또한 이 보고서에는 액세스를 시도한 총 엔터티 수가 포함됩니다.

> **Note**
>
> IAM의 리소스에 대한 액세스 데이터를 보려면 먼저 보고 기간, 보고된 엔터티 및 데이터에 대해 평가된 정책 유형을 이해해야 합니다. 자세한 내용은 the section called “알아야 할 것들” (p. 468) 단원을 참조하십시오.

IAM 데이터 보기(콘솔)

IAM 콘솔의 Access Advisor 탭에서 IAM에 대해 서비스에서 마지막으로 액세스한 데이터를 볼 수 있습니다.

IAM 데이터를 보려면(콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 그룹, 사용자, 역할 또는 정책을 선택합니다.
3. 사용자, 그룹, 역할 또는 정책 이름을 선택하여 요약 페이지를 열고 액세스 관리자 탭을 선택합니다. 선택한 리소스를 기반으로 다음 정보를 확인합니다.

   - 그룹 – 그룹 멤버(사용자)가 액세스할 수 있는 서비스 목록, 멤버가 마지막으로 서비스에 액세스한 시간, 사용된 그룹 정책 및 요청한 그룹 멤버를 표시합니다. 정책의 이름을 선택하여 정책이 관리형 정책인지 아니면 인라인 그룹 정책인지 확인합니다. 그룹 멤버의 이름을 선택하여 그룹의 모든 멤버를 확인하고 마지막으로 서비스에 액세스한 시간을 확인합니다.
   - 사용자 – 사용자가 액세스할 수 있는 서비스 목록, 서비스에 마지막으로 액세스한 시간 및 사용된 정책 목록을 표시합니다. 정책이 관리되는지 여부를 확인할 정책 이름, 인라인 사용자 정책 또는 사용자가 속한 그룹의 인라인 정책을 확인합니다.
   - 역할 – 역할이 액세스할 수 있는 서비스 목록, 서비스에 마지막으로 액세스한 역할 및 사용된 정책 목록을 표시합니다. 정책의 이름을 선택하여 정책이 관리형 정책인지 아니면 인라인 역할 정책인지 확인합니다.

- 정책 – 정책에 허용된 작업, 서비스에 마지막으로 액세스한 정책 및 해당 정책을 사용한 엔터티(사용자 또는 역할)가 포함된 서비스 목록을 표시합니다. 엔터티의 이름을 선택하여 어떤 엔터티에 이 정책이 연결되어 있는지 그리고 마지막으로 서비스에 액세스한 시간을 확인합니다.

IAM 데이터 보기(AWS CLI)

AWS CLI를 사용하여 AWS 서비스에 액세스하기 위해 IAM 리소스가 사용된 마지막 시간에 대한 데이터를 검색할 수 있습니다. IAM 리소스는 사용자, 그룹, 역할 또는 정책입니다.

IAM 데이터를 보려면(AWS CLI)

1. 보고서를 생성합니다. 요청에는 보고서가 필요한 IAM 리소스(사용자, 그룹, 역할 또는 정책)의 ARN이 포함되어야 합니다. 작업이 완료될 때까지 `get-service-last-accessed-details` 및 `get-service-last-accessed-details-with-entities` 작업에서 `job-status`를 모니터링하기 위해 사용할 수 있는 `job-id`를 반환합니다.

   - aws iam generate-service-last-accessed-details
2. 이전 단계의 `job-id` 파라미터를 사용하여 보고서에 대한 세부 정보를 검색합니다.

   - aws iam get-service-last-accessed-details

   이 작업은 `generate-service-last-accessed-details` 작업에서 요청한 리소스 유형에 따라 다음 정보를 반환합니다.

   - 사용자 – 지정한 사용자가 액세스할 수 있는 서비스 목록을 반환합니다. 각 서비스에 대해 작업은 사용자의 마지막 시도 날짜 및 시간과 사용자의 ARN을 반환합니다.
   - 그룹 – 그룹에 연결된 정책을 사용하여 지정된 그룹의 멤버가 액세스할 수 있는 서비스 목록을 반환합니다. 각 서비스에 대해 작업은 그룹 멤버(사용자)가 마지막으로 시도한 날짜와 시간을 반환합니다. 또한 해당 사용자의 ARN과 서비스에 액세스하려고 시도한 그룹 멤버의 총 수를 반환합니다. 모든 멤버 목록을 반환하려면 GetServiceLastAccessedDetailsWithEntities 작업을 사용합니다.
   - 역할 – 지정한 역할이 액세스할 수 있는 서비스 목록을 반환합니다. 각 서비스에 대해 작업은 역할의 마지막 시도 날짜 및 시간과 역할의 ARN을 반환합니다.
   - 정책 – 지정된 정책으로 액세스할 수 있는 서비스 목록을 반환합니다. 각 서비스에 대해 작업은 엔터티(사용자 또는 역할)가 정책을 사용하여 마지막으로 서비스에 액세스하려고 시도한 날짜와 시간을 반환합니다. 또한 엔터티의 ARN과 액세스를 시도한 엔터티의 총 수를 반환합니다.
3. 특정 서비스에 액세스하기 위해 그룹 또는 정책 권한을 사용하는 엔터티에 대해 자세히 알아봅니다. 이 작업은 각 엔터티의 ARN, ID, 이름, 경로, 유형(사용자 또는 역할) 및 마지막으로 서비스에 액세스하려고 시도한 엔터티의 목록을 반환합니다. 사용자와 역할에 대해 이 작업을 사용할 수도 있지만 해당 엔터티에 대한 정보만 반환합니다.

   - aws iam get-service-last-accessed-details-with-entities
4. 특정 서비스에 액세스하기 위해 자격 증명(사용자, 그룹 또는 역할)이 사용하는 자격 기반 정책에 대해 자세히 알아봅니다. 자격 증명 및 서비스를 지정한 경우 이 작업은 해당 자격 증명이 지정된 서비스에 액세스하는 데 사용할 수 있는 권한 정책 목록을 반환합니다. 이 작업은 정책의 현재 상태를 제공하며 생성된 보고서에 의존하지 않습니다. 또한 리소스 기반 정책, 액세스 제어 목록, AWS Organizations 정책, IAM 권한 경계 또는 세션 정책 등의 다른 정책 유형을 반환하지 않습니다. 자세한 내용은 정책 유형 (p. 349) 또는 단일 계정 내에서 정책 평가 (p. 623) 단원을 참조하십시오.

   - aws iam list-policies-granting-service-access

IAM 데이터 보기(AWS API)

AWS API를 사용하여 AWS 서비스에 액세스하기 위해 IAM 리소스가 사용된 마지막 시간에 대한 데이터를 검색할 수 있습니다. IAM 리소스는 사용자, 그룹, 역할 또는 정책입니다.

IAM 데이터를 보려면(AWS API)

1. 보고서를 생성합니다. 요청에는 보고서가 필요한 IAM 리소스(사용자, 그룹, 역할 또는 정책)의 ARN이 포함되어야 합니다. 작업이 완료될 때까지 `GetServiceLastAccessedDetails` 및 `GetServiceLastAccessedDetailsWithEntities` 작업에서 `JobStatus`를 모니터링하기 위해 사용할 수 있는 `JobId`를 반환합니다.

   - GenerateServiceLastAccessedDetails
2. 이전 단계의 `JobId` 파라미터를 사용하여 보고서에 대한 세부 정보를 검색합니다.

   - GetServiceLastAccessedDetails

   이 작업은 `GenerateServiceLastAccessedDetails` 작업에서 요청한 리소스 유형에 따라 다음 정보를 반환합니다.

   - 사용자 – 지정한 사용자가 액세스할 수 있는 서비스 목록을 반환합니다. 각 서비스에 대해 작업은 사용자의 마지막 시도 날짜 및 시간과 사용자의 ARN을 반환합니다.
   - 그룹 – 그룹에 연결된 정책을 사용하여 지정된 그룹의 멤버가 액세스할 수 있는 서비스 목록을 반환합니다. 각 서비스에 대해 작업은 그룹 멤버(사용자)가 마지막으로 시도한 날짜와 시간을 반환합니다. 또한 해당 사용자의 ARN과 서비스에 액세스하려고 시도한 그룹 멤버의 총 수를 반환합니다. 모든 멤버 목록을 반환하려면 GetServiceLastAccessedDetailsWithEntities 작업을 사용합니다.
   - 역할 – 지정한 역할이 액세스할 수 있는 서비스 목록을 반환합니다. 각 서비스에 대해 작업은 역할의 마지막 시도 날짜 및 시간과 역할의 ARN을 반환합니다.
   - 정책 – 지정된 정책으로 액세스할 수 있는 서비스 목록을 반환합니다. 각 서비스에 대해 작업은 엔터티(사용자 또는 역할)가 정책을 사용하여 마지막으로 서비스에 액세스하려고 시도한 날짜와 시간을 반환합니다. 또한 엔터티의 ARN과 액세스를 시도한 엔터티의 총 수를 반환합니다.
3. 특정 서비스에 액세스하기 위해 그룹 또는 정책 권한을 사용하는 엔터티에 대해 자세히 알아봅니다. 이 작업은 각 엔터티의 ARN, ID, 이름, 경로, 유형(사용자 또는 역할) 및 마지막으로 서비스에 액세스하려고 시도한 엔터티의 목록을 반환합니다. 사용자와 역할에 대해 이 작업을 사용할 수도 있지만 해당 엔터티에 대한 정보만 반환합니다.

   - GetServiceLastAccessedDetailsWithEntities
4. 특정 서비스에 액세스하기 위해 자격 증명(사용자, 그룹 또는 역할)이 사용하는 자격 기반 정책에 대해 자세히 알아봅니다. 자격 증명 및 서비스를 지정한 경우 이 작업은 해당 자격 증명이 지정된 서비스에 액세스하는 데 사용할 수 있는 권한 정책 목록을 반환합니다. 이 작업은 정책의 현재 상태를 제공하며 생성된 보고서에 의존하지 않습니다. 또한 리소스 기반 정책, 액세스 제어 목록, AWS Organizations 정책, IAM 권한 경계 또는 세션 정책 등의 다른 정책 유형을 반환하지 않습니다. 자세한 내용은 정책 유형 (p. 349) 또는 단일 계정 내에서 정책 평가 (p. 623) 단원을 참조하십시오.

   - ListPoliciesGrantingServiceAccess

조직에 대해 서비스에서 마지막으로 액세스한 데이터 보기

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWS Organizations에 대해 서비스에서 마지막으로 액세스한 데이터를 볼 수 있습니다. 데이터, 필요 권한, 문제 해결, 지원되는 리전에 대한 중요 정보는 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

AWS Organizations 마스터 계정 자격 증명을 사용하여 IAM 콘솔에 로그인하면 조직의 엔터티에 대한 데이터를 볼 수 있습니다. 조직 엔터티에는 조직 루트, 조직 단위(OU) 및 계정이 포함됩니다. 또한 IAM 콘솔을 사용하여 조직의 모든 서비스 제어 정책(SCP)에 대한 데이터를 볼 수 있습니다. IAM에는 SCP가 해당 엔터티에 적용되도록 허용하는 서비스의 목록이 표시됩니다. 각 서비스에 대해, 선택한 조직 엔터티 또는 엔터티 하위에 대한 가장 최근의 계정 활동 데이터를 볼 수 있습니다.

마스터 계정 자격 증명으로 AWS CLI 또는 AWS API를 사용하면 조직의 모든 엔터티 또는 정책에 대한 데이터 보고서를 생성할 수 있습니다. 엔터티에 대한 프로그래밍 방식 보고서는 SCP가 엔터티에 적용되도록 허

용하는 서비스의 목록을 포함합니다. 각 서비스에 대해, 보고서는 지정된 조직 엔터티 또는 엔터티 하위 트리의 계정에 대한 가장 최근의 활동을 포함합니다.

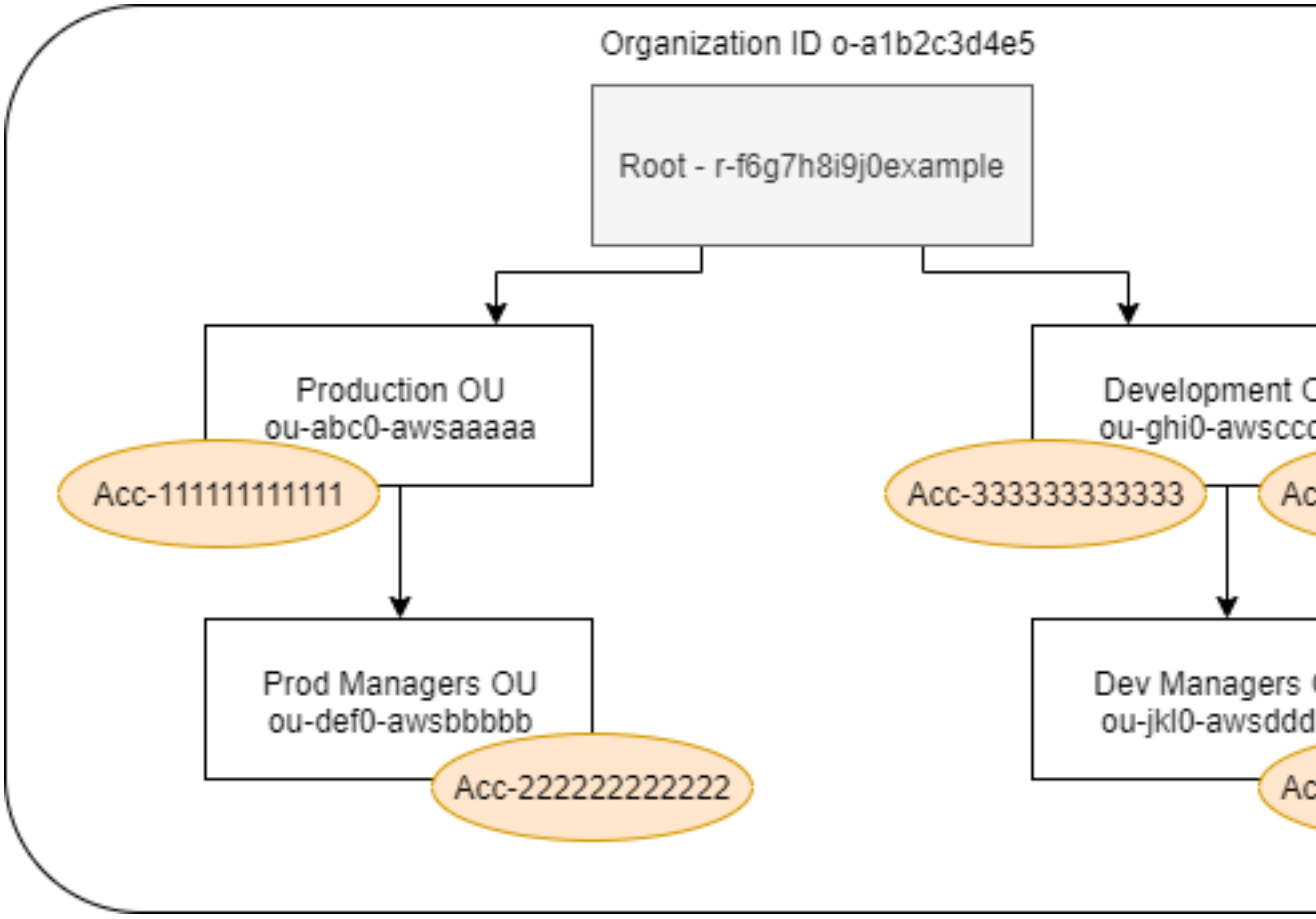
정책에 대한 프로그래밍 방식 보고서를 생성할 때 조직 엔터티를 지정해야 합니다. 이 보고서는 지정된 SCP가 허용하는 서비스의 목록을 포함합니다. 각 서비스에 대해, 해당 정책이 권한을 부여한 엔터티 또는 엔터티 하위의 가장 최근 계정 활동이 포함됩니다. 자세한 내용은 aws iam generate-organizations-access-report 또는 GenerateOrganizationsAccessReport를 참조하십시오.

보고서를 보려면 마스터 계정 요건 및 데이터, 보고 주기, 보고된 개체 및 평가된 정책 유형을 이해하고 있어야 합니다. 자세한 내용은 the section called “알아야 할 것들” (p. 468) 단원을 참조하십시오.

AWS Organizations 엔터티 경로 이해

AWS CLI 또는 AWS API를 사용하여 AWS Organizations 액세스 보고서를 생성하는 경우 엔터티 경로를 지정해야 합니다. 경로는 조직 엔터티 구조의 텍스트 표현입니다.

조직의 알려진 구조를 사용하여 엔터티 경로를 작성할 수 있습니다. 예를 들어 AWS Organizations에 다음과 같은 조직 구조가 있다고 가정합니다.



Dev Managers(개발자 관리자) OU의 경로는 조직의 ID, 루트 및 경로에 있는 모든 OU(해당 OU 포함)를 사용하여 작성됩니다.

```
o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-awsddddd
```

프로덕션 OU의 계정 경로는 조직의 ID, 루트, OU 및 계정 번호를 사용하여 작성됩니다.

```
o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-abc0-awsaaaaa/111111111111
```

Note

조직 ID는 전역적으로 고유하지만 OU ID와 루트 ID는 조직 내에서만 고유합니다. 즉, 두 조직이 동일한 조직 ID를 공유하지 않습니다. 그러나 다른 조직에는 사용자 ID와 동일한 OU 또는 루트가 있을 수 있습니다. OU 또는 루트를 지정할 때는 항상 조직 ID를 포함하는 것이 좋습니다.

조직 데이터 보기(콘솔)

IAM 콘솔을 사용하여 루트, OU, 계정 또는 정책에 대해 서비스에서 마지막으로 액세스한 데이터를 볼 수 있습니다.

루트에 대한 데이터를 보려면(콘솔)

1. 조직 마스터 계정 자격 증명을 사용하여 AWS Management 콘솔에 로그인하고 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. Access reports(보고서 액세스) 섹션 아래의 탐색 창에서 Organization activity(조직 활동)를 선택합니다.
3. Organization activity(조직 활동) 페이지에서 루트를 선택합니다.
4. Details and activity(세부 정보 및 활동) 탭에서 Service access report(서비스 액세스 보고서) 섹션을 봅니다. 데이터에는 루트에 직접 연결된 정책이 허용하는 서비스의 목록이 포함됩니다. 이 데이터는 서비스에 마지막으로 액세스한 계정 및 그 시간을 보여줍니다. 서비스에 액세스한 보안 주체에 대한 세부 정보를 보려면 해당 계정의 관리자로 로그인하고 IAM 서비스에서 마지막으로 액세스한 데이터 (p. 472)를 봅니다.
5. Attached SCPs(연결된 SCP) 탭을 선택하여 루트에 연결된 서비스 제어 정책(SCP)의 목록을 봅니다. IAM에 각 정책이 연결된 대상 엔터티의 수가 표시됩니다. 이 정보를 사용하여 어느 SCP를 검토할지 결정할 수 있습니다.
6. SCP의 이름을 선택하여 해당 정책이 허용하는 모든 서비스를 봅니다. 각 서비스에 대해, 서비스에 마지막으로 액세스한 계정 및 그 시간을 봅니다.
7. AWS Organizations에서 편집을 선택하여 추가 세부 정보를 보고 조직 콘솔에서 SCP를 편집합니다. 자세한 내용은 AWS Organizations 사용 설명서의 SCP 업데이트를 참조하십시오.

OU 또는 계정에 대한 데이터를 보려면(콘솔)

1. 조직 마스터 계정 자격 증명을 사용하여 AWS Management 콘솔에 로그인하고 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. Access reports(보고서 액세스) 섹션 아래의 탐색 창에서 Organization activity(조직 활동)를 선택합니다.
3. Organization activity(조직 활동) 페이지에서 조직의 구조를 확장합니다. 그런 다음 OU의 이름 또는 마스터 계정을 제외하고 보려는 임의의 계정의 이름을 선택합니다.
4. Details and activity(세부 정보 및 활동) 탭에서 Service access report(서비스 액세스 보고서) 섹션을 봅니다. 데이터에는 OU 또는 계정 및 모든 해당 상위 항목에 연결된 SCP가 허용하는 서비스의 목록이 포함됩니다. 이 데이터는 서비스에 마지막으로 액세스한 계정 및 그 시간을 보여줍니다. 서비스에 액세스한 보안 주체에 대한 세부 정보를 보려면 해당 계정의 관리자로 로그인하고 IAM 서비스에서 마지막으로 액세스한 데이터 (p. 472)를 봅니다.
5. Attached SCPs(연결된 SCP) 탭을 선택하여 OU 또는 계정에 연결된 서비스 제어 정책(SCP)의 목록을 봅니다. IAM에 각 정책이 연결된 대상 엔터티의 수가 표시됩니다. 이 정보를 사용하여 어느 SCP를 검토할지 결정할 수 있습니다.
6. SCP의 이름을 선택하여 해당 정책이 허용하는 모든 서비스를 봅니다. 각 서비스에 대해, 서비스에 마지막으로 액세스한 계정 및 그 시간을 봅니다.
7. AWS Organizations에서 편집을 선택하여 추가 세부 정보를 보고 조직 콘솔에서 SCP를 편집합니다. 자세한 내용은 AWS Organizations 사용 설명서의 SCP 업데이트를 참조하십시오.

마스터 계정에 대한 데이터를 보려면(콘솔)

1. 조직 마스터 계정 자격 증명을 사용하여 AWS Management 콘솔에 로그인하고 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. Access reports(보고서 액세스) 섹션 아래의 탐색 창에서 Organization activity(조직 활동)를 선택합니다.
3. Organization activity(조직 활동) 페이지에서 조직의 구조를 확장하고 마스터 계정의 이름을 선택합니다.
4. Details and activity(세부 정보 및 활동) 탭에서 Service access report(서비스 액세스 보고서) 섹션을 봅니다. 데이터에는 모든 AWS 서비스의 목록이 포함됩니다. 마스터 계정은 SCP에 의해 제한되지 않습니다. 이 데이터는 계정이 서비스에 액세스했는지 여부와 마지막으로 액세스한 시간을 보여줍니다 . 서비스에 액세스한 보안 주체에 대한 세부 정보를 보려면 해당 계정의 관리자로 로그인하고 IAM 서비스에서 마지막으로 액세스한 데이터 (p. 472)를 봅니다.
5. Attached SCPs(연결된 SCP) 탭을 선택하여 연결된 SCP가 없음을 확인합니다(해당 계정이 마스터 계정이기 때문).

정책에 대한 데이터를 보려면(콘솔)

1. 조직 마스터 계정 자격 증명을 사용하여 AWS Management 콘솔에 로그인하고 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. Access reports(보고서 액세스) 섹션 아래의 탐색 창에서 Service control policies (SCPs)(서비스 제어 정책(SCP))를 선택합니다.
3. Service control policies (SCPs)(서비스 제어 정책(SCP)) 페이지에서 조직의 정책 목록을 봅니다. 각 정책이 연결된 대상 엔터티의 수를 볼 수 있습니다.
4. SCP의 이름을 선택하여 해당 정책이 허용하는 모든 서비스를 봅니다. 각 서비스에 대해, 서비스에 마지막으로 액세스한 계정 및 그 시간을 봅니다.
5. AWS Organizations에서 편집을 선택하여 추가 세부 정보를 보고 조직 콘솔에서 SCP를 편집합니다. 자세한 내용은 AWS Organizations 사용 설명서의 SCP 업데이트를 참조하십시오.

조직 데이터 보기(AWS CLI)

AWS CLI를 사용하여 조직 루트, OU, 계정 또는 정책에 대해 서비스에서 마지막으로 액세스한 데이터를 검색할 수 있습니다.

조직 서비스에서 마지막으로 액세스한 데이터를 보려면(AWS CLI)

1. 필요한 IAM 및 조직 권한이 있는 조직 마스터 계정 자격 증명을 사용하여 루트에 대해 SCP가 활성화되어 있는지 확인합니다. 자세한 내용은 알아야 할 것들 (p. 468) 단원을 참조하십시오.
2. 보고서를 생성합니다. 요청은 보고서를 작성할 조직 엔터티(루트, OU 또는 계정)의 경로를 포함해야 합니다. 선택적으로 `organization-policy-id` 파라미터를 포함하여 특정 정책에 대한 보고서를 볼 수 있습니다. 이 명령은 작업이 완료될 때까지 `get-organizations-access-report` 명령에 사용하여 `job-status`를 모니터링하기 위해 사용할 수 있는 `job-id`를 반환합니다.

   - aws iam generate-organizations-access-report
3. 이전 단계의 `job-id` 파라미터를 사용하여 보고서에 대한 세부 정보를 검색합니다.

   - aws iam get-organizations-access-report

   이 명령은 엔터티 멤버가 액세스할 수 있는 서비스의 목록을 반환합니다. 각 서비스에 대해, 계정 멤버에 의한 마지막 시도의 날짜 및 시간과 계정의 엔터티 경로가 반환됩니다. 또한 액세스 가능한 서비스의 총 개수와 액세스되지 않은 서비스의 수도 반환됩니다. 선택적으로 `organizations-policy-id` 파라미터를 지정한 경우 액세스 가능한 서비스는 지정된 정책이 허용하는 서비스입니다.

조직 데이터 보기(AWS API)

AWS API를 사용하여 조직 루트, OU, 계정 또는 정책에 대해 서비스에서 마지막으로 액세스한 데이터를 검색할 수 있습니다.

조직 서비스에서 마지막으로 액세스한 데이터를 보려면(AWS API)

1. 필요한 IAM 및 조직 권한이 있는 조직 마스터 계정 자격 증명을 사용하여 루트에 대해 SCP가 활성화되어 있는지 확인합니다. 자세한 내용은 알아야 할 것들 (p. 468) 단원을 참조하십시오.
2. 보고서를 생성합니다. 요청은 보고서를 작성할 조직 엔터티(루트, OU 또는 계정)의 경로를 포함해야 합니다. 선택적으로 `OrganizationsPolicyId` 파라미터를 포함하여 특정 정책에 대한 보고서를 볼 수 있습니다. 이 작업은 작업이 완료될 때까지 `GetOrganizationsAccessReport` 작업에서 `JobStatus`를 모니터링하기 위해 사용할 수 있는 `JobId`를 반환합니다.

   - GenerateOrganizationsAccessReport
3. 이전 단계의 `JobId` 파라미터를 사용하여 보고서에 대한 세부 정보를 검색합니다.

   - GetOrganizationsAccessReport

   이 작업은 엔터티 멤버가 액세스할 수 있는 서비스의 목록을 반환합니다. 각 서비스에 대해, 계정 멤버에 의한 마지막 시도의 날짜 및 시간과 계정의 엔터티 경로가 반환됩니다. 또한 액세스 가능한 서비스의 총 개수와 액세스되지 않은 서비스의 수도 반환됩니다. 선택적으로 `OrganizationsPolicyId` 파라미터를 지정한 경우 액세스 가능한 서비스는 지정된 정책이 허용하는 서비스입니다.

서비스에서 마지막으로 액세스한 데이터를 사용하는 예제 시나리오

서비스에서 마지막으로 액세스한 데이터를 사용하여 IAM 엔터티 또는 AWS Organizations 엔터티에 부여할 권한을 결정할 수 있습니다. 자세한 내용은 서비스에서 마지막으로 액세스한 데이터를 사용하여 권한 세분화 (p. 467) 단원을 참조하십시오.

> **Note**
>
> IAM 또는 AWS Organizations의 엔터티 또는 정책에 대한 액세스 데이터를 보려면 먼저 보고 기간, 보고된 엔터티 및 데이터에 대해 평가된 정책 유형을 이해해야 합니다. 자세한 내용은 the section called “알아야 할 것들” (p. 468) 단원을 참조하십시오.

회사에 적합한 액세스 가능성과 최소 권한 간에 적절한 균형을 유지하는 것은 관리자에게 달려 있습니다.

데이터를 사용하여 IAM 그룹의 권한 축소

서비스에서 마지막으로 액세스한 데이터를 사용하여 사용자에게 필요한 서비스만 포함하도록 IAM 그룹 권한을 줄일 수 있습니다. 이 방법은 서비스 수준에서 최소 권한을 부여 (p. 61)하는 데 있어 중요한 단계입니다.

예를 들어, Paulo Santos는 Example Corp.의 AWS 사용자 권한을 정의하는 관리자입니다. 이 회사는 AWS를 사용한 지 얼마 되지 않았기 때문에 소프트웨어 개발 팀에서 아직 사용할 AWS 서비스를 정의하지 않았습니다. Paulo는 팀에게 필요한 서비스에만 액세스할 수 있는 권한을 부여하려고 하지만, 아직 정의되지 않았기 때문에 일시적으로 파워 사용자 권한을 부여합니다. 그런 다음 그는 서비스에서 마지막으로 액세스한 데이터를 사용하여 그룹의 권한을 줄입니다.

Paulo는 다음 JSON 텍스트를 사용하여 `ExampleDevelopment` 관리 정책을 만듭니다. 그런 다음 이 정책을 `Development` 그룹에 연결하고 모든 개발자를 그룹에 추가합니다.

```
{

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

```
        {
            "Sid": "FullAccessToAllServicesExceptPeopleManagement",
            "Effect": "Allow",
            "NotAction": [
                "iam:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RequiredIamAndOrgsActions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:DeleteServiceLinkedRole",
                "iam:ListRoles",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Paulo는 90일 후에 AWS Management 콘솔을 사용하여 `Development` 그룹에 대해 서비스에서 마지막으로 액세스한 데이터 (p. 472)를 보기로 결정합니다. 그는 그룹 멤버가 액세스한 서비스 목록을 확인합니다. 그는 사용자가 지난 주에 5개의 서비스(AWS CloudTrail, Amazon CloudWatch Logs, Amazon EC2, AWS KMS 및 Amazon S3)에 액세스했다는 사실을 알게 되었습니다. 그들은 AWS를 처음 평가할 때 몇 가지 다른 서비스에 액세스했지만 그 이후에는 액세스하지 않았습니다.

Paulo는 5가지 서비스와 필요한 IAM 및 조직 작업만 포함하도록 정책 권한을 줄이기로 결정합니다. 그는 다음 JSON 텍스트를 사용하여 `ExampleDevelopment` 정책을 편집합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "FullAccessToListedServices",
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "kms:*",
                "cloudtrail:*",
                "logs:*",
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RequiredIamAndOrgsActions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:DeleteServiceLinkedRole",
                "iam:ListRoles",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

권한을 더 줄이기 위해 Paulo는 AWS CloudTrail 이벤트 기록에서 계정의 이벤트를 확인할 수 있습니다. 여기서 그는 개발자가 필요로 하는 작업과 리소스만 포함하도록 정책 권한을 줄이기 위해 사용할 수 있는 자

세한 이벤트 정보를 볼 수 있습니다. 자세한 정보는 AWS CloudTrail 사용 설명서에서 CloudTrail 콘솔에서 CloudTrail 이벤트 보기 단원을 참조하십시오.

데이터를 사용하여 IAM 사용자의 권한 축소

서비스에서 마지막으로 액세스한 데이터를 사용하여 개별 IAM 사용자의 권한을 줄일 수 있습니다.

예를 들어 Martha Rivera는 회사 직원들의 AWS 권한이 초과되지 않도록 관리하는 IT 관리자입니다. 정기 보안 검사의 일환으로 Martha는 모든 IAM 사용자의 권한을 검토합니다. 이러한 사용자 가운데는 애플리케이션 개발자로, 이전에 보안 엔지니어의 역할을 담당했던 Nikhil Jayashankar 씨도 있습니다. 작업 요구 사항의 변화로 인해 Nikhil은 `app-dev` 그룹과 `security-team` 그룹의 멤버입니다. 그의 새로운 직무와 관련된 `app-dev` 그룹은 Amazon EC2, Amazon EBS, Auto Scaling, Route 53 및 Elastic Transcoder를 포함하여 여러 서비스에 대한 권한을 부여합니다. 이전 직무와 관련된 `security-team` 그룹은 IAM 및 CloudTrail에 대한 권한을 부여합니다.

관리자인 Martha는 IAM 콘솔에 로그인하고 사용자를 선택한 다음 `nikhilj`을 선택하고 액세스 관리자 탭을 선택합니다.

Martha는 마지막 액세스 열을 검토하여 Nikhil이 최근에 IAM, CloudTrail, Route 53, Amazon Elastic Transcoder 및 기타 여러 AWS 서비스에 액세스하지 않았다는 것을 확인합니다. 회사 내에서 Martha는 Nikhil이 더 이상 내부 보안 팀의 멤버가 아니므로 업무적으로 IAM 및 CloudTrail에 액세스할 필요가 없다는 것을 확인합니다.

Martha는 이제 서비스에서 마지막으로 액세스한 데이터에 대한 작업을 수행할 수 있습니다. 그러나 이전 예제의 그룹과 달리 `nikhilj`과 같은 IAM 사용자는 여러 정책을 준수하고 여러 그룹의 멤버가 될 수 있습니다. Martha는 `nikhilj` 또는 다른 그룹 멤버의 액세스를 실수로 방해하지 않도록 주의해서 진행해야 합니다. Nikhil에게 부여할 액세스 권한의 종류뿐만 아니라, 이러한 권한을 받는 방법을 결정해야 합니다.

Martha는 권한 탭을 선택합니다. 이 탭에서 `nikhilj`에 직접 연결된 정책 및 그룹을 통해 연결된 정책을 확인합니다. 그녀는 각 정책을 확장하고 Nikhil이 사용하지 않는 서비스에 대한 액세스를 허용하는 정책을 알아보기 위해 정책 요약을 확인합니다.

- IAM – `IAMFullAccess` AWS 관리형 정책은 `nikhilj`에 직접 연결되고 `security-team` 그룹에 연결됩니다.
- CloudTrail – `AWSCloudTrailReadOnlyAccess` AWS 관리형 정책은 `security-team` 그룹에 연결됩니다.
- Route 53 – `App-Dev-Route53` 고객 관리형 정책은 `app-dev` 그룹에 연결됩니다.
- Elastic Transcoder – `App-Dev-ElasticTranscoder` 고객 관리형 정책은 `app-dev` 그룹에 연결됩니다.

Martha는 `nikhilj`에 직접 연결된 `IAMFullAccess` AWS 관리형 정책을 제거하기로 결정했습니다. 또한 `security-team` 그룹에 대한 Nikhil의 멤버십을 제거합니다. 이 두 작업은 IAM 및 CloudTrail에 대한 불필요한 액세스를 제거합니다.

Route 53 및 Elastic Transcoder에 액세스할 수 있는 Nikhil의 권한은 `app-dev` 그룹에 의해 부여됩니다. Nikhil은 이러한 서비스를 사용하지 않지만 그룹의 다른 멤버에게는 필요할 수 있습니다. Martha는 `app-dev` 그룹에 대해 서비스에서 마지막으로 액세스한 데이터를 검토하고 최근에 Route 53에 액세스한 멤버가 여러 명 있지만 작년에는 Elastic Transcoder에 액세스한 그룹 멤버가 없었음을 확인했습니다. 그녀는 그룹에서 `App-Dev-ElasticTranscoder` 고객 관리형 정책을 제거합니다.

그런 다음 Martha는 고객 관리형 정책인 `App-Dev-ElasticTranscoder`에 대해 서비스에서 마지막으로 액세스한 데이터를 검토합니다. 그녀는 정책이 다른 IAM 자격 증명에 연결되지 않았다는 것을 알게 됩니다. 그녀는 회사 내에서 앞으로 해당 정책이 필요하지 않다는 것을 조사한 다음 삭제합니다.

IAM 리소스 삭제 전 데이터 사용

IAM 리소스를 삭제하기 전에 서비스에서 마지막으로 액세스한 데이터를 사용하여 마지막으로 리소스를 사용한 이후로 일정 시간이 경과했는지 확인할 수 있습니다. 이는 사용자, 그룹, 역할 및 정책에 적용됩니다. 이러한 작업에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 사용자 – 사용자 삭제 (p. 94)
- 그룹 – 그룹 삭제 (p. 172)
- 역할 – 역할 삭제 (p. 284)
- 정책 – 관리형 정책 삭제(이로 인해 자격 증명에서 정책이 분리됨) (p. 465)

IAM 정책 편집 전 데이터 사용

해당 리소스에 영향을 미치는 정책을 편집하기 전에 서비스에서 마지막으로 액세스한 데이터를 IAM 자격 증명(사용자, 그룹 또는 역할) 또는 IAM 정책에 대해 검토할 수 있습니다. 이 기능은 사용 중인 사용자의 액세스 권한을 제거하지 않으려는 경우 중요합니다.

예를 들어, Arnav Desai는 개발자이고 Example Corp.의 AWS 관리자입니다. Arnav의 팀이 AWS를 사용하기 시작했을 때 그들은 모든 개발자에게 IAM 및 조직를 제외한 모든 서비스에 대한 전체 액세스를 허용하는 파워 사용자 권한을 부여했습니다. Arnav는 최소 권한 부여 (p. 61)를 위한 첫 걸음으로 AWS CLI를 사용하여 자신의 계정에서 관리형 정책을 검토하려고 합니다.

이렇게 하기 위해 Arnav는 먼저 다음 명령을 사용하여 자격 증명에 연결된 계정에 고객 관리형 권한 정책을 나열합니다.

```
aws iam list-policies --scope Local --only-attached --policy-usage-filter PermissionsPolicy
```

응답에서 그는 각 정책에 대한 ARN을 캡처합니다. 그런 다음 Arnav는 다음 명령을 사용하여 각 정책에 대해 서비스에서 마지막으로 액세스한 데이터 보고서를 생성합니다.

```
aws iam generate-service-last-accessed-details --arn arn:aws:iam::123456789012:policy/
ExamplePolicy1
```

이 응답에서 그는 `JobId` 필드에서 생성된 보고서의 ID를 캡처합니다. 그런 다음 Arnav는 `JobStatus` 필드가 `COMPLETED` 또는 `FAILED` 값을 반환할 때까지 다음 명령을 폴링합니다. 작업이 실패할 경우 오류를 캡처합니다.

```
aws iam get-service-last-accessed-details --job-id 98a765b4-3cde-2101-2345-example678f9
```

작업의 상태가 `COMPLETED`이면 Arnav는 JSON 형식의 `ServicesLastAccessed` 배열에 대한 콘텐츠를 구문 분석합니다.

```
 "ServicesLastAccessed": [
        {
            "TotalAuthenticatedEntities": 1,
            "LastAuthenticated": 2018-11-01T21:24:33.222Z,
            "ServiceNamespace": "dynamodb",
            "LastAuthenticatedEntity": "arn:aws:iam::123456789012:user/IAMExampleUser",
            "ServiceName": "Amazon DynamoDB"
        },

        {
            "TotalAuthenticatedEntities": 0,
            "ServiceNamespace": "ec2",
            "ServiceName": "Amazon EC2"
        },

        {
            "TotalAuthenticatedEntities": 3,
            "LastAuthenticated": 2018-08-25T15:29:51.156Z,
            "ServiceNamespace": "s3",
            "LastAuthenticatedEntity": "arn:aws:iam::123456789012:role/IAMExampleRole",
```

```
            "ServiceName": "Amazon S3"
        }
    ]
```

이 정보를 통해 Arnav는 `ExamplePolicy1` 정책이 Amazon DynamoDB, Amazon S3 및 Amazon EC2 세 가지 서비스에 대한 액세스를 허용한다는 것을 알게 됩니다. 11월 1일 IAM 사용자 `IAMExampleUser`가 DynamoDB에 마지막으로 액세스하려고 시도했으며, 8월 25일에는 어떤 사용자가 Amazon S3에 액세스하기 위해 `IAMExampleRole` 역할을 사용했습니다. 작년에 Amazon S3에 액세스하려고 시도한 엔터티가 두 개 더 있습니다. 그러나 작년에 Amazon EC2에 액세스하려고 시도한 사용자는 아무도 없었습니다.

이는 Arnav가 정책에서 Amazon EC2 작업을 안전하게 제거할 수 있음을 의미합니다. Arnav는 정책에 대한 현재 JSON 문서를 검토하려고 합니다. 먼저, 다음 명령을 사용하여 정책의 버전 번호를 결정해야 합니다.

```
aws iam list-policy-versions --policy-arn arn:aws:iam::123456789012:policy/ExamplePolicy1
```

응답에서 Arnav는 `Versions` 배열에서 현재 기본 버전 번호를 수집합니다. 그런 다음, 다음 명령을 통해 해당 버전 번호(`v2`)를 사용하여 JSON 정책 문서를 요청합니다.

```
aws iam get-policy-version --policy-arn arn:aws:iam::123456789012:policy/ExamplePolicy1 --
version-id v2
```

Arnav는 반환된 JSON 정책 문서를 `PolicyVersion` 배열의 `Document` 필드에 저장합니다. 정책 문서에서 Arnav는 `ec2` 네임스페이스에서 작업을 검색합니다. 정책에 남아 있는 다른 네임스페이스의 작업이 없는 경우 영향을 받는 자격 증명(사용자, 그룹 및 역할)에서 정책을 분리합니다. 그런 다음 정책을 삭제합니다. 이 경우, 정책에는 Amazon DynamoDB 및 Amazon S3 서비스가 포함됩니다. 그래서 Arnav는 문서에서 Amazon EC2 작업을 제거하고 변경 사항을 저장합니다. 그는 다음 명령을 사용하여 새 버전의 문서를 통해 정책을 업데이트하고 해당 버전을 기본 정책 버전으로 설정합니다.

```
aws iam create-policy-version --policy-arn arn:aws:iam::123456789012:policy/ExamplePolicy1
 --policy-document file://UpdatedPolicy.json --set-as-default
```

이제 `ExamplePolicy1` 정책이 업데이트되어 불필요한 Amazon EC2 서비스에 대한 액세스를 제거합니다.

기타 IAM 시나리오

IAM 리소스(사용자, 그룹, 역할 또는 정책)가 서비스에 마지막으로 액세스하려고 시도한 시점에 대한 정보는 다음 작업 중 하나를 완료할 때 도움이 될 수 있습니다.

- 정책 – 기존 고객 관리형 또는 인라인 정책을 편집하여 권한 제거 (p. 460)
- 정책 – 인라인 정책을 관리형 정책으로 변환한 다음 삭제 (p. 62)
- 정책 – 기존 정책에 명시적 거부 추가 (p. 629)
- 정책 – 자격 증명(사용자, 그룹 또는 역할)에서 관리형 정책 분리 (p. 453)
- 엔터티 – 엔터티(사용자 또는 역할)가 가질 수 있는 최대 권한을 제어하도록 권한 경계 설정 (p. 450)
- 그룹 – 그룹에서 사용자 제거 (p. 170)

데이터를 사용하여 조직 단위의 권한 구체화

서비스에서 마지막으로 액세스한 데이터를 사용하여 AWS Organizations의 조직 단위(OU)의 권한을 세분화할 수 있습니다.

예를 들어 John Stiles는 AWS Organizations 관리자입니다. 그는 회사 AWS 계정의 사람들에게 과도한 권한이 부여되지 않도록 할 책임이 있습니다. 정기 보안 검사의 일환으로 그는 자신의 조직에 부여된 권한을 검토합니다. 그의 `Development` OU에는 새로운 AWS 서비스를 테스트하는 데 자주 사용되는 계정이 포함되어

있습니다. John은 180일 이상 액세스되지 않은 서비스에 대한 보고서를 주기적으로 검토하기로 결정합니다. 그런 다음 OU 멤버가 이러한 서비스에 액세스할 수 있는 권한을 제거합니다.

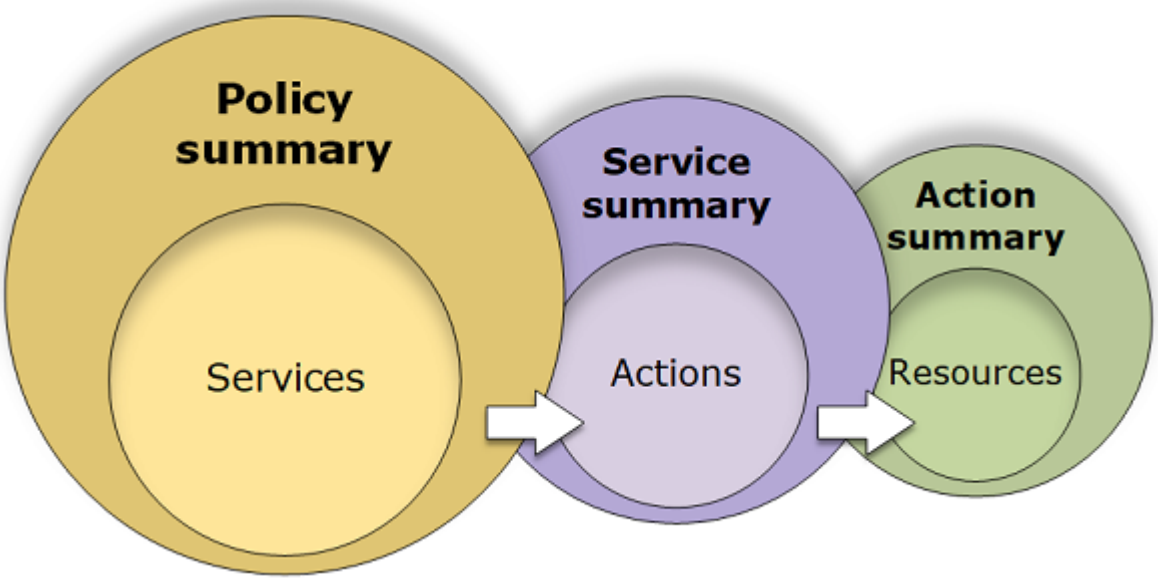
John은 자신의 마스터 계정 자격 증명을 사용하여 IAM 콘솔에 로그인합니다. IAM 콘솔에서 `Development` OU에 대한 조직 데이터를 찾습니다. 그는 서비스 액세스 보고서 표를 검토하여 180일 이상 액세스되지 않은 2개의 AWS 서비스를 발견합니다. 그는 개발 팀이 Amazon Lex 및 AWS Database Migration Service에 액세스할 수 있는 권한을 추가한 것을 기억합니다. 그래서 개발 팀에 연락하여 더 이상 이러한 서비스를 테스트할 업무상 필요가 없는지 확인합니다.

John은 이제 서비스에서 마지막으로 액세스한 데이터에 대한 작업을 수행할 수 있습니다. 그는 AWS Organizations에서 편집을 선택합니다. 그러면 이 SCP가 여러 엔터티에 연결되어 있다는 메시지가 표시됩니다. 계속을 선택합니다. 그는 AWS Organizations에서 대상을 검토하여 SCP에 어떤 조직 엔터티가 연결되어 있는지 확인합니다. 모든 엔터티가 `Development` OU에 속해 있습니다.

John은 `NewServiceTest` SCP에서 Amazon Lex 및 AWS Database Migration Service 작업에 대한 액세스를 거부하기로 결정합니다. 이 작업은 서비스에 대한 불필요한 액세스 권한을 제거합니다.

정책에 의해 부여된 권한 이해

IAM 콘솔에는 정책에서 각 서비스에 대해 허용되거나 거부되는 액세스 레벨, 리소스, 조건을 설명하는 정책 요약 테이블이 포함되어 있습니다. 정책은 3가지 테이블, 즉 정책 요약 (p. 484), 서비스 요약 (p. 493), 작업 요약 (p. 497)으로 요약됩니다. 정책 요약 테이블에는 서비스 목록이 포함되어 있습니다. 서비스 요약을 보려면 여기서 서비스를 선택합니다. 이 요약 테이블에는 작업 목록과 선택한 서비스에 대해 연결된 권한이 포함되어 있습니다. 해당 테이블에서 작업을 선택하여 작업 요약을 볼 수 있습니다. 이 테이블에는 리소스 목록과 선택한 작업에 대한 조건이 포함되어 있습니다.



사용자 페이지 또는 역할 페이지에서 해당 사용자에 연결된 모든 정책(관리형 및 인라인)에 대한 정책 요약을 볼 수 있습니다. 정책 페이지에서 모든 관리형 정책에 대한 요약을 봅니다. 관리형 정책에는 AWS 관리형 정책, AWS 관리형 직무 정책, 고객 관리형 정책이 포함되어 있습니다. 정책이 사용자 또는 다른 IAM 자격 증명에 연결되어 있는지 여부와 상관없이 정책 페이지에서 이러한 정책에 대한 요약을 볼 수 있습니다.

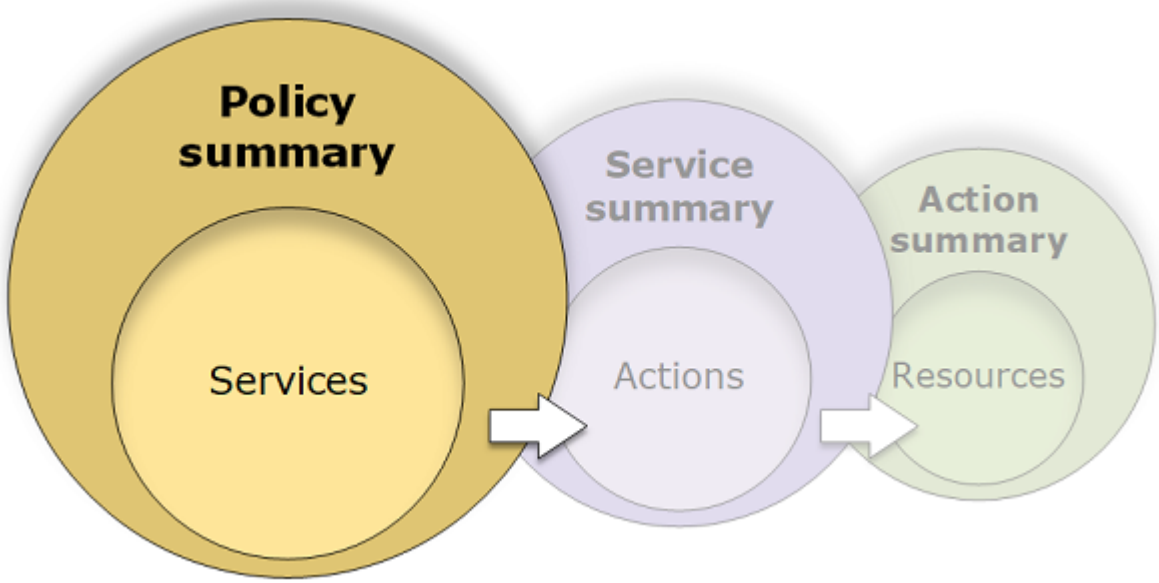
정책 요약의 정보를 사용하여 정책에서 허용되거나 거부된 권한을 확인할 수 있습니다. 정책 요약은 예상한 권한을 제공하지 않는 정책의 문제를 해결 (p. 537)하고 정책을 수정하는 데 도움이 됩니다.

주제

- 정책 요약(서비스 목록) (p. 484)

정책 요약(서비스 목록)

정책은 3가지 테이블, 즉 정책 요약, 서비스 요약 (p. 493), 작업 요약 (p. 497)으로 요약됩니다. 정책 요약 테이블에는 서비스 목록과 선택한 정책에 의해 정의된 권한의 요약이 포함되어 있습니다.



정책 요약 테이블은 하나 이상의 Uncategorized services(미분류 서비스), 명시적 거부, 허용 섹션으로 그룹화됩니다. IAM에서 인식하지 못하는 서비스가 정책에 포함되어 있으면 해당 서비스는 테이블의 Uncategorized services(미분류 서비스) 섹션에 포함됩니다. IAM에서 서비스를 인식하면 해당 서비스는 정책(`Deny` 또는 `Allow`)의 효과에 따라 테이블의 명시적 거부 또는 허용 섹션에 포함됩니다.

정책 요약 보기

사용자 페이지에서 사용자에게 연결된 정책에 대한 요약을 볼 수 있습니다. 역할 페이지에서 역할에 연결된 정책에 대한 요약을 볼 수 있습니다. 정책 페이지에서 관리형 정책에 대한 정책 요약을 볼 수 있습니다. 정책에 정책 요약이 포함되지 않은 경우 정책 요약 누락 (p. 541)을 참조하여 이유를 알아보십시오.

정책 페이지에서 정책 요약을 확인하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 보려는 정책의 이름을 선택합니다.
4. 정책 요약을 보려면 해당 정책의 요약 페이지에서 권한 탭을 확인합니다.

사용자에 연결된 정책의 요약을 확인하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.

2. 탐색 창에서 사용자를 선택합니다.
3. 사용자 목록에서 정책을 보려는 사용자의 이름을 선택합니다.
4. 사용자에게 직접 연결되거나 그룹에서 연결된 정책의 목록을 보려면 해당 사용자의 요약 페이지에서 권한 탭을 봅니다.
5. 사용자에 대한 정책 테이블에서 보려는 정책의 행을 확장합니다.

역할에 연결된 정책의 요약 정보를 보려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택합니다.
3. 역할 목록에서 정책을 보려는 역할의 이름을 선택합니다.
4. 역할의 요약 페이지에서 권한 탭을 보고 역할에 연결된 정책 목록을 확인합니다.
5. 역할에 대한 정책 테이블에서 보려는 정책의 행을 확장합니다.

정책을 편집하여 경고 수정

정책 요약을 보는 동안 정책에서 예상한 권한을 제공하지 않는다는 알림이나 오타를 찾을 수 있습니다. 정책 요약을 직접 편집할 수 없습니다. 그러나 정책 요약이 보고하는 것과 동일한 여러 개의 오류 및 경고를 파악하는 시각적 정책 편집기를 사용하여 관리형 정책을 편집할 수 있습니다. 그런 다음 정책 요약의 변경 사항을 확인하여 모든 문제가 수정되었는지 확인할 수 있습니다. 인라인 정책을 편집하는 방법에 대해 자세히 알아보려면 the section called “IAM 정책 편집” (p. 460) 단원을 참조하십시오. 단, AWS 관리형 정책은 편집할 수 없습니다.

시각적 편집기 탭을 사용하여 정책 요약에 대한 정책을 편집하려면

1. 이전 절차에서 설명한 대로 정책의 요약을 엽니다.
2. 정책 편집을 선택합니다.

   사용자 페이지에서 해당 사용자에게 연결된 고객 관리형 정책을 편집하려는 경우, 정책 페이지로 리디렉션됩니다. 고객 관리형 정책은 정책 페이지에서만 편집할 수 있습니다.
3. 편집 가능한 정책의 시각적 표시를 보려면 시각적 편집기 탭을 선택합니다. IAM은 시각적 편집기에서 모양을 최적화하고 문제를 쉽게 찾아 수정하기 위해 정책을 재구성할 수 있습니다. 페이지의 경고 및 오류 메시지는 정책 문제를 수정하도록 안내할 수 있습니다. IAM이 정책을 재구성하는 방법에 대한 자세한 내용은 정책 재구성 (p. 538) 단원을 참조하십시오.
4. 정책을 편집하고 정책 검토를 선택하여 정책 요약에 반영된 변경 사항을 봅니다. 문제가 계속 표시되면 이전을 선택하여 편집 화면으로 돌아갑니다.
5. [Save]를 선택하여 변경 사항을 저장합니다.

JSON 탭을 사용하여 정책 요약에 대한 정책을 편집하려면

1. 이전 절차에서 설명한 대로 정책의 요약을 엽니다.
2. { } JSON과 정책 요약을 선택하여 정책 요약과 JSON 정책 문서를 비교합니다. 이 정보를 사용하여 정책 문서에서 변경할 행을 결정할 수 있습니다.
3. 정책 편집을 선택한 다음 JSON 탭을 선택하여 JSON 정책 문서를 편집합니다.

   Note

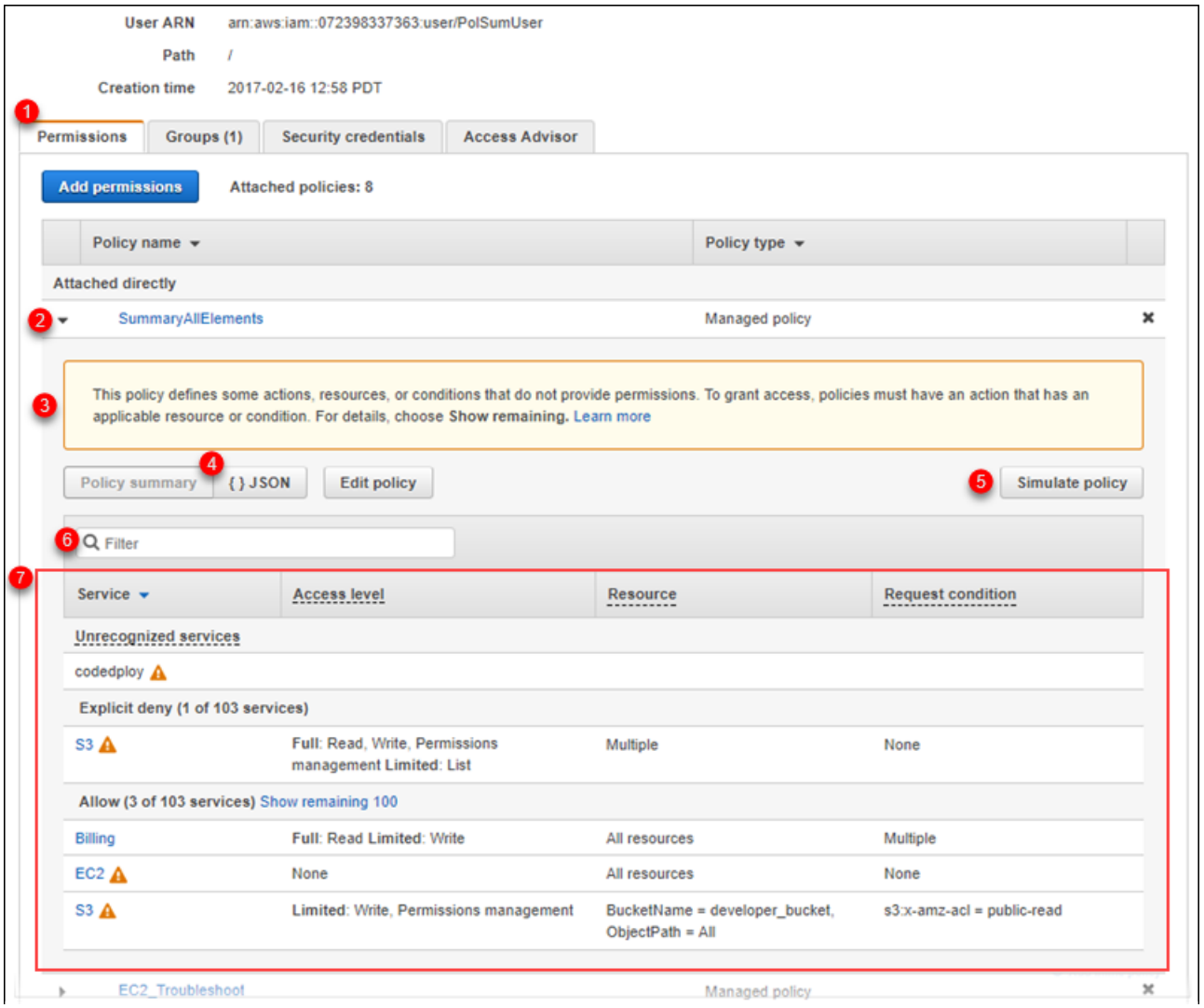
   언제든지 Visual editor(시각적 편집기) 및 JSON 탭을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 정책 재구성 (p. 538) 단원을 참조하십시오.

사용자 페이지에서 해당 사용자에게 연결된 고객 관리형 정책을 편집하려는 경우, 정책 페이지로 리디렉션됩니다. 고객 관리형 정책은 정책 페이지에서만 편집할 수 있습니다.

4. 정책을 편집하고 정책 검토를 선택하여 정책 요약에 반영된 변경 사항을 봅니다. 문제가 계속 표시되면 이전을 선택하여 편집 화면으로 돌아갑니다.
5. [Save]를 선택하여 변경 사항을 저장합니다.

정책 요약의 요소 이해하기

다음의 사용자 세부 정보 페이지 예제에서는 PolSumUser 사용자에 8개 정책이 연결되어 있습니다. SummaryAllElements 정책은 사용자에 직접 연결된 관리형 정책(고객 관리형 정책)입니다. 이 정책이 확장되어 정책 요약을 표시합니다. 이 정책의 JSON 정책 문서를 보려면 the section called “SummaryAllElements JSON 정책 문서” (p. 490) 단원을 참조하십시오.

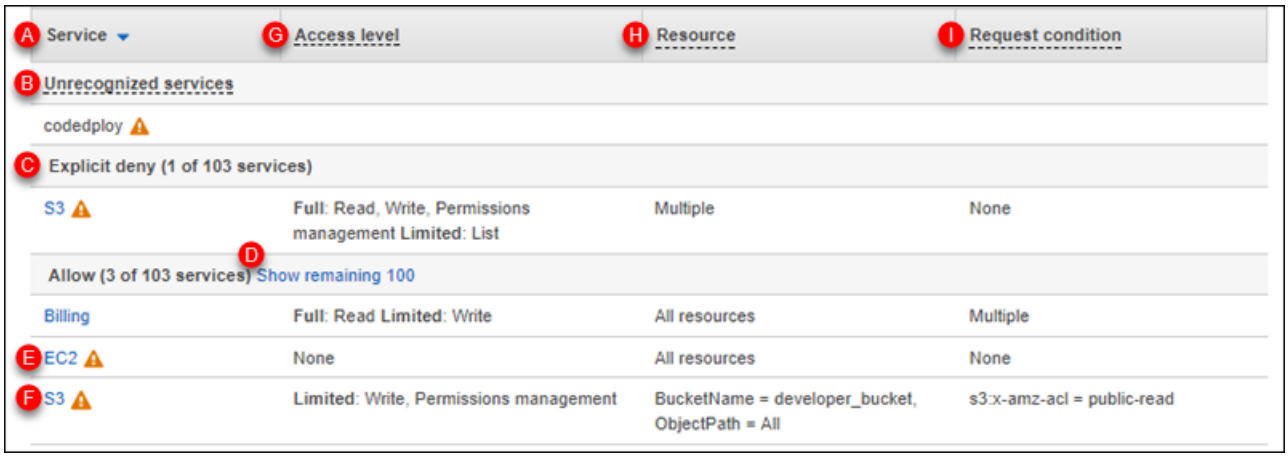


이전 이미지에서 정책 요약은 사용자 세부 정보 페이지에 표시되어 있습니다.

1. 사용자의 권한 탭에는 PolSumUser 사용자에 연결된 정책이 포함됩니다.
2. SummaryAllElements 정책은 사용자에게 연결된 몇 가지 정책 중 하나입니다. 정책 요약을 보려면 정책을 확장합니다.

3. 정책에서 정책에 정의된 일부 작업, 리소스 및 조건에 권한을 부여하지 않는 경우 페이지 상단에 경고 또는 오류 배너가 나타납니다. 그런 다음 정책 요약에 문제에 대한 세부 정보가 포함됩니다. 정책 요약이 정책에서 부여하는 권한을 이해하고 문제를 해결하는 데 얼마나 도움이 되는지 알아보려면 the section called “정책이 필요한 권한을 부여하지 않음” (p. 543) 단원을 참조하십시오.
4. 정책 요약 및 { } JSON 버튼을 사용하여 정책 요약과 JSON 정책 문서 사이를 전환합니다.
5. 정책 시뮬레이션(Simulate policy)을 선택하면 정책을 테스트하기 위한 정책 시뮬레이터가 열립니다.
6. 검색 상자를 사용하여 서비스 목록을 제한하면 용이하게 특정 서비스를 찾을 수 있습니다.
7. 확장된 보기는 SummaryAllElements 정책의 세부 정보를 보여 줍니다.

다음 정책 요약 테이블 이미지는 PolSumUser 사용자 세부 정보 페이지에서 확장된 SummaryAllElements 정책입니다.



이전 이미지에서 정책 요약은 사용자 세부 정보 페이지에 표시되어 있습니다.

A. 서비스 – 이 열에는 정책에서 정의된 서비스가 나열되고 각 서비스의 세부 정보를 제공합니다. 정책 요약 테이블에서 각 서비스 이름은 서비스 요약 테이블에 대한 링크(서비스 요약(작업 목록) (p. 493) 단원 참조)입니다. 이 예제에서는 Amazon S3, 결제 및 Amazon EC2 서비스에 대해 권한이 정의되어 있습니다. 정책은 IAM에서 인식하지 못하는 (잘못 입력한) `codedploy` 서비스에 대한 권한도 정의합니다.

B. Unrecognized services(미분류 서비스) – 이 정책에는 인식할 수 없는 서비스(이 경우 codedploy )가 포함됩니다. 이 경고를 사용하여 서비스 이름에 오타가 포함되어 있는지 확인할 수 있습니다. 서비스 이름이 정확하면 서비스는 정책 요약을 지원할 수 없거나 프리뷰에 있거나 사용자 지정 서비스일 수 있습니다. 일반적으로 사용할 수 있는(GA) 서비스에 대한 정책 요약 지원을 요청하려면 서비스가 IAM 정책 요약을 지원하지 않음 (p. 542)을 참조하십시오. 이 예제에서는 정책이 `codedploy`가 누락된 인식할 수 없는 `e` 서비스를 포함합니다. 이 오타로 인해 정책은 예상되는 AWS CodeDeploy 권한을 제공하지 않습니다. 정확한 `codedeploy` 서비스 이름을 포함하도록 정책을 편집 (p. 485)할 수 있습니다. 그러면 서비스가 정책 요약에 나타납니다.

C. IAM에서 인식하는 해당 서비스의 경우 정책이 서비스 사용을 허용하거나 명시적으로 거부하는지 여부에 따라 서비스가 정렬됩니다. 이 예제에서는 정책이 Amazon S3 서비스에 대한 `Allow` 및 `Deny` 설명문을 포함합니다. 따라서 정책 요약의 명시적 거부 및 허용 섹션 모두에 S3가 포함되어 있습니다.

D. Show remaining 100(나머지 100개 보기) – 이 링크를 선택하여 정책에 의해 정의되지 않은 서비스를 포함하도록 테이블을 확장합니다. 이러한 서비스는 이 정책 내에서 명시적으로 거부(또는 기본적으로 거부)됩니다. 그러나 다른 정책 문으로 서비스를 사용하여 허용하거나 명시적으로 거부할 수 있습니다. 정책 요약에는 단일 정책의 권한이 요약되어 있습니다. AWS 서비스가 지정된 요청을 허용하거나 거부할지 여부를 결정하는 방법에 대해 알아보려면 정책 평가 로직 (p. 622)을 참조하십시오.

E. EC2  – 이 서비스에는 미인식 작업이 포함됩니다. IAM은 정책 요약을 지원하는 서비스 이름, 작업 및 리소스 유형을 인식합니다. 서비스는 인식되지만 인식되지 않은 작업을 포함하면 IAM은 해당 서비스 옆에 경고를 포함합니다. 이 예제에서는 IAM이 한 개 이상의 Amazon EC2 작업을 인식하지 못합니다. 인식할

수 없는 작업에 대해 자세히 알아보고 S3 서비스 요약에서 인식할 수 없는 작업을 보려면 서비스 요약(작업 목록) (p. 493) 단원을 참조하십시오.

Note

IAM은 정책 요약을 지원하는 서비스의 이름, 작업 및 리소스 유형을 검토합니다. 그러나 존재하지 않는 리소스 값이나 조건이 정책 요약에 포함될 수 있습니다. 항상 정책 시뮬레이터 (p. 441)로 정책을 테스트합니다.

F. S3  – 이 서비스에는 미인식 리소스가 포함됩니다. IAM은 정책 요약을 지원하는 서비스 이름, 작업 및 리소스 유형을 인식합니다. 서비스가 인식되지만 인식되지 않는 리소스 유형이 있는 경우 IAM은 해당 서비스 옆에 경고를 표시합니다. 이 예제에서는 IAM이 한 개 이상의 Amazon S3 작업을 인식하지 못합니다. 인식할 수 없는 리소스에 대해 자세히 알아보고 S3 서비스 요약에서 인식할 수 없는 리소스 유형을 보려면 서비스 요약(작업 목록) (p. 493) 단원을 참조하십시오.

G. Access level(액세스 레벨) – 이 열은 정책이 각 액세스 레벨(`List`, `Read`, `Write`, 및 `Permissions management`)의 작업에 대해 `Full` 또는 `Limited` 중 어느 권한을 정의했는지 보여줍니다. 액세스 레벨 요약에 대한 자세한 정보 및 예제는 정책 요약에서 액세스 레벨 요약 이해하기 (p. 491) 단원을 참조하십시오.

- Full access(전체 액세스) – 이 항목은 해당 서비스가 서비스에 대해 사용 가능한 4개 액세스 레벨 모두에서 모든 작업에 액세스할 수 있음을 나타냅니다. 이 예제에서는 이 행이 테이블의 명시적 거부 섹션에 포함되어 있으므로 정책에 포함된 리소스에서 모든 Amazon S3 작업이 거부됩니다.
- 항목에 Full access(전체 액세스)가 포함되지 않은 경우 해당 서비스는 서비스를 위한 모든 작업이 아니라 일부 작업에 액세스할 수 있습니다. 그러면 액세스 권한이 4개 액세스 레벨(`List`, `Read`, `Write` 및 `Permissions management`) 각각에 대한 다음의 설명으로 정의됩니다.

  Full(전체): 정책이 나열된 각 액세스 레벨 분류의 모든 작업에 대한 액세스 권한을 제공합니다. 이 예제에서는 정책이 모든 결제 `Read` 작업에 대한 액세스 권한을 제공합니다.

  Limited(제한): 정책이 나열된 각 액세스 레벨 분류에서 하나 이상의 작업(모든 작업은 아님)에 대한 액세스 권한을 제공합니다. 이 예제에서는 정책이 일부 결제 `Write` 작업에 대한 액세스 권한을 제공합니다.

H. 리소스 – 이 열은 정책이 각 서비스에 대해 지정한 리소스를 보여줍니다.

- 다중 – 정책이 서비스 내 둘 이상(모든 리소스는 아님)의 리소스를 포함합니다. 이 예제에서는 둘 이상의 Amazon S3 리소스에 대한 액세스가 명시적으로 거부됩니다.
- All resources(모든 리소스) – 정책이 서비스의 모든 리소스에 대해 정의되어 있습니다. 이 예제에서는 정책이 모든 결제 리소스에 대해 나열된 작업을 수행할 수 있도록 허용합니다.
- Resource text – 정책이 서비스의 리소스 하나를 포함합니다. 이 예제에서는 나열된 작업이 `developer_bucket` Amazon S3 버킷 리소스에서만 허용됩니다. 서비스가 IAM에 제공하는 정보에 따라 `arn:aws:s3:::developer_bucket/*` 등의 ARN이 표시되거나 `BucketName = developer_bucket` 등의 정의된 리소스 유형이 표시될 수 있습니다.

  Note

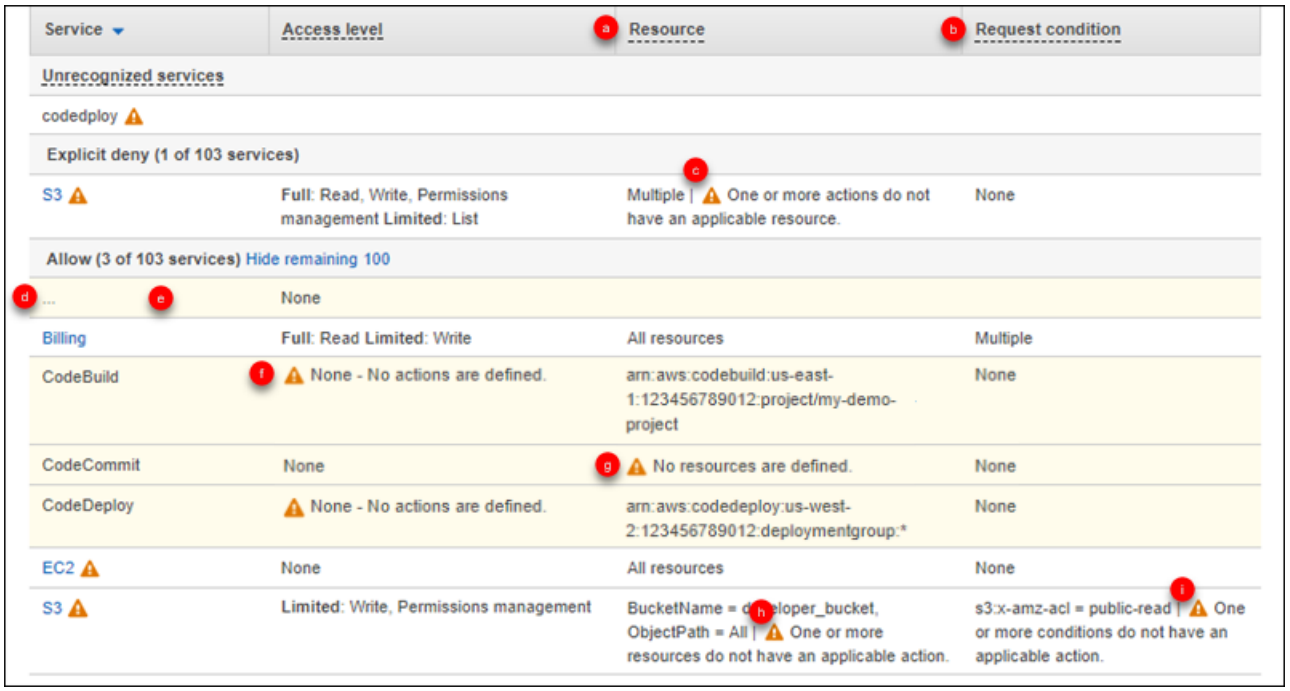
  이 열은 다른 서비스의 리소스를 포함할 수 있습니다. 리소스를 포함하는 정책 설명에 동일한 서비스의 작업과 리소스를 모두 포함하지 않으면 정책에 일치하지 않는 리소스가 포함됩니다. IAM은 정책을 생성하거나 정책 요약에서 정책을 볼 때 일치하지 않는 리소스에 대해 경고하지 않습니다. 이 열에 일치하지 않는 리소스가 포함되어 있으면 정책에 오류가 있는지 검토해야 합니다. 정책을 더 잘 이해하려면 항상 정책 시뮬레이터 (p. 441)로 테스트합니다.

I. Request condition(요청 조건) – 이 열은 리소스와 연결된 서비스 또는 작업에 조건이 적용되는지 여부를 나타냅니다.

- 없음 – 정책이 서비스에 대한 조건을 포함하지 않습니다. 이 예제에서는 Amazon S3 서비스에서 거부된 작업에 적용된 조건이 없습니다.
- Condition text – 정책이 서비스에 대한 조건 하나를 포함합니다. 이 예제에서는 소스의 IP 주소가 `203.0.113.0/24`와 일치하는 경우에만 나열된 결제 작업이 허용됩니다.

- 다중 – 정책이 서비스에 대해 둘 이상의 조건을 포함합니다. 이 예제에서는 나열된 Amazon S3 작업에 대한 액세스가 복수의 조건에 따라 허용됩니다. 정책에 대한 여러 조건을 각각 보려면 { } JSON을 선택하여 정책 문서를 봅니다.

정책 또는 정책 내 요소가 권한을 부여하지 않는 경우 IAM은 정책 요약에 추가 경고 및 정보를 제공합니다. 다음 정책 요약 테이블은 PolSumUser 사용자 세부 정보 페이지에 확장된 Show remaining 100(나머지 100개 보기) 서비스와 가능한 경고를 보여줍니다.



앞의 그림에는 권한이 없이 정의된 작업, 리소스 또는 조건을 포함하는 모든 서비스가 나와 있습니다.

a. Resource warnings(리소스 경고) – 포함된 모든 작업이나 리소스에 대해 권한을 제공하지 않는 서비스의 경우 테이블의 리소스 열에 다음 경고 중 하나가 나타납니다.

   - 정의된 리소스가 없습니다. – 서비스에 작업이 정의되었지만 정책에 지원되는 리소스가 포함되지 않았음을 의미합니다.
   - 하나 이상의 작업이 적용할 리소스가 없습니다. – 서비스에 정의된 작업이 있지만 일부 작업에 지원되는 리소스가 없음을 의미합니다.
   - 하나 이상의 리소스가 적용할 작업이 없습니다. – 서비스에 정의된 리소스가 있지만 일부 리소스에 지원 작업이 없음을 의미합니다.

   서비스에 적용 가능한 리소스가 없는 작업과 적용 가능한 작업이 없는 리소스가 있는 경우, One or more resources do not have an applicable action(하나 이상의 리소스에 적용할 작업이 없습니다). 경고가 표시됩니다. 그 이유는 서비스에 대한 서비스 요약을 볼 때 어떤 작업에도 적용되지 않는 리소스가 표시되지 않기 때문입니다. `ListAllMyBuckets` 작업의 경우 리소스 수준 권한을 지원하지 않고 `s3:x-amz-acl` 조건 키를 지원하지 않기 때문에 이 정책에 마지막 경고가 포함됩니다. 리소스 문제나 조건 문제를 수정한 경우 나머지 문제가 세부 경고에 나타납니다.

b. Request condition warnings(요청 조건 경고) – 포함된 모든 조건에 대해 권한을 제공하지 않는 서비스의 경우 테이블의 Request condition(요청 조건)열에 다음 경고 중 하나가 나타납니다.

   - 하나 이상의 작업이 적용할 조건이 없습니다. – 서비스에 정의된 작업이 있지만 일부 작업에 지원되는 조건이 없음을 의미합니다.

- ⚠ 하나 이상의 조건이 적용할 작업이 없습니다. – 서비스에 정의된 조건이 있지만 일부 조건에 지원 작업이 없음을 의미합니다.

c. Multiple | ⚠ 하나 이상의 작업이 적용할 리소스가 없습니다. – Amazon S3의 `Deny` 문에 리소스가 두 개 이상 포함되어 있습니다. 또한 작업이 두 개 이상 포함되어 있으며, 일부 작업은 리소스를 지원하고, 일부 작업은 리소스를 지원하지 않습니다. 정책을 보려면 the section called “SummaryAllElements JSON 정책 문서” (p. 490)를 참조하십시오. 이 경우 정책에는 모든 Amazon S3 작업과, 정의된 버킷 또는 버킷 객체에서 수행될 수 있는 작업만 포함됩니다.

d. 줄임표(...)는 모든 서비스가 페이지에 포함되었지만 이 정책과 관련된 정보가 있는 행만 표시되었음을 나타냅니다. AWS Management 콘솔에서 이 페이지를 보면 모든 AWS 서비스를 볼 수 있습니다.

e. 테이블 행의 배경색은 어떤 권한도 부여하지 않는 서비스를 나타냅니다. 정책 요약에서 이러한 서비스에 대한 추가 정보를 볼 수 없습니다. 흰색 행의 서비스의 경우, 서비스 이름을 선택하여 서비스 요약(작업 목록) 페이지를 볼 수 있습니다. 이 페이지에는 해당 서비스에 대해 부여된 권한에 대한 자세한 정보가 표시됩니다.

f. ⚠ 없음 - 정의된 작업이 없습니다. – 서비스가 리소스나 조건으로 정의되었지만, 서비스에 대해 포함된 작업이 없으며 따라서 서비스가 권한을 제공하지 않음을 의미합니다. 이 경우 정책에 CodeBuild 리소스가 포함되지만 CodeBuild 작업은 포함되지 않습니다.

g. ⚠ 정의된 리소스가 없습니다. – 서비스에 정의된 작업이 있지만, 지원되는 리소스가 정책에 없으며 따라서 서비스가 권한을 제공하지 않습니다. 이 경우 정책에 CodeCommit 작업이 포함되지만 CodeCommit 리소스는 포함되지 않습니다.

h. BucketName = developer_bucket, ObjectPath = All | ⚠ 하나 이상의 리소스가 적용할 작업이 없습니다. – 서비스에 정의된 버킷 객체 리소스가 한 개 있고, 지원 작업이 없는 리소스가 한 개 이상 있습니다.

i. s3:x-amz-acl = public-read | ⚠ 하나 이상의 조건이 적용할 작업이 없습니다. – 서비스에 정의된 `s3:x-amz-acl` 조건 키가 한 개 있고, 지원 작업이 없는 조건 키가 한 개 이상 있습니다.

SummaryAllElements JSON 정책 문서

SummaryAllElements 정책은 해당 계정의 권한을 정의하는 데 사용하기 위한 것이 아닙니다. 이것은 정책 요약을 보는 중 만날 수 있는 오류와 경고를 보여주기 위한 것입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods",
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount",
                "aws-portal:ViewUsage"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "203.0.113.0/24"
                }
            }
        },
        {
```

```
            "Effect": "Deny",
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::customer",
                "arn:aws:s3:::customer/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetConsoleScreenshots"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "codedploy:*",
                "codecommit:*"
            ],
            "Resource": [
                "arn:aws:codedeploy:us-west-2:123456789012:deploymentgroup:*",
                "arn:aws:codebuild:us-east-1:123456789012:project/my-demo-project"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetObject",
                "s3:DeletObject",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::developer_bucket",
                "arn:aws:s3:::developer_bucket/*",
                "arn:aws:autoscling:us-east-2:123456789012:autoscalgrp"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": [
                        "public-read"
                    ],
                    "s3:prefix": [
                        "custom",
                        "other"
                    ]
                }
            }
        }
    ]
}
```

정책 요약에서 액세스 레벨 요약 이해하기

AWS 액세스 레벨 요약

정책 요약에는 해당 정책에서 언급된 각 서비스에 정의된 작업 권한을 설명하는 액세스 레벨 요약이 포함됩니다. 정책 요약에 대한 자세한 내용은 정책에 의해 부여된 권한 이해 (p. 483) 단원을 참조하십시오. 액세

스 레벨 요약은 각 액세스 레벨(`List`, `Read`, `Write`, `Permissions management`)의 작업에 정책에 정의된 `Full` 또는 `Limited` 권한이 있는지 여부를 나타냅니다. 서비스의 각 작업에 할당된 액세스 레벨 분류를 보려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

다음 예제에서는 한 정책이 지정된 서비스에 대해 제공하는 액세스 권한을 설명합니다. 전체 JSON 정책 문서 및 관련 요약의 예는 정책 요약 예제 (p. 499) 단원을 참조하십시오.

서비스	액세스 레벨	이 정책은 다음을 제공합니다.
IAM	모든 액세스	IAM 서비스 내의 모든 작업에 대한 액세스 권한
CloudWatch	전체: 목록	`List` 액세스 레벨의 모든 CloudWatch 작업에 대한 액세스 권한. 하지만 `Read`, `Write` 또는 `Permissions management` 액세스 레벨 분류의 작업에 대한 액세스 권한은 제공하지 않음
데이터 파이프라인	제한: 목록, 읽기	`List` 및 `Read` 액세스 레벨의 AWS Data Pipeline 작업 하나 이상(모든 작업은 아님)에 대한 액세스 권한. 단, `Write` 또는 `Permissions management` 작업에 대한 액세스 권한은 제외됨
EC2	전체: 목록, 읽기 제한: 쓰기	모든 Amazon EC2 `List` 및 `Read` 작업에 대한 액세스 권한, 하나 이상의 Amazon EC2 `Write` 작업(모든 작업은 아님)에 대한 액세스 권한. 단, `Permissions management` 액세스 레벨 분류의 작업에 대한 액세스 권한은 제외됨
S3	제한: 읽기, 쓰기, 권한 관리	하나 이상의 Amazon S3 `Read`, `Write` 및 `Permissions management` 작업(모든 작업은 아님)에 대한 액세스 권한
CodeDeploy	(비어 있음)	알 수 없는 액세스(IAM에서 이 서비스를 인식하지 않음)
API 게이트웨이	없음	정책에 정의된 액세스 없음
CodeBuild	⚠ 정의된 작업 없음.	서비스에 대해 작업이 정의되지 않아서 액세스할 수 없습니다. 이 문제를 이해하고 문제를 해결하는 방법을 보려면 the section called “정책이 필요한 권한을 부여하지 않음” (p. 543) 단원을 참조하십시오.

앞서 언급한 바와 같이 (p. 488), 모든 액세스는 정책이 서비스 내 모든 작업에 대한 액세스를 제공함을 나타냅니다. 서비스의 모든 작업이 아니라 일부에 대한 액세스 권한을 제공하는 정책은 액세스 레벨 분류에 따라 추가로 그룹화됩니다. 이는 다음 액세스 레벨 그룹 중 하나에 의해 표시됩니다.

- 전체: 정책이 지정된 액세스 레벨 분류의 모든 작업에 대한 액세스 권한을 제공합니다.
- 제한: 정책이 지정된 액세스 레벨 분류 내 하나 이상의 작업(모든 작업은 아님)에 대한 액세스 권한을 제공합니다.
- 없음: 정책에서 액세스를 제공하지 않습니다.
- (비어 있음): IAM에서 이 서비스를 인식하지 않습니다. 서비스 이름에 오타가 포함되어 있으면 정책은 서비스에 대한 액세스를 제공하지 않습니다. 서비스 이름이 정확하면 서비스는 정책 요약을 지원할 수 없거나 프리뷰에 있을 수 있습니다. 이 경우 정책은 액세스를 제공할 수 있지만 해당 액세스를 정책 요약에 표시할 수 없습니다. 일반적으로 사용할 수 있는(GA) 서비스에 대한 정책 요약 지원을 요청하려면 서비스가 IAM 정책 요약을 지원하지 않음 (p. 542)을 참조하십시오.

작업에 대한 제한적(부분적) 액세스 권한을 포함하는 액세스 레벨 요약은 AWS 액세스 레벨 분류 `List`, `Read`, `Write`, `Permissions Management` 또는 `Tagging`을 사용하여 그룹화됩니다.

AWS 액세스 레벨

AWS는 서비스의 작업에 대해 다음과 같은 액세스 레벨 분류를 정의합니다.

- 목록: 서비스의 리소스를 나열하여 객체가 존재하는지 판단할 수 있는 권한입니다. 이 액세스 레벨의 작업은 객체를 나열할 수 있으나 리소스의 내용을 확인할 수 없습니다. 예를 들어 Amazon S3 작업 `ListBucket`의 액세스 레벨은 목록입니다.
- 읽기: 서비스에서 리소스 내용과 속성을 읽을 수 있으나 편집할 수 없는 권한입니다. 예를 들어 Amazon S3 작업 `GetObject` 및 `GetBucketLocation`의 액세스 레벨은읽기입니다.
- 쓰기: 서비스에서 리소스를 생성, 삭제하거나 수정할 수 있는 권한입니다. 예를 들어 Amazon S3 작업 `CreateBucket`, `DeleteBucket` 및 `PutObject`는 쓰기 액세스 레벨입니다. `Write` 작업은 리소스 태그 수정을 허용할 수도 있습니다. 그러나 태그 변경만 허용하는 작업은 `Tagging` 액세스 레벨입니다.
- 권한 관리: 서비스에서 리소스 권한을 부여하거나 수정할 수 있는 권한입니다. 예를 들어 대부분의 IAM 및 AWS Organizations 작업과 Amazon S3 작업 `PutBucketPolicy` 및 `DeleteBucketPolicy` 등의 액세스 레벨은 권한 관리입니다.

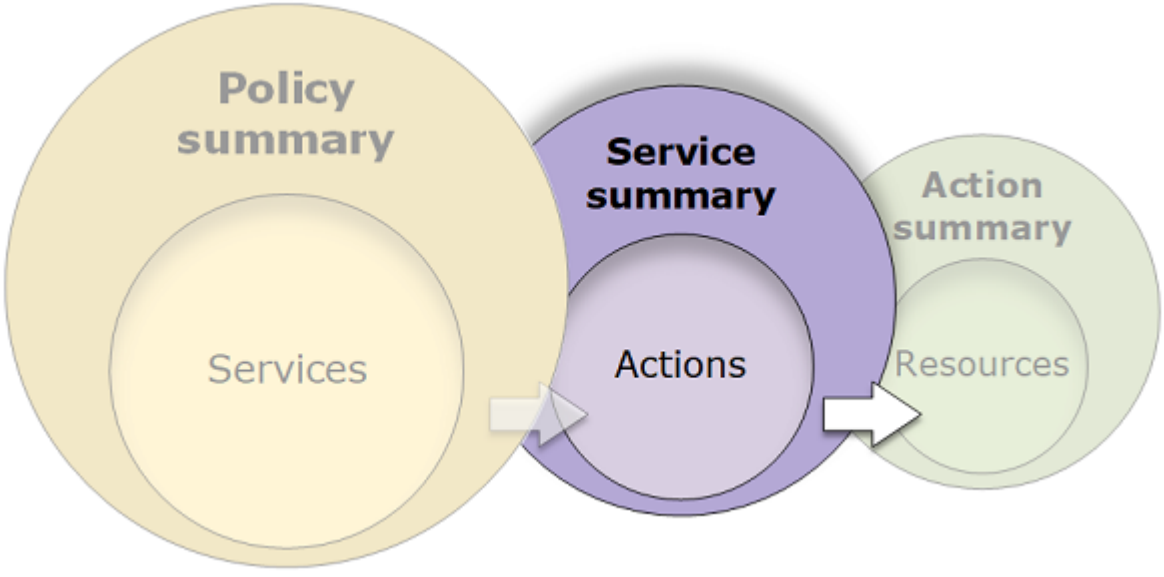
  도움말

  AWS 계정의 보안을 개선하려면 권한 관리 액세스 레벨 분류를 포함하는 정책을 제한하거나 정기적으로 모니터링합니다.
- 태그 지정: 리소스 태그의 상태만 변경하는 작업을 수행할 수 있는 권한입니다. 예를 들어 IAM 작업 `TagRole` 및 `UntagRole`은 역할에 대한 태그 지정 또는 태그 취소만 허용하므로 태그 지정 액세스 레벨입니다. 그러나 `CreateRole` 작업은 사용자가 역할을 생성할 때 역할 리소스에 태그를 지정하도록 허용합니다. 이 작업은 태그를 추가하는 것만이 아니므로 `Write` 액세스 레벨입니다.

특정 서비스의 모든 작업에 대한 액세스 레벨 분류를 보려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

서비스 요약(작업 목록)

정책은 3가지 테이블, 즉 정책 요약 (p. 484), 서비스 요약, 작업 요약 (p. 497)으로 요약됩니다. 서비스 요약 테이블에는 작업 목록과 선택한 서비스의 정책에 의해 정의된 권한의 요약이 포함되어 있습니다.



권한을 부여하는 정책 요약에 나열되어 있는 각 서비스에 대해 서비스 요약을 볼 수 있습니다. 이 테이블은 Uncategorized actions(미분류 작업), Uncategorized resource types(미분류 리소스 유형) 및 액세스 수준 섹션으로 분류되어 있습니다. IAM에서 인식하지 못하는 작업이 정책에 포함되어 있으면 해당 작업은 테이블의 Uncategorized actions(미분류 작업) 섹션에 포함됩니다. IAM에서 작업을 인식하면 해당 작업은 테이블의 액세스 레벨(목록, 읽기, 쓰기, 권한 관리) 섹션 중 하나에 포함됩니다. 서비스의 각 작업에 할당된 액세스 레벨 분류를 보려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

서비스 요약 보기

정책 페이지에서 관리형 정책에 대한 서비스 요약을 보거나, 사용자 페이지 및 역할을 통해 사용자나 역할에 연결된 인라인 및 관리형 정책에 대한 서비스 요약을 볼 수 있습니다. 단, 관리형 정책의 사용자 페이지 또는 역할 페이지에서 서비스 이름을 선택한 경우에는 정책 페이지로 리디렉션됩니다. 관리형 정책에 대한 서비스 요약은 정책 페이지에서 확인해야 합니다.

관리형 정책의 서비스 요약을 확인하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 보려는 정책의 이름을 선택합니다.
4. 정책 요약을 보려면 해당 정책의 요약 페이지에서 권한 탭을 확인합니다.
5. 정책 요약 서비스 목록에서 확인하려는 서비스의 이름을 선택합니다.

사용자에게 연결된 정책의 서비스 요약을 확인하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 사용자 목록에서 정책을 보려는 사용자의 이름을 선택합니다.
4. 사용자에게 직접 연결되거나 그룹에서 연결된 정책의 목록을 보려면 해당 사용자의 요약 페이지에서 권한 탭을 봅니다.
5. 사용자에 대한 정책 테이블에서 보려는 정책의 행을 확장합니다.
6. 정책 요약 서비스 목록에서 확인하려는 서비스의 이름을 선택합니다.

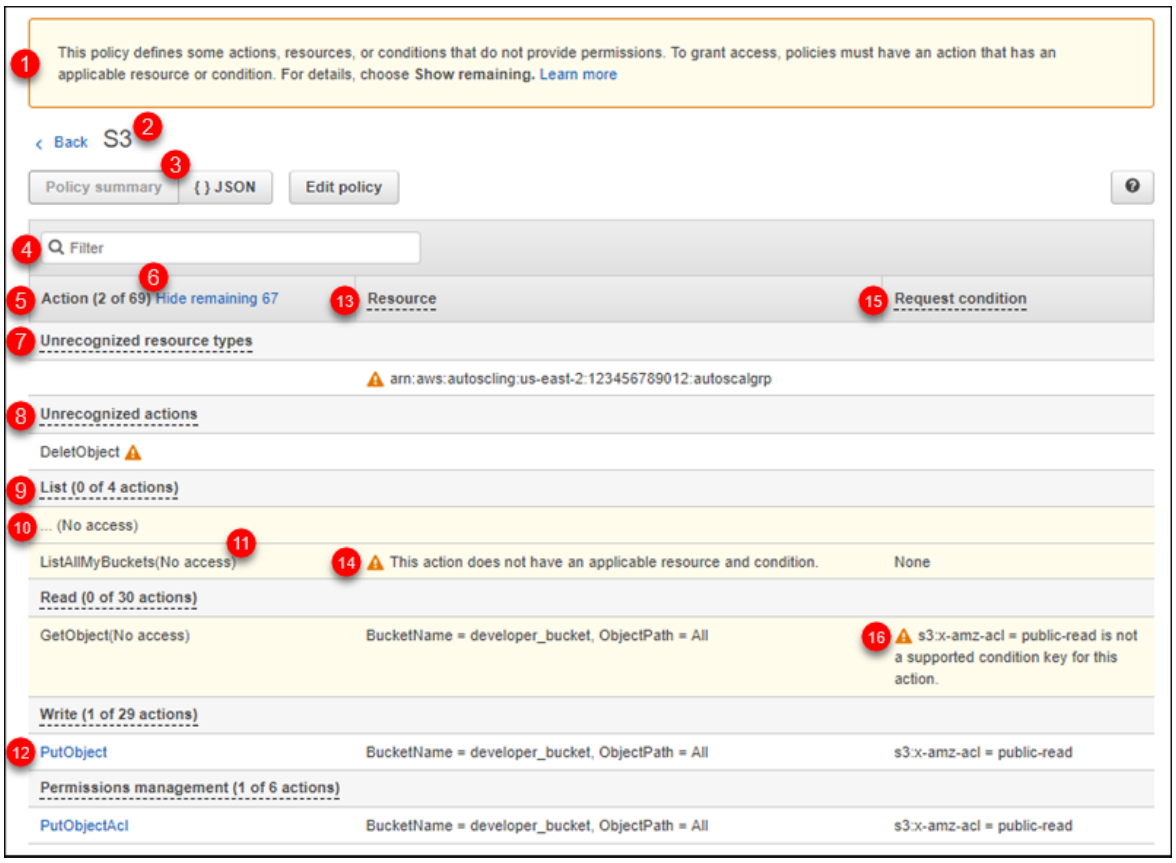
> **Note**
>
> 선택한 정책이 사용자에게 직접 연결된 인라인 정책인 경우 서비스 요약 테이블이 표시됩니다. 정책이 그룹에서 연결한 인라인 정책인 경우 해당 그룹의 JSON 정책 문서로 자동으로 이동합니다. 정책이 관리형 정책인 경우 정책 페이지에서 해당 정책의 서비스 요약이 게시된 부분으로 자동으로 이동합니다.

역할에 연결된 정책의 서비스 요약 정보를 보려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택합니다.
3. 역할 목록에서 정책을 보려는 역할의 이름을 선택합니다.
4. 역할의 요약 페이지에서 권한 탭을 보고 역할에 연결된 정책 목록을 확인합니다.
5. 역할에 대한 정책 테이블에서 보려는 정책의 행을 확장합니다.
6. 정책 요약 서비스 목록에서 확인하려는 서비스의 이름을 선택합니다.

서비스 요약의 요소 이해하기

아래 예제는 SummaryAllElements 정책 요약에서 허용한 Amazon S3 작업의 서비스 요약입니다(the section called “SummaryAllElements JSON 정책 문서” (p. 490) 참조). 이 서비스에 대한 작업은 Uncategorized actions(미분류 작업), Uncategorized resource types(미분류 리소스 유형) 및 액세스 레벨로 그룹화됩니다. 예를 들어 서비스에서 이용 가능한 총 21개 쓰기 작업 중에서 2개 쓰기 작업이 정의됩니다.



관리형 정책에 대한 서비스 요약 페이지에 포함되는 정보는 다음과 같습니다.

1. 정책에서 정책의 서비스에 대해 정의된 일부 작업, 리소스 및 조건에 권한을 부여하지 않는 경우 페이지 상단에 경고 배너가 나타납니다. 그런 다음 서비스 요약에 문제에 대한 세부 정보가 포함됩니다. 정책 요약이 정책에서 부여하는 권한을 이해하고 문제를 해결하는 데 얼마나 도움이 되는지 알아보려면 the section called “정책이 필요한 권한을 부여하지 않음” (p. 543) 단원을 참조하십시오.
2. 뒤로 링크 옆에 서비스 이름(이 경우 S3)이 표시됩니다. 이 서비스의 서비스 요약에는 정책에서 정의한 허용되는 작업의 목록이 수록되어 있습니다. 그 대신, 서비스 이름 옆에 (명시적으로 거부됨) 텍스트가 표시된 경우 서비스 요약 테이블에 나열된 작업은 명시적으로 거부됩니다.
3. { } JSON을 선택하면 정책에 대한 추가 세부 정보를 볼 수 있습니다. 이를 통해 작업에 적용된 모든 조건을 볼 수 있습니다. (사용자에게 직접 연결된 인라인 정책의 서비스 요약을 보려면 서비스 요약 대화 상자를 닫고 정책 요약으로 돌아가 JSON 정책 문서에 액세스해야 합니다.)
4. 특정 작업의 요약을 보려면 검색 상자에 키워드를 입력하여, 사용할 수 있는 작업의 목록을 줄이십시오.
5. 작업(69개 중 2개 작업) – 이 열에는 정책 내에 정의된 작업이 나열되고 각 작업에 해당하는 리소스와 조건이 제시됩니다. 정책에서 작업에 권한을 부여한 경우 작업 이름이 작업 요약 (p. 497) 테이블에 링크됩니다. 개수는 권한을 제공하는 인식할 수 있는 작업의 수를 나타냅니다. 총계는 서비스에 대해 알려진 작업의 수입니다. 이 예제에서는 총 69개의 알려진 S3 작업에서 2개의 작업이 권한을 제공합니다.
6. Show/Hide remaining 67(나머지 67개 작업 보기/숨기기) – 알려졌지만 이 서비스에 대한 권한을 제공하지 않는 작업을 포함하는 테이블을 확장하거나 숨기려면 이 링크를 선택합니다. 링크를 확장하면 권한을 제공하지 않는 모든 요소에 대해 경고가 표시됩니다.

7. Unrecognized resource types(인식되지 않은 리소스 유형) – 이 정책에, 이 서비스에 대한 정책 내에서 인식되지 않은 리소스 유형이 한 개 이상 있습니다. 이 경고를 사용하여 리소스 유형에 오타가 포함되어 있는지 확인할 수 있습니다. 리소스 유형이 정확하면 서비스는 정책 요약을 완전히 지원할 수 없거나 프리뷰에 있거나 사용자 지정 서비스일 수 있습니다. 일반적으로 사용할 수 있는(GA) 서비스에서 특정 리소스 유형에 대한 정책 요약 지원을 요청하려면 서비스가 IAM 정책 요약을 지원하지 않음 (p. 542)을 참조하십시오. 이 예제에서는 `autoscling` 서비스 이름에 `a`가 누락되었습니다.
8. Unrecognized actions(인식되지 않은 작업) – 이 정책에, 이 서비스에 대한 정책 내에서 인식되지 않은 작업이 한 개 이상 있습니다. 이 경고를 사용하여 작업에 오타가 포함되어 있는지 확인할 수 있습니다. 작업 이름이 정확하면 서비스는 정책 요약을 완전히 지원할 수 없거나 프리뷰에 있거나 사용자 지정 서비스일 수 있습니다. 일반적으로 사용할 수 있는(GA) 서비스에서 특정 작업에 대한 정책 요약 지원을 요청하려면 서비스가 IAM 정책 요약을 지원하지 않음 (p. 542)을 참조하십시오. 이 예제에서는 `DeletObject` 작업에 `e`가 누락되었습니다.

   Note

   IAM은 정책 요약을 지원하는 서비스의 이름, 작업 및 리소스 유형을 검토합니다. 그러나 존재하지 않는 리소스 값이나 조건이 정책 요약에 포함될 수 있습니다. 항상 정책 시뮬레이터 (p. 441)로 정책을 테스트합니다.
9. IAM에서 인식하는 해당 작업의 경우 테이블은 정책이 허용하거나 거부하는 액세스 레벨에 따라 최소 1개 이상에서 최대 4개의 섹션으로 이러한 작업을 그룹화합니다. 섹션은 목록, 읽기, 쓰기, 권한 관리입니다. 각 액세스 레벨 내에서 사용할 수 있는 총 작업 수로부터 정의된 작업 수도 확인할 수 있습니다. 서비스의 각 작업에 할당된 액세스 레벨 분류를 보려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.
10. 줄임표(…)는 모든 작업이 페이지에 포함되었지만 이 정책과 관련된 정보가 있는 행만 표시되었음을 나타냅니다. AWS Management 콘솔에서 이 페이지를 보면 서비스에 대한 모든 작업을 볼 수 있습니다.
11. (No access)(액세스 권한 없음) – 이 정책에 권한을 제공하지 않는 작업이 한 개 있습니다.
12. 권한을 제공하지 않는 작업에는 작업 요약에 대한 링크가 포함됩니다.
13. 리소스 – 이 열은 정책이 서비스에 대해 정의한 리소스를 보여줍니다. IAM은 리소스가 각 작업에 적용되는지 여부를 확인하지 않습니다. 이 예제에서는 S3 서비스의 작업이 `developer_bucket` Amazon S3 버킷 리소스에서만 허용됩니다. 서비스가 IAM에 제공하는 정보에 따라 `arn:aws:s3:::developer_bucket/*` 등의 ARN이 표시되거나 `BucketName = developer_bucket` 등의 정의된 리소스 유형이 표시될 수 있습니다.

    Note

    이 열은 다른 서비스의 리소스를 포함할 수 있습니다. 리소스를 포함하는 정책 설명에 동일한 서비스의 작업과 리소스를 모두 포함하지 않으면 정책에 일치하지 않는 리소스가 포함됩니다. IAM은 정책을 생성하거나 정책 요약에서 정책을 볼 때 일치하지 않는 리소스에 대해 경고하지 않습니다. 또한 IAM은 작업이 리소스에 적용되는지 여부는 나타내지 않고 서비스가 일치하는지 여부만 나타냅니다. 이 열에 일치하지 않는 리소스가 포함되어 있으면 정책에 오류가 있는지 검토해야 합니다. 정책을 더 잘 이해하려면 항상 정책 시뮬레이터 (p. 441)로 테스트합니다.
14. 리소스 경고 – 전체 권한을 제공하지 않는 리소스를 포함하는 작업의 경우 다음 경고 중 하나가 나타납니다.
    - This action does not support resource-level permissions. 리소스에 대하여 와일드카드(*)가 필요합니다. – 정책에 리소스 수준 권한이 있지만, 이 작업에 대한 권한을 제공하려면 `"Resource": ["*"]`를 포함해야 함을 의미합니다.
    - 이 작업은 적용할 리소스가 없습니다. – 지원되는 리소스 없이 작업이 정책에 포함됨을 의미합니다.
    - 이 작업은 적용할 리소스 및 조건이 없습니다. – 지원되는 리소스 및 조건 없이 작업이 정책에 포함됨을 의미합니다. 이 경우 이 서비스의 정책에 포함된 조건도 있지만 이 작업에 적용되는 조건은 없습니다.

    `ListAllMyBuckets` 작업의 경우 리소스 수준 권한을 지원하지 않고 `s3:x-amz-acl` 조건 키를 지원하지 않기 때문에 이 정책에 마지막 경고가 포함됩니다. 리소스 문제나 조건 문제를 수정한 경우 나머지 문제가 세부 경고에 나타납니다.
15. Request condition(요청 조건) – 이 열은 리소스와 연결된 작업에 조건이 적용되는지 여부를 나타냅니다. 이러한 조건에 대해 자세히 알아보려면 { } JSON을 선택하여 JSON 정책 문서를 검토합니다.

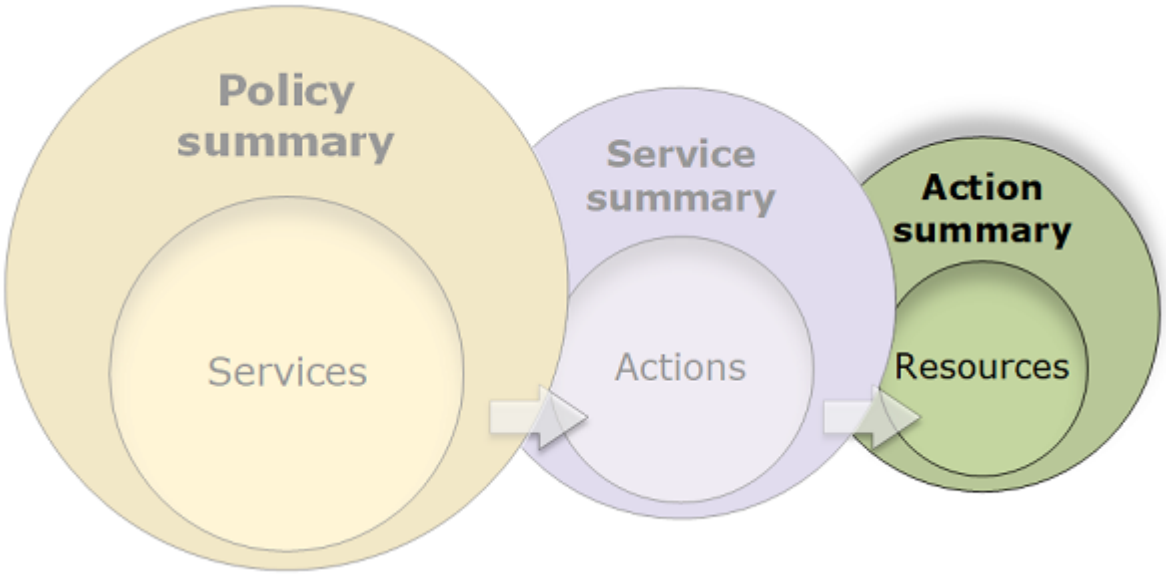
16.Condition warning(조건 경고) – 전체 권한을 제공하지 않는 조건을 포함하는 작업의 경우 다음 경고 중 하나가 나타납니다.

- <CONDITION_KEY>는 이 작업에 대해 지원되는 조건 키가 아닙니다. – 정책에 이 작업에 지원되지 않는 서비스 조건 키가 한 개 있습니다.
- 해당 작업은 여러 개의 조건 키를 지원하지 않습니다. – 정책에 이 작업에 지원되지 않는 서비스 조건 키가 두 개 이상 있습니다.

`GetObject`의 경우 이 정책에 `s3:x-amz-acl` 조건 키가 포함되며 이 키는 이 작업에서 작동하지 않습니다. 작업이 리소스를 지원하더라도, 조건이 이 작업에 대해 true가 되지 않기 때문에 정책에서 이 작업을 위한 권한을 부여하지 않습니다.

작업 요약(리소스 목록)

정책은 3가지 테이블, 즉 정책 요약 (p. 484), 서비스 요약 (p. 493), 작업 요약으로 요약됩니다. 작업 요약 테이블에는 리소스 목록과 선택한 작업에 적용되는 연결 조건이 포함되어 있습니다.



권한을 부여하는 각 작업에 대한 작업 요약을 보려면 서비스 요약의 링크를 선택합니다. 작업 요약 테이블에는 리소스의 리전 및 계정을 비롯하여 리소스에 대한 세부 정보가 포함되어 있습니다. 또한 각 리소스에 적용하는 조건을 볼 수 있습니다. 이를 통해 일부 리소스에 적용되고 다른 리소스에는 적용되지 않는 조건을 볼 수 있습니다.

작업 요약 보기

사용자 페이지에서는 사용자에게 연결된 정책에 대한 작업 요약을 볼 수 있습니다. 역할 페이지에서는 역할에 연결된 정책에 대한 작업 요약을 볼 수 있습니다. 정책 페이지에서는 관리형 정책에 대한 작업 요약을 볼 수 있습니다. 그러나 사용자 또는 역할 페이지에서 관리형 정책에 대한 작업 요약을 보려고 하면 정책 페이지로 리디렉션됩니다.

관리형 정책의 작업 요약을 확인하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 보려는 정책의 이름을 선택합니다.

4. 정책 요약을 보려면 해당 정책의 요약 페이지에서 권한 탭을 확인합니다.
5. 정책 요약 서비스 목록에서 확인하려는 서비스의 이름을 선택합니다.
6. 작업의 서비스 요약 목록에서 확인하려는 작업의 이름을 선택합니다.

사용자에게 연결된 정책의 작업 요약을 확인하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자를 선택합니다.
3. 사용자 목록에서 정책을 보려는 사용자의 이름을 선택합니다.
4. 사용자에게 직접 연결되거나 그룹에서 연결된 정책의 목록을 보려면 해당 사용자의 요약 페이지에서 권한 탭을 봅니다.
5. 사용자에 대한 정책 테이블에서 보려는 정책의 행을 확장합니다.
6. 정책 요약 서비스 목록에서 확인하려는 서비스의 이름을 선택합니다.

   Note

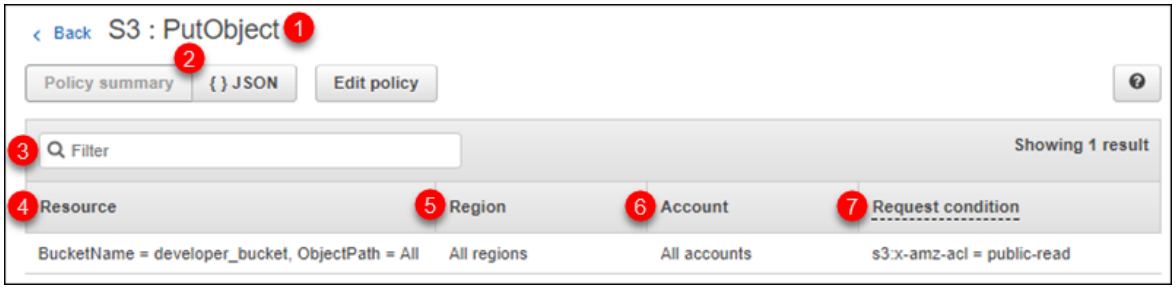
   선택한 정책이 사용자에게 직접 연결된 인라인 정책인 경우 서비스 요약 테이블이 표시됩니다. 정책이 그룹에서 연결한 인라인 정책인 경우 해당 그룹의 JSON 정책 문서로 자동으로 이동합니다. 정책이 관리형 정책인 경우 정책 페이지에서 해당 정책의 서비스 요약이 게시된 부분으로 자동으로 이동합니다.
7. 작업의 서비스 요약 목록에서 확인하려는 작업의 이름을 선택합니다.

역할 연결된 정책의 작업 요약을 보려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택합니다.
3. 역할 목록에서 정책을 보려는 역할의 이름을 선택합니다.
4. 역할의 요약 페이지에서 권한 탭을 보고 역할에 연결된 정책 목록을 확인합니다.
5. 역할에 대한 정책 테이블에서 보려는 정책의 행을 확장합니다.
6. 정책 요약 서비스 목록에서 확인하려는 서비스의 이름을 선택합니다.
7. 작업의 서비스 요약 목록에서 확인하려는 작업의 이름을 선택합니다.

작업 요약의 요소 이해하기

아래 예제는 Amazon S3 서비스 요약의 `PutObject`(쓰기) 작업에 대한 작업 요약입니다(서비스 요약(작업 목록) (p. 493) 참조). 이 작업의 경우 정책이 단일 리소스에 대한 여러 조건을 정의합니다.



작업 요약 페이지에 포함되는 정보는 다음과 같습니다.

1. 뒤로 링크 옆에 서비스와 작업의 이름이 형식 `service: action`으로 표시됩니다(이 경우 S3: PutObject). 이 서비스의 작업 요약에는 정책에서 정의된 리소스의 목록이 포함되어 있습니다.
2. { } JSON을 선택하면 작업에 적용되는 여러 가지 조건 등 정책에 관한 추가 세부 정보를 볼 수 있습니다. (사용자에게 직접 연결된 인라인 정책에 대한 작업 요약을 보는 경우에는 단계가 달라집니다. 그러한 경우에 JSON 정책 문서에 액세스하려면 작업 요약 대화 상자를 닫고 정책 요약으로 돌아가야 합니다.)
3. 특정 리소스의 요약을 보려면 검색 상자에 키워드를 입력하여 사용할 수 있는 리소스의 목록을 줄입니다.
4. 리소스 – 이 열에는 정책이 선택한 서비스에 대해 정의한 리소스가 나열됩니다. 이 예제에서는 PutObject 작업이 모든 객체 경로와 `developer_bucket` Amazon S3 버킷 리소스에서만 허용됩니다. 서비스가 IAM에 제공하는 정보에 따라 `arn:aws:s3:::developer_bucket/*` 등의 ARN이 표시되거나 `BucketName = developer_bucket, ObjectPath = All` 등의 정의된 리소스 유형이 표시될 수 있습니다.
5. 리전 – 이 열은 리소스가 정의된 리전을 보여줍니다. 리소스는 모든 리전 또는 단일 리전에 대해 정의할 수 있습니다. 리소스는 둘 이상의 리전에 존재할 수 없습니다.
   - All regions(모든 리전) – 리소스와 연결된 작업은 모든 리전에 적용됩니다. 이 예제에서는 작업이 전역적 서비스 Amazon S3에 속합니다. 전역적 서비스에 속하는 작업은 모든 리전에 적용됩니다.
   - Region text(리전 텍스트) – 리소스와 연결된 작업은 한 리전에 적용됩니다. 예를 들어 정책은 리소스에 대한 `us-east-2` 리전을 지정할 수 있습니다.
6. 계정 – 이 열은 리소스와 연결된 서비스 또는 작업이 특정 계정에 적용되는지를 나타냅니다. 리소스는 모든 계정 또는 단일 계정에 존재할 수 있습니다. 리소스는 둘 이상의 특정 계정에 존재할 수 없습니다.
   - All accounts(모든 계정) – 리소스와 연결된 작업은 모든 계정에 적용됩니다. 이 예제에서는 작업이 전역적 서비스 Amazon S3에 속합니다. 전역적 서비스에 속하는 작업은 모든 계정에 적용됩니다.
   - This account(현재 계정) – 리소스와 연결된 작업은 현재 로그인된 계정에만 적용됩니다.
   - Account number(계정 번호) – 리소스와 연결된 작업은 하나의 계정(현재 로그인되지 않은 계정)에 적용됩니다. 예를 들어 정책이 리소스에 대한 `123456789012` 계정을 지정하면 계정 번호가 정책 요약에 나타납니다.
7. Request condition(요청 조건) – 이 열은 리소스와 연결된 작업에 조건이 적용되는지를 보여줍니다. 이 예제에는 `s3:x-amz-acl = public-read` 조건이 포함됩니다. 이러한 조건에 대해 자세히 알아보려면 { } JSON을 선택하여 JSON 정책 문서를 검토합니다.

정책 요약 예제

다음 예제에는 정책을 통해 부여되는 권한을 이해하는 데 도움이 되는 JSON 정책과 그에 연결된 정책 요약 (p. 484), 서비스 요약 (p. 493), 작업 요약 (p. 497)이 포함되어 있습니다.

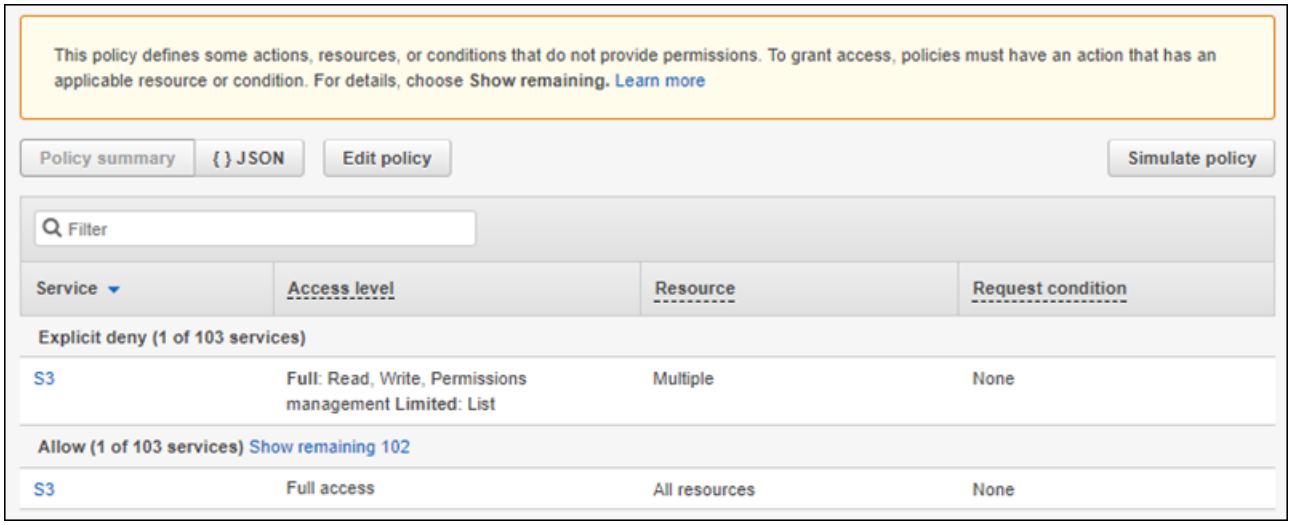
정책 1: DenyCustomerBucket

이 정책은 동일한 서비스에 대한 허용과 거부를 보여줍니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "FullAccess",
            "Effect": "Allow",
            "Action": ["s3:*"],
            "Resource": ["*"]
        },
        {
            "Sid": "DenyCustomerBucket",
            "Action": ["s3:*"],
            "Effect": "Deny",
            "Resource": ["arn:aws:s3:::customer", "arn:aws:s3:::customer/*" ]
        }
```

```
    ]
}
```

DenyCustomerBucket 정책 요약:



DenyCustomerBucket S3 (Explicit deny) 서비스 요약:

Action (66 of 69) Hide remaining 3	Resource	Request condition
List (1 of 4 actions)		
HeadBucket (No access)	⚠ This action does not support resource-level permissions. This requires a wildcard (*) for the resource.	None
ListAllMyBuckets(No access)	⚠ This action does not support resource-level permissions. This requires a wildcard (*) for the resource.	None
ListBucket	BucketName = customer	None
ListObjects (No access)	⚠ This action does not support resource-level permissions. This requires a wildcard (*) for the resource.	None
Read (30 of 30 actions)		
GetAccelerateConfiguration	BucketName = customer	None
GetAnalyticsConfiguration	BucketName = customer	None
GetBucketAcl	BucketName = customer	None
GetBucketCORS	BucketName = customer	None
GetBucketLocation	BucketName = customer	None
GetBucketLogging	BucketName = customer	None
GetBucketNotification	BucketName = customer	None
GetBucketPolicy	BucketName = customer	None
GetBucketRequestPayment	BucketName = customer	None
GetBucketTagging	BucketName = customer	None
GetBucketVersioning	BucketName = customer	None
GetBucketWebsite	BucketName = customer	None
GetInventoryConfiguration	BucketName = customer	None
GetIpConfiguration	BucketName = customer	None
GetLifecycleConfiguration	BucketName = customer	None
GetMetricsConfiguration	BucketName = customer	None
GetObject	BucketName = customer, ObjectPath = All	None
GetObjectAcl	BucketName = customer, ObjectPath = All	None
GetObjectTagging	BucketName = customer, ObjectPath = All	None
GetObjectTorrent	BucketName = customer, ObjectPath = All	None
GetObjectVersion	BucketName = customer, ObjectPath = All	None

GetObject(읽기) 작업 요약:

Resource	Region	Account	Request condition
BucketName = customer, ObjectPath = All	All regions	All accounts	None

정책 2: DynamoDbRowCognitoID

이 정책은 사용자의 Amazon Cognito ID를 기반으로 Amazon DynamoDB에 대한 행 수준 액세스 권한을 제공합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:DeleteItem",
                "dynamodb:GetItem",
                "dynamodb:PutItem",
                "dynamodb:UpdateItem"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-west-1:123456789012:table/myDynamoTable"
            ],
            "Condition": {
                "ForAllValues:StringEquals": {
                    "dynamodb:LeadingKeys": [
                        "${cognito-identity.amazonaws.com:sub}"
                    ]
                }
            }
        }
    ]
}
```

DynamoDbRowCognitoID 정책 요약:

Service ▾	Access level	Resource	Request condition
Allow (1 of 102 services) Show remaining 101			
DynamoDB	**Limited**: Read, Write	TableName = myDynamoTable	dynamodb:LeadingKeys = ${cognito-identity.amazonaws.com:sub}

DynamoDbRowCognitoID DynamoDB(허용) 서비스 요약:

Action (4 of 25) Show remaining 21	Resource	Request condition
Read (1 of 14 actions)		
GetItem	TableName = myDynamoTable	dynamodb:LeadingKeys = ${cognito-identity.amazonaws.com:sub}
Write (3 of 10 actions)		
DeleteItem	TableName = myDynamoTable	dynamodb:LeadingKeys = ${cognito-identity.amazonaws.com:sub}
PutItem	TableName = myDynamoTable	dynamodb:LeadingKeys = ${cognito-identity.amazonaws.com:sub}
UpdateItem	TableName = myDynamoTable	dynamodb:LeadingKeys = ${cognito-identity.amazonaws.com:sub}

GetItem(나열) 작업 요약:

Resource	Region	Account	Request
TableName = myDynamoTable	us-west-1	123456789012	dynamod ${cognito identity.a

정책 3: MultipleResourceCondition

이 정책에는 다수의 리소스와 조건이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": ["arn:aws:s3:::Apple_bucket/*"],
            "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": ["arn:aws:s3:::Orange_bucket/*"],
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": ["custom"],
                "s3:x-amz-grant-full-control": ["1234"]
            }}
        }
    ]
}
```

MultipleResourceCondition 정책 요약:

Service	Access level	Resource	Reques
Allow (1 of 100 services) Show remaining 99			
S3	**Limited**: Write, Permissions management	Multiple	Multiple

MultipleResourceCondition S3(허용) 서비스 요약:

Action (2 of 52 actions) Show remaining 50	Resource	Request
Write (1 of 21 actions)		
PutObject	Multiple	Multiple
Permissions management (1 of 5 actions)		
PutObjectAcl	Multiple	Multiple

PutObject(쓰기) 작업 요약:

Resource	Region	Account	Request condition
BucketName = Orange_bucket, ObjectPath = All	All regions	All accounts	Multiple
BucketName = Apple_bucket, ObjectPath = All	All regions	All accounts	s3:x-amz-acl = public-read

정책 4: EC2_Troubleshoot

다음 정책을 통해 사용자는 실행 중인 Amazon EC2 인스턴스의 스크린샷을 만들어 EC2 문제 해결에 필요한 도움을 얻을 수 있습니다. 또한 이 정책은 Amazon S3 개발자 버킷의 항목에 대한 정보를 확인할 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetConsoleScreenshot"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::developer"
            ]
        }
    ]
}
```

EC2_Troubleshoot 정책 요약:

Service	Access level	Resource	Request condition
Allow (2 of 102 services) Show remaining 100			
EC2	**Limited**: Read	All resources	None
S3	**Limited**: List	BucketName = developer	None

EC2_Troubleshoot S3(허용) 서비스 요약:

Action (1 of 52) Show remaining 51	Resource	Request condition
List (1 of 4 actions)		
ListBucket	BucketName = developer	None

ListBucket(나열) 작업 요약:

Filter

Resource	Region	Account	Request
BucketName = developer	All regions	All accounts	None

정책 5: Unrecognized_Service_Action

다음 정책은 DynamoDB에 대한 모든 액세스 권한을 제공하기 위해 마련되었지만 `dynamodb`가 `dynamobd`로 잘못 입력되었기 때문에 해당 액세스는 실패합니다. 이 정책은 `us-east-2` 리전의 일부 Amazon EC2 작업에 대한 액세스를 허용하지만 `ap-northeast-2` 리전에 대한 해당 액세스를 거부하기 위

해 마련되었습니다. 그러나 `ap-northeast-2` 리전에서 인스턴스를 재부팅하기 위한 액세스는 o 작업 중에 인식할 수 없는 `RebootInstances`로 인해 명시적으로 거부되지 않습니다. 이 예제에서는 정책 요약을 사용하여 정책에서 오류를 찾는 방법을 보여줍니다. 정책 요약의 정보를 기반으로 정책을 편집하는 방법을 알아보려면 정책을 편집하여 경고 수정 (p. 485)을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "dynamobd:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Action": [
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:ReboootInstances"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "ap-northeast-2"
                }
            }
        },
        {
            "Action": [
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2"
                }
            }
        }
    ]
}
```

Unrecognized_Service_Action 정책 요약:

Service	Access level	Resource	Request condition
Unrecognized services			
dynamobd ⚠			
Explicit deny (1 of 103 services)			
EC2 ⚠	**Limited**: Write	All resources	ec2:Region = ap-northeast-2
Allow (1 of 103 services) Show remaining 102			
EC2	**Limited**: Write	All resources	ec2:Region = us-east-2

Unrecognized_Service_Action EC2 (Explicit deny) 서비스 요약:

Action (3 of 229) Show remaining 226	Resource	Request condition
Unrecognized actions		
RebootInstances ⚠		
Write (3 of 157 actions)		
RunInstances	All resources	ec2:Region = ap-northeast-2
StartInstances	All resources	ec2:Region = ap-northeast-2
StopInstances	All resources	ec2:Region = ap-northeast-2

Unrecognized_Service_Action StartInstances (Write) 작업 요약:

Resource	Region	Account	Request condition
All resources	All regions	All accounts	ec2:Region = ap-northeast-2

정책 6: CodeBuild_CodeCommit_CodeDeploy

이 정책은 특정 CodeBuild, CodeCommit, CodeDeploy 리소스에 대한 액세스 권한을 제공합니다. 이러한 리소스는 각 서비스에 고유하므로 일치하는 서비스에서만 나타납니다. `Action` 요소에 서비스와 일치하지 않는 리소스를 포함하는 경우 리소스가 모든 작업 요약에 나타납니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1487980617000",
            "Effect": "Allow",
            "Action": [
                "codebuild:*",
                "codecommit:*",
                "codedeploy:*"
            ],
            "Resource": [
                "arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project",
                "arn:aws:codecommit:us-east-2:123456789012:MyDemoRepo",
                "arn:aws:codedeploy:us-east-2:123456789012:application:WordPress_App",
                "arn:aws:codedeploy:us-east-2:123456789012:instance/AssetTag*"
            ]
        }
    ]
}
```

CodeBuild_CodeCommit_CodeDeploy 정책 요약:

Service ▾	Access level	Resource	Request condition
Allow (3 of 103 services) Show remaining 100			
CodeBuild	**Limited**: List, Read, Write	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
CodeCommit	**Full**: Read, Write **Limited**: List	arn:aws:codecommit:us-east-2:123456789012:MyDemoRepo	None
CodeDeploy	**Limited**: List, Read, Write	Multiple	None

CodeBuild_CodeCommit_CodeDeploy CodeBuild(허용) 서비스 요약:

Action (9 of 15) Show remaining 6	Resource	Request condition
List (1 of 3 actions)		
ListBuildsForProject	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
Read (2 of 5 actions)		
BatchGetBuilds	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
BatchGetProjects	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
Write (6 of 7 actions)		
BatchDeleteBuilds	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
CreateProject	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
DeleteProject	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
StartBuild	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
StopBuild	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None
UpdateProject	arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	None

CodeBuild_CodeCommit_CodeDeploy StartBuild (Write) 작업 요약:

Resource	Region	Account	Request condition
arn:aws:codebuild:us-east-2:123456789012:project/my-demo-project	us-east-2	123456789012	None

IAM 리소스에 액세스하는 데 필요한 권한

리소스는 서비스 내의 객체입니다. IAM에는 그룹, 사용자, 역할 및 정책이 있습니다. AWS 계정 루트 사용자 자격 증명으로 로그인한 경우 IAM 자격 증명 또는 IAM 리소스를 관리하는 데 아무런 제한이 없습니다. 하지만 IAM 사용자가 자격 증명이나 IAM 리소스를 관리하려면 그러한 권한이 명시적으로 부여되어야 합니다. 자격 증명 기반 정책을 사용자에 연결하여 권한을 부여할 수 있습니다.

> Note
>
> AWS 설명서 전체에서 특정 범주를 언급하지 않고 IAM 정책을 칭할 때는 자격 증명 기반 고객 관리형 정책을 의미합니다. 정책 범주에 대한 자세한 내용은 the section called “정책 및 권한” (p. 349) 단원을 참조하십시오.

IAM 자격 증명을 관리하기 위한 권한

IAM 그룹, 사용자, 역할 및 자격 증명을 관리하는 데 필요한 권한은 일반적으로 작업에 대한 API 작업에 해당합니다. 예를 들어 IAM 사용자를 생성하려면 해당하는 API 명령 `CreateUser`가 있는 `iam:CreateUser` 권

한이 있어야 합니다. IAM 사용자가 다른 IAM 사용자를 생성할 수 있도록 다음과 같은 IAM 정책을 해당 사용자에게 연결할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:CreateUser",
    "Resource": "*"
  }
}
```

정책에서 Resource 요소의 값은 작업 및 그 작업이 적용될 수 있는 리소스에 따라 다릅니다. 앞의 예에서 정책은 사용자가 어떤 사용자도 생성할 수 있도록 허용합니다(*는 모든 문자열을 나타내는 와일드카드). 반면에, 사용자가 자신의 액세스 키(API 작업 CreateAccessKey 및 UpdateAccessKey)만 변경할 수 있도록 하는 정책에는 일반적으로 Resource 요소가 포함됩니다. 이 경우 ARN에는 다음 예제와 같이 현재 사용자의 이름을 해석하는 변수(${aws:username})가 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListUsersForConsole",
            "Effect": "Allow",
            "Action": "iam:ListUsers",
            "Resource": "arn:aws:iam::*:*"
        },
        {
            "Sid": "ViewAndUpdateAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:UpdateAccessKey",
                "iam:CreateAccessKey",
                "iam:ListAccessKeys"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        }
    ]
}
```

앞의 예에서 ${aws:username}은 현재 사용자의 사용자 이름으로 변환되는 변수입니다. 정책 변수에 대한 자세한 내용은 IAM 정책 요소: 변수 및 태그 (p. 615) 단원을 참조하십시오.

작업 이름에 와일드카드 문자(*)를 사용하면 특정 작업에 관련된 모든 작업에 대한 권한을 쉽게 부여할 수 있습니다. 예를 들어 사용자가 IAM 작업을 수행할 수 있게 하려면 그 작업에 대해 iam:*를 사용하면 됩니다. 사용자가 액세스 키에 관련된 작업만 수행할 수 있게 하려면 정책 문의 iam:*AccessKey* 요소에 Action를 사용하면 됩니다. 이렇게 하면 사용자에게 CreateAccessKey, DeleteAccessKey, GetAccessKeyLastUsed, ListAccessKeys, UpdateAccessKey 작업을 수행할 수 있는 권한이 부여됩니다. (나중에 이름에 "AccessKey"가 포함되는 작업이 IAM에 추가될 경우에도 Action 요소에 대해 iam:*AccessKey*를 사용하며 사용자에게 새 작업에 대한 권한이 부여됩니다.) 다음 예는 사용자가 자신의 액세스 키에 속하는 모든 작업을 수행할 수 있게 허용하는 정책을 보여 줍니다(ACCOUNT-ID-WITHOUT-HYPHENS를 해당 AWS 계정 ID로 변경).

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:*AccessKey*",
    "Resource": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:user/${aws:username}"
  }
```

```
}
```

그룹 삭제와 같은 일부 작업에는 여러 작업이 포함됩니다. 즉, 먼저 그룹에서 사용자를 제거한 후 그룹의 정책을 분리 또는 삭제하고 나서 실제로 그룹을 삭제합니다. 사용자가 그룹을 삭제할 수 있게 하려는 경우 이러한 모든 관련 작업을 수행할 수 있는 권한을 부여해야 합니다.

AWS Management 콘솔에서의 작업 권한

앞의 예는 사용자가 AWS CLI 또는 AWS SDK를 사용하여 작업을 수행할 수 있게 허용하는 정책을 보여 줍니다.

사용자가 콘솔에서 작업할 경우 콘솔은 그룹, 사용자, 역할 및 정책을 나열하고 그룹, 사용자 또는 역할과 연결된 정책을 가져오는 요청을 IAM에 보냅니다. 또한 콘솔은 AWS 계정 정보와 보안 주체에 대한 정보를 가져오는 요청도 보냅니다. 보안 주체는 콘솔에서 요청하는 사용자입니다.

일반적으로 작업을 수행하려면 일치하는 작업만 정책에 포함해야 합니다. 사용자를 생성하려면 `CreateUser` 작업을 호출하는 권한이 필요합니다. 콘솔을 사용하여 작업을 수행할 때 경우에 따라 콘솔에서 리소스를 표시하고 나열하며 가져오거나 볼 권한이 있어야 합니다. 이는 콘솔을 탐색하여 지정된 작업을 수행하기 위해 필요합니다. 예를 들어 Jorge라는 사용자가 콘솔을 사용하여 자신의 액세스 키를 변경하려면 IAM 콘솔에서 사용자를 선택할 것입니다. 이 작업은 콘솔에서 `ListUsers` 요청을 생성하게 합니다. Jorge에게 `iam:ListUsers` 작업에 대한 권한이 없을 경우 사용자를 나열하려고 시도할 때 콘솔이 액세스를 거부합니다. 그 결과, Jorge는 `CreateAccessKey` 및 `UpdateAccessKey` 작업에 대한 권한이 있는 경우에도 자신의 이름과 액세스 키를 가져올 수 없습니다.

예를 들어 Bob이라는 사용자가 콘솔을 사용하여 자신의 액세스 키를 변경하려면 IAM 콘솔에서 사용자를 선택할 것입니다. 이 작업은 콘솔에서 `ListUsers` 요청을 생성하게 합니다. Bob에게 `iam:ListUsers` 작업에 대한 권한이 없을 경우 콘솔은 사용자를 조회하려고 시도할 때 액세스를 거부당합니다. 따라서 Bob은 `CreateAccessKey` 및 `UpdateAccessKey` 작업에 대한 권한이 있을 경우에도 자신의 이름과 액세스 키를 받지 못합니다.

사용자에게 AWS Management 콘솔에서 그룹, 사용자, 역할, 정책, 자격 증명을 관리할 수 있는 권한을 부여하려면 콘솔에서 수행하는 작업에 대한 권한도 포함시켜야 합니다. 사용자에게 이러한 권한들을 부여하는 데 사용할 수 있는 몇 가지 정책의 예를 보려면 IAM 리소스를 관리하기 위한 정책의 예 (p. 510) 단원을 참조하십시오.

전 AWS 계정에 권한 부여

계정의 IAM 사용자에게 리소스에 대한 액세스 권한을 직접 부여할 수 있습니다. 다른 계정의 사용자에게 리소스에 대한 액세스 권한이 필요한 경우, 권한을 포함하지만 특정 사용자와 연결되지 않는 엔터티인 IAM 역할을 만들 수 있습니다. 다른 계정의 사용자는 해당 역할을 사용하여 해당 역할에 할당된 권한에 따라 리소스에 액세스할 수 있습니다. 자세한 내용은 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공 (p. 178)를 참조하십시오.

> **Note**
>
> 일부 서비스는 자격 증명 기반 정책 및 리소스 기반 정책 (p. 372)에 설명된 대로 리소스 기반 정책을 지원합니다(Amazon S3, Amazon SNS, Amazon SQS 등). 그런 서비스의 역할 사용 대안은 공유할 리소스(버킷, 주제 또는 대기열)에 정책을 연결하는 것입니다. 리소스 기반 정책은 리소스에 대한 액세스 허가를 받은 AWS 계정을 지정할 수 있습니다.

한 서비스에서 다른 서비스에 액세스할 권한

많은 AWS 제품은 다른 AWS 제품에 액세스합니다. 예를 들어, 어떤 AWS 제품(Amazon EMR, Elastic Load Balancing, Amazon EC2 Auto Scaling 등)은 Amazon EC2 인스턴스를 관리하고 다른 AWS 제품은 Amazon S3 버킷, Amazon SNS 주제, Amazon SQS 대기열 등을 사용합니다.

이러한 경우 권한 관리 시나리오가 서비스별로 다릅니다. 다음은 다양한 서비스에 대한 권한을 처리하는 방법의 예입니다.

- Amazon EC2 Auto Scaling에서 사용자는 Auto Scaling을 사용할 권한이 있어야 하지만, 이 사용자에게 Amazon EC2 인스턴스를 관리할 권한을 명시적으로 부여할 필요는 없습니다.
- AWS Data Pipeline에서 IAM 역할은 파이프라인에서 수행할 수 있는 작업을 결정합니다. 또한 사용자에게는 해당 역할을 수임할 권한이 필요합니다. (자세한 내용은 AWS Data Pipeline 개발자 안내서의 Granting Permissions to Pipelines with IAM 단원을 참조하십시오.)

AWS 제품에서 원하는 작업을 수행할 수 있도록 권한을 적절히 구성하는 방법에 대한 자세한 내용은 요청할 서비스 설명서를 참조하십시오. 서비스에 대한 역할을 생성하는 방법에 대해 알아보려면 AWS 서비스에 대한 권한을 위임할 역할 생성 (p. 233) 단원을 참조하십시오.

사용자를 대신하여 작동하도록 IAM 역할로 서비스 구성

AWS 서비스를 사용자를 대신하여 작동하도록 구성하려면 일반적으로 서비스에서 수행할 수 있는 작업을 정의하는 IAM 역할의 ARN을 입력합니다. AWS는 사용자에게 서비스에 역할을 전달할 권한이 있는지 확인합니다. 자세한 내용은 사용자에게 AWS 서비스에 역할을 전달할 권한 부여 (p. 254)를 참조하십시오.

필수 작업

작업은 리소스 보기, 생성, 편집 및 삭제와 같이 리소스에 대해 수행할 수 있는 사항입니다. 작업은 각 AWS 서비스별로 정의됩니다.

누군가 작업을 수행할 수 있도록 허용하려면 호출 자격 증명 또는 영향을 받은 리소스에 적용되는 정책에 필요한 작업을 포함시켜야 합니다. 일반적으로 작업을 수행하는 데 필요한 권한을 제공하려면 정책에 해당 작업을 포함시켜야 합니다. 예를 들어 사용자를 생성하려면 정책에 CreateUser 작업을 추가해야 합니다.

경우에 따라 정책에 관련된 작업을 추가로 포함해야 할 수도 있습니다. 예를 들어, `ds:CreateDirectory` 작업을 사용하여 AWS Directory Service에서 누군가에게 디렉터리를 생성할 권한을 제공하려면 정책에 다음 작업을 포함시켜야 합니다.

- `ds:CreateDirectory`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:CreateSecurityGroup`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:AuthorizeSecurityGroupEgress`

시각적 편집기를 사용하여 정책을 생성하거나 편집할 때 경고 및 정책에 필요한 모든 작업을 선택하라는 메시지가 표시됩니다.

AWS Directory Service에서 디렉터리를 생성하는 데 필요한 권한에 대한 자세한 내용은 예제 2: 사용자에게 디렉터리 생성 허용을 참조하십시오.

IAM 리소스를 관리하기 위한 정책의 예

다음은 사용자가 IAM 사용자, 그룹 및 자격 증명을 관리하기 위한 작업을 수행할 수 있게 하는 IAM 정책의 예시입니다. 여기에는 사용자가 자신의 암호, 액세스 키 및 멀티 팩터 인증(MFA) 디바이스를 관리할 수 있게 하는 정책이 포함됩니다.

사용자가 다른 AWS 제품(Amazon S3, Amazon EC2, DynamoDB 등)으로 작업을 수행할 수 있도록 허용하는 예제 정책은 IAM 자격 증명 기반 정책 예제 (p. 387) 단원을 참조하십시오.

주제

사용자가 보고를 목적으로 계정의 그룹, 사용자, 정책 및 그 이상의 정보를 조회할 수 있도록 허용

다음 정책은 사용자가 `Get` 또는 `List` 문자열로 시작하는 모든 IAM 작업을 호출하고, 보고서를 생성할 수 있게 허용합니다. 예시 정책을 보려면 IAM: IAM 콘솔에 대한 읽기 전용 액세스 허용 (p. 420) 단원을 참조하십시오.

사용자가 그룹의 멤버십을 관리할 수 있도록 허용

다음 정책은 사용자가 MarketingGroup이라는 그룹의 멤버십을 업데이트할 수 있도록 허용합니다. 예시 정책을 보려면 IAM: 프로그래밍 방식으로, 그리고 콘솔에서 그룹의 멤버십을 관리하도록 허용 (p. 417) 단원을 참조하십시오.

IAM 사용자를 관리할 수 있도록 허용

다음 정책은 사용자가 IAM 사용자 관리와 관련된 모든 작업을 수행할 수 있게 허용하지만 그룹이나 정책의 생성과 같은 다른 엔터티에 대한 작업 수행은 허용하지 않습니다. 허용되는 작업은 다음과 같습니다.

- 사용자 생성(`CreateUser` 작업).
- 사용자 삭제. 이 작업은 `DeleteSigningCertificate`, `DeleteLoginProfile`, `RemoveUserFromGroup`, `DeleteUser` 작업 모두를 수행할 수 있는 권한이 필요합니다.
- 계정 및 그룹의 사용자 조회(`GetUser`, `ListUsers`, `ListGroupsForUser` 작업).
- 사용자의 정책 조회 및 제거(`ListUserPolicies`, `ListAttachedUserPolicies`, `DetachUserPolicy`, `DeleteUserPolicy` 작업).
- 사용자의 경로 이름 바꾸기 또는 변경(`UpdateUser` 작업). `Resource` 요소에는 소스 경로와 대상 경로를 모두 다루는 ARN이 포함되어야 합니다. 경로에 대한 자세한 내용은 표시 이름 및 경로 (p. 563) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUsersToPerformUserActions",
            "Effect": "Allow",
            "Action": [
                "iam:ListPolicies",
                "iam:GetPolicy",
                "iam:UpdateUser",
                "iam:AttachUserPolicy",
                "iam:ListEntitiesForPolicy",
                "iam:DeleteUserPolicy",
                "iam:DeleteUser",
                "iam:ListUserPolicies",
                "iam:CreateUser",
                "iam:RemoveUserFromGroup",
                "iam:AddUserToGroup",
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:PutUserPolicy",
                "iam:ListAttachedUserPolicies",
                "iam:ListUsers",
                "iam:GetUser",
                "iam:DetachUserPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUsersToSeeStatsOnIAMConsoleDashboard",
            "Effect": "Allow",
            "Action": [
                "iam:GetAccount*",
                "iam:ListAccount*"
            ],
            "Resource": "*"
        }
    ]
}
```

위의 정책에 포함된 많은 권한은 사용자가 AWS Management 콘솔에서 작업을 수행하도록 허용합니다. 사용자가 AWS CLI, AWS SDK 또는 IAM HTTP 쿼리 API를 사용하여 사용자 관련 작업을 수행할 경우 특정 권한이 필요하지 않을 수 있습니다. 예를 들어 사용자가 어떤 사용자에게서 연결을 해제할 정책의 ARN을 이미 알고 있다면 `iam:ListAttachedUserPolicies` 권한이 필요하지 않습니다. 사용자에게 필요한 권한의 정확한 목록은 사용자가 다른 사용자를 관리할 때 수행해야 하는 작업에 따라 다릅니다.

정책에 있는 다음 권한들은 AWS Management 콘솔을 통해 사용자 작업에 액세스할 수 있도록 허용합니다.

- `iam:GetAccount*`
- `iam:ListAccount*`

사용자가 계정 암호 정책을 설정할 수 있도록 허용

일부 사용자들에게 AWS 계정의 암호 정책 (p. 101)을 확인하고 업데이트할 수 있는 권한을 부여할 수도 있습니다. 예시 정책을 보려면 IAM: 프로그래밍 방식으로, 그리고 콘솔에서 계정 암호 요구 사항을 설정하도록 허용 (p. 421) 단원을 참조하십시오.

사용자가 IAM 자격 증명 보고서를 생성하고 검색할 수 있도록 허용

AWS 계정에 있는 모든 사용자가 나열된 보고서를 생성하고 다운로드할 수 있는 권한을 사용자에게 부여할 수 있습니다. 이 보고서에는 암호, 액세스 키, MFA 디바이스, 서명 인증서를 포함한 다양한 사용자 자격 증명의 상태도 나열됩니다. 자격 증명 보고서에 대한 자세한 내용은 AWS 계정의 자격 증명 보고서 가져오기 (p. 156) 단원을 참조하십시오. 예시 정책을 보려면 IAM: IAM 자격 증명 보고서 생성 및 검색 (p. 417) 단원을 참조하십시오.

모든 IAM 작업 허용 (관리자 액세스 권한)

일부 사용자들에게 암호, 액세스 키, MFA 디바이스, 사용자 인증서 관리를 비롯하여 IAM에서의 모든 작업을 수행할 수 있는 권한을 부여할 수 있습니다. 다음 예시와 같은 정책은 이러한 권한들을 부여합니다.

> Warning
>
> 사용자에게 IAM에 대한 모든 액세스 권한을 부여하면 해당 사용자가 자기 자신 또는 다른 사용자에게 부여할 수 있는 권한에 제한이 없습니다. 사용자는 새로운 IAM 엔터티(사용자나 역할)을 생성하고 그러한 엔터티에 AWS 계정의 모든 리소스에 대한 모든 액세스 권한을 부여할 수 있습니다. 사용

자에게 IAM에 대한 모든 액세스 권한을 부여하면 실제로 사용자들에게 AWS 계정의 모든 리소스에 대한 모든 액세스 권한을 부여하는 것입니다. 여기에는 모든 리소스를 삭제하는 권한도 포함됩니다. 이러한 권한은 신뢰할 수 있는 관리자에게만 부여해야 하며, 그러한 관리자에 대해 멀티 팩터 인증(MFA)을 적용해야 합니다.

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

IAM Access Analyzer이란 무엇입니까?

IAM Access Analyzer은 외부 보안 주체와 공유 중인 계정의 리소스를 알려줍니다. 이를 위해 로직 기반 추론을 사용하여 AWS 환경에서 리소스 기반 정책을 분석합니다. 외부 엔터티는 다른 AWS 계정, 루트 사용자, IAM 사용자 또는 역할, 연합된 사용자, AWS 서비스, 익명 사용자 또는 필터 생성 (p. 524)에 사용할 수 있는 기타 엔터티일 수 있습니다. 자세한 내용은 AWS JSON 정책 요소: 보안 주체를 참조하십시오.

Access Analyzer을 활성화할 때 계정에 대한 분석기가 생성되지 않습니다. 사용자의 계정은 분석기의 신뢰 영역입니다. 분석기는 신뢰 영역 내에서 지원되는 모든 리소스를 모니터링합니다. 신뢰 영역 내에 있는 보안 주체에 의한 리소스 액세스는 신뢰할 수 있는 것으로 간주됩니다. Access Analyzer가 활성화되면 계정에서 지원되는 모든 리소스에 적용되는 정책이 분석됩니다. 첫 번째 분석 후 Access Analyzer은 24시간마다 한 번씩 이들 정책을 분석합니다. 새 정책이 추가되거나 기존 정책이 변경된 경우, Access Analyzer는 약 30분 내에 새 정책 또는 업데이트된 정책을 분석합니다.

정책을 분석할 때 Access Analyzer이 신뢰 영역 내에 없는 외부 보안 주체에 액세스 권한을 부여하는 정책을 식별하면 결과가 생성됩니다. 각 결과에는 리소스에 대한 세부 정보, 리소스에 대한 액세스 권한이 있는 외부 엔터티, 적절한 작업을 수행할 수 있도록 부여된 권한에 대한 세부 정보가 포함되어 있습니다. 결과에 포함된 세부 정보를 확인하여 리소스 액세스가 의도적인지, 아니면 확인해야 할 잠재적 위험 요소인지 확인할 수 있습니다. 리소스에 정책을 추가하거나 기존 정책을 업데이트할 때 Access Analyzer에서 정책을 분석합니다. Access Analyzer은 24시간마다 모든 리소스 기반 정책을 분석합니다.

드문 경우지만 특정 조건에서는 Access Analyzer에 정책이 추가 또는 업데이트되었음을 알리지 않습니다. 이런 경우 Access Analyzer는 다음 주기적 검색 중에 (24시간 이내) 새 정책 또는 업데이트된 정책을 분석합니다. 정책에 대한 변경이 결과에 보고된 액세스 문제를 확인하는지 알아보고 싶은 경우에는 결과에 보고된 리소스를 다시 스캔할 수 있습니다. 자세한 내용은 결과 확인 (p. 526) 단원을 참조하십시오.

> **Important**
>
> Access Analyzer에서는 활성화된 AWS 리전과 동일한 AWS 리전의 리소스에 적용되는 정책만 분석합니다. AWS 환경의 모든 리소스를 모니터링하려면 지원되는 AWS 리소스를 사용 중인 각 리전에서 Access Analyzer를 활성화하기 위해 분석기를 생성해야 합니다.

Access Analyzer은 다음과 같은 리소스 유형을 분석합니다.

- Amazon Simple Storage Service 버킷 (p. 515)
- AWS Identity and Access Management 역할 (p. 515)
- AWS Key Management Service 키 (p. 515)
- AWS Lambda 함수 및 계층 (p. 516)
- Amazon Simple Queue Service 대기열 (p. 516)

지원되는 리소스 유형

Access Analyzer에서는 Access Analyzer를 활성화한 리전의 AWS 리소스에 적용되는 리소스 기반 정책을 분석합니다. 리소스 기반 정책만 분석됩니다. Access Analyzer에서 각 리소스 유형에 대한 검색 결과를 생성하는 방법에 대한 자세한 내용은 각 리소스에 대한 정보를 검토합니다.

지원되는 리소스 유형:

- Amazon Simple Storage Service 버킷 (p. 515)

Amazon Simple Storage Service 버킷

Access Analyzer은 Amazon S3 버킷을 분석하여 버킷에 적용된 버킷 정책 또는 ACL이 외부 엔터티에 액세스 권한을 부여할 때 결과를 생성합니다. 외부 엔터티는 신뢰 영역 내에 없는 필터를 생성 (p. 524)하는 데 사용할 수 있는 보안 주체 또는 기타 엔터티입니다. 예를 들어 버킷 정책이 다른 계정에 액세스 권한을 부여하거나 퍼블릭 액세스를 허용하는 경우, Access Analyzer에서 결과가 생성됩니다. 그러나 버킷에서 Block public access(퍼블릭 액세스 차단)를 활성화하면 계정 수준 또는 버킷 수준에서 액세스를 차단할 수 있습니다.

Amazon S3 block public access(퍼블릭 액세스 차단) 설정은 버킷에 적용되는 버킷 정책을 재정의합니다. Access Analyzer은 정책이 변경될 때마다 버킷 수준에서 퍼블릭 액세스 차단 설정을 분석합니다. 하지만 6시간마다 한 번씩만 계정 수준에서 퍼블릭 액세스 차단 설정을 평가합니다. 즉, Access Analyzer에서 버킷에 대한 퍼블릭 액세스의 결과를 최대 6시간 동안 생성 또는 확인하지 못할 수 있습니다. 예를 들어 퍼블릭 액세스를 허용하는 버킷 정책이 있는 경우, Access Analyzer에서 해당 액세스에 대한 결과가 생성됩니다. 퍼블릭 액세스 차단을 활성화하여 계정 수준에서 버킷에 대한 모든 퍼블릭 액세스를 차단하면 버킷에 대한 모든 퍼블릭 액세스가 차단되더라도 Access Analyzer에서 최대 6시간 동안 버킷 정책에 대한 결과를 확인하지 못합니다.

AWS Identity and Access Management 역할

IAM 역할에서 Access Analyzer는 신뢰 정책을 분석합니다. 역할 신뢰 정책에서 역할을 수임하기 위해 신뢰하는 보안 주체를 정의합니다. 역할 신뢰 정책은 IAM의 역할에 연결되는 필수 리소스 기반 정책입니다. Access Analyzer는 신뢰 영역 밖에 있는 외부 엔터티가 액세스할 수 있는 신뢰 영역 내에서 역할에 대한 결과를 생성합니다.

> **Note**
>
> IAM 역할은 글로벌 리소스입니다. 역할 신뢰 정책이 외부 엔터티에 액세스 권한을 부여하는 경우, Access Analyzer가 활성화된 각 리전에서 결과를 생성합니다.

AWS Key Management Service 키

AWS KMS 고객 마스터 키(CMK)에서 Access Analyzer는 키에 적용되는 키 정책 및 권한 부여를 분석합니다. Access Analyzer은 키 정책 또는 권한 부여가 외부 엔터티가 키에 액세스할 수 있도록 허용할 경우 결과를 생성합니다. 예를 들어 정책 설명에서 kms:CallerAccount 조건 키를 사용하여 특정 AWS 계정의 모든 사용자에게 액세스를 허용하고 현재 계정(Access Analyzer가 활성화된)이 아닌 다른 계정을 지정하면 Access Analyzer에서 결과가 생성됩니다. IAM 정책 설명의 KMS 조건 키에 대한 자세한 내용은 AWS KMS 조건 키를 참조하십시오.

Access Analyzer은 KMS 키를 분석할 때 키 정책 및 권한 부여 목록과 같은 주요 메타데이터를 읽습니다. 키 정책에서 Access Analyzer 역할이 키 메타데이터를 읽을 수 없는 경우, 액세스 거부 오류 결과가 생성됩니다. 예를 들어 다음과 같은 예제 정책 설명이 키에 적용되는 유일한 정책인 경우, Access Analyzer에서 액세스 거부 오류 결과가 생성됩니다.

```
{
    "Sid": "Allow access for Key Administrators",
    "Effect": "Allow",
    "Principal": {
       "AWS": "arn:aws:iam::111122223333:role/Admin"
    },
```

```
    "Action": "kms:*",
    "Resource": "*"
}
```

이 문은 AWS 계정 111122223333의 Admin이라는 역할만 키에 액세스할 수 있도록 허용하므로 Access Analyzer에서 키를 완전히 분석할 수 없기 때문에 액세스 거부 오류 결과가 생성됩니다. 오류 결과는 Findings(결과) 테이블에 빨간색 텍스트로 표시됩니다. 결과는 다음과 비슷합니다.

```
{
    "error": "ACCESS_DENIED",
    "id": "12345678-1234-abcd-dcba-111122223333",
    "analyzedAt": "2019-09-16T14:24:33.352Z",
    "resource": "arn:aws:kms:us-
west-2:1234567890:key/1a2b3c4d-5e6f-7a8b-9c0d-1a2b3c4d5e6f7g8a",
    "resourceType": "AWS::KMS::Key",
    "status": "ACTIVE",
    "updatedAt": "2019-09-16T14:24:33.352Z"
}
```

KMS CMK를 생성할 때 키에 액세스할 수 있도록 부여된 권한은 키를 생성하는 방법에 따라 다릅니다. 키 리소스에 대해 액세스 거부 오류 결과를 수신하는 경우, Access Analyzer에 키에 액세스할 수 있는 권한을 부여하기 위해 키 리소스에 다음과 같은 정책 설명을 적용합니다.

```
{
    "Sid": "Allow Access Analyzer access to key metadata",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
        },
    "Action": [
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:List*"
    ],
    "Resource": "*"
},
```

KMS 키 리소스에 대한 액세스 거부 결과를 수신한 다음 키 정책을 업데이트하여 결과를 확인하면 결과가 확인 완료 상태로 업데이트됩니다. 외부 엔터티에 키에 대한 권한을 부여하는 정책 설명 또는 키 부여가 있는 경우, 키 리소스에 대한 추가 결과가 표시될 수 있습니다.

AWS Lambda 함수 및 계층

AWS Lambda 함수의 경우, Access Analyzer는 외부 엔터티에 함수에 대한 액세스 권한을 부여하는 정책(정책의 조건 문 포함)을 분석합니다. Access Analyzer은 `EventSourceToken`과 함께 AWS Lambda API의 AddPermission 작업을 사용할 때 부여된 권한도 분석합니다.

Amazon Simple Queue Service 대기열

Amazon SQS 대기열에서 Access Analyzer는 외부 엔터티가 대기열에 액세스할 수 있도록 허용하는 정책의 조건 문을 포함하여 정책을 분석합니다.

Access Analyzer 작동 방식

이 항목에서는 Access Analyzer에서 AWS 리소스에 대한 액세스를 모니터링하는 방법을 익히는 데 도움이 되도록 Access Analyzer에서 사용되는 개념과 용어에 대해 설명합니다.

IAM Access Analyzer은 IAM 정책을 동등한 논리적 문으로 변환하는 Zelkova를 기반으로 구축되었으며 문제에 대해 범용 및 특수 논리 해석기(만족성 모듈로 이론)를 실행합니다. Access Analyzer은 정책의 내용에 따라 정책이 허용하는 행동 클래스를 특성화하기 위해 점점 더 구체적인 쿼리가 있는 정책에 Zelkova를 반복적으로 적용합니다. 만족성 모듈로 이론에 대한 자세한 내용은 만족성 모듈로 이론을 참조하십시오.

Access Analyzer은 외부 엔터티가 신뢰 영역 내의 리소스에 액세스했는지 여부를 확인하기 위해 액세스 로그를 검사하지 않습니다. 외부 엔터티가 리소스에 액세스하지 않은 경우에도 리소스 기반 정책에서 리소스에 대한 액세스를 허용할 때는 결과를 생성합니다. 또한 Access Analyzer는 결정을 내릴 때 외부 계정의 상태를 고려하지 않습니다. 즉, 계정 111122223333이 S3 버킷에 액세스할 수 있음을 나타내는 경우에는 사용자 상태, 역할, 서비스 제어 정책 및 해당 계정의 기타 관련 구성에 대해서는 알 수 없습니다. 이것은 고객 개인 정보 보호를 위한 것입니다. – Access Analyzer는 누가 다른 계정을 소유하고 있는지 고려하지 않습니다. 또한 이것은 보안용입니다.– Access Analyzer 고객이 계정을 소유하지 않은 경우, 계정에 현재 리소스에 액세스할 수 있는 보안 주체가 없더라도 외부 엔터티가 리소스에 대한 액세스 권한을 획득할 수 있음을 아는 것이 중요합니다.

Access Analyzer에서는 외부 사용자가 직접 영향을 줄 수 없거나 권한 부여에 영향력을 행사하는 특정 IAM 조건 키만 고려합니다.

현재 Access Analyzer에서는 AWS 서비스 보안 주체 또는 내부 서비스 계정에서 결과를 보고하지 않습니다. 드물지만 Access Analyzer에서 정책 설명이 외부 엔터티에 대한 액세스 권한을 부여하는지 여부를 완전히 확인할 수 없는 경우에는 거짓 긍정 결과를 선언하는 측면에서 오류가 발생합니다. Access Analyzer은 계정에서 리소스 공유를 포괄적으로 볼 수 있도록 설계되었으며 거짓 부정을 최소화하기 위해 노력합니다.

AWS IAM Access Analyzer 시작하기

이 항목의 정보를 사용하여 AWS IAM Access Analyzer을 사용하고 관리하는 데 필요한 요구 사항과 Access Analyzer를 활성화하는 방법에 대해 알아봅니다. Access Analyzer에 대한 서비스 연결 역할에 대한 자세한 내용은 단원을 참조하십시오 (p. 519).

Access Analyzer 사용에 필요한 권한

Access Analyzer을 성공적으로 구성하고 사용하려면 사용하는 계정에 필요한 권한을 부여해야 합니다. 모든 Access Analyzer 기능을 액세스하여 사용하려면 계정에 IAMAccessAnalyzerFullAccess 관리형 정책을 적용할 수 있습니다. 전체 액세스 정책은 다음 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "access-analyzer:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "access-analyzer.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource": "*"
    }
  ]
}
```

Access Analyzer을 관리하기 위한 사용자 지정 정책에는 다음 권한이 포함되어야 합니다.

- access-analyzer: *
- iam:CreateServiceLinkedRole

Access Analyzer에 대한 읽기 전용 액세스를 허용하려면 AccessAnalyzerReadOnlyAccess 관리형 정책을 사용합니다. 이 정책은 다음 권한을 부여합니다.

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

AWS IAM Access Analyzer에서 정의한 리소스

Access Analyzer은 다음 리소스를 생성합니다.

리소스	ARN
분석기	arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${analyzerName}
archive-rule	arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${analyzerName}/archive-rule/${ruleName}

필요한 Access Analyzer 서비스 권한

Access Analyzer은 사용자를 대신해 리소스 기반 정책으로 AWS 리소스를 분석할 수 있도록 `AWSAccessAnalyzerServiceRole`라는 서비스 연결 역할을 사용해 서비스에 읽기 전용 액세스 권한을 부여합니다. Access Analyzer를 활성화하기 위해 분석기를 생성하면 서비스가 계정에서 역할을 생성합니다. 자세한 내용은 AWS IAM Access Analyzer에 서비스 연결 역할 사용 (p. 519) 단원을 참조하십시오.

Note

Access Analyzer은 리전입니다. 각 리전에서 독립적으로 Access Analyzer를 활성화해야 합니다.

경우에 따라 Access Analyzer을 활성화한 후 Findings(결과) 페이지가 결과 없이 로드됩니다. 이는 결과를 채우기 위해 콘솔에서 발생하는 지연으로 인한 것일 수 있습니다. 결과를 보려면 브라우저를 수동으로 새로 고침 해야 합니다. 그래도 결과가 표시되지 않으면 외부 엔터티가 액세스할 수 있는 지원 리소스가 계정에 없기 때문입니다. 외부 엔터티에 대한 액세스 권한을 부여하는 정책이 리소스에 적용되는 경우 Access Analyzer에서 결과가 생성됩니다.

Note

Access Analyzer이 리소스를 생성하도록 정책이 수정된 후 새 결과를 생성하거나 리소스에 액세스하기 위해 기존 결과를 업데이트하는 데 최대 30분이 걸릴 수 있습니다.

Access Analyzer 활성화

리전에서 Access Analyzer을 활성화하려면 해당 리전에서 분석기를 생성해야 합니다. 리소스에 대한 액세스 권한을 모니터링하려는 각 리전에서 분석기를 생성해야 합니다.

분석기를 생성하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. Access analyzer(분석기 액세스)를 선택합니다.
3. Create analyzer(분석기 생성)를 선택합니다.
4. Create analyzer(분석기 생성) 페이지에서 Access Analyzer를 활성화하려는 리전이 표시된 리전인지 확인합니다.
5. 분석기의 이름을 입력합니다.
6. 선택 사항입니다. 분석기에 적용할 태그를 추가합니다.
7. Create Analyzer(분석기 생성)를 선택합니다.

Access Analyzer을 활성화하기 위해 분석기를 생성하면 `AWSAccessAnalyzerServiceRole`라는 이름의 서비스 연결 역할이 계정에서 생성됩니다.

Access Analyzer 할당량

Access Analyzer에는 다음과 같은 할당량이 있습니다.

리소스	기본 할당량
신뢰 계정 영역이 있는 최대 분석기 수	1
분석기당 최대 아카이브 규칙 수	100

AWS IAM Access Analyzer에 서비스 연결 역할 사용

AWS IAM Access Analyzer은 IAM 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Access Analyzer에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Access Analyzer에서 사전 정의되며. 사용자를 대신해 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 통해 Access Analyzer 설정이 쉬워지는데 필요한 권한을 수동으로 추가할 필요가 없기 때문입니다. Access Analyzer에서 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 Access Analyzer에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 개체에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS IAM Access Analyzer에 대한 서비스 연결 역할 권한

AWS IAM Access Analyzer에서는 AccessAnalyzerServiceRolePolicy – Allow Access Analyzer라는 서비스 연결 역할을 사용하여 리소스 메타데이터를 분석합니다.

AccessAnalyzerServiceRolePolicy 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `access-analyzer.amazonaws.com`

역할 권한 정책은 Access Analyzer가 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeAddresses",
        "lambda:ListFunctions",
        "lambda:GetPolicy",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:GetLayerVersionPolicy",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM 개체(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 단원을 참조하십시오.

Access Analyzer에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management 콘솔 또는 AWS API에서 enable Access Analyzer을 할 때 Access Analyzer가 사용자를 대신해 서비스 연결 역할을 생성합니다. Access Analyzer을 활성화한 모든 리전에서 동일한 서비스 연결 역할이 사용됩니다.

> Note
>
> Access Analyzer은 리전입니다. 각 리전에서 독립적으로 Access Analyzer를 활성화해야 합니다.

이 서비스 연결 역할을 삭제하면 다음에 분석기를 생성할 때 Access Analyzer에서 역할이 다시 생성됩니다.

IAM 콘솔을 사용해 Access Analyzer 사용 사례로 서비스 연결 역할을 생성할 수도 있습니다. AWS CLI 또는 AWS API에서 `access-analyzer.amazonaws.com` 서비스 이름의 서비스 연결 역할을 생성합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 만들기를 참조하십시오. 이 서비스 연결 역할을 삭제한 후에는 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

Access Analyzer에 대한 서비스 연결 역할 편집

Access Analyzer에서는 AWSAccessAnalyzerServiceRole 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 IAM를 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하십시오.

Access Analyzer에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 이렇게 하면 적극적으로 모니터링하거나 유지 관리하지 않는 미사용 개체가 없게 됩니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> Note
>
> 리소스를 삭제할 때 Access Analyzer가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하십시오.

AWSAccessAnalyzerServiceRole에서 사용하는 Access Analyzer 리소스를 삭제하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. Access reports(보고서 액세스) 섹션의 Access analyzer(분석기 액세스)에서 Analyzer details(분석기 세부 정보)를 선택합니다.
3. 삭제를 선택합니다.
4. 분석기를 삭제할 것인지 확인하려면 **`delete`**을 입력한 다음, 삭제를 선택합니다.

IAM을 사용하여 서비스 연결 역할을 수동으로 삭제하려면

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWSAccessAnalyzerServiceRole 서비스 연결 역할을 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

Access Analyzer 서비스 연결 역할에 대해 지원되는 리전

Access Analyzer에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS Regions and Endpoints 단원을 참조하십시오.

Access Analyzer 결과

Access Analyzer는 외부 엔터티에 대한 신뢰 영역(계정)의 리소스에게 액세스 권한을 부여하는 리소스 기반 정책의 각 인스턴스에 대한 결과를 생성합니다. 신뢰 영역 내에서의 모든 공유는 안전한 것으로 간주되므로 Access Analyzer에서 결과가 생성되지 않습니다. 예를 들어 다른 AWS 계정에 계정의 S3 버킷에 대한 액세스 권한을 부여할 경우, Access Analyzer에서 결과가 생성됩니다. 하지만 계정의 IAM 역할에 계정의 버킷에 대한 액세스 권한을 부여하는 경우에는 Access Analyzer에서 결과가 생성되지 않습니다.

주제

결과 작업

결과는 신뢰 영역 외부에서 공유되는 리소스의 각 인스턴스에 대해 한 번만 생성됩니다. 리소스 기반 정책이 수정될 때마다 Access Analyzer이 정책을 분석합니다. 업데이트된 정책이 결과에서 이미 식별되었지만 사용 권한 또는 조건이 다른 리소스를 공유하는 경우, 리소스를 공유하는 해당 인스턴스에 대해 새 결과가 생성됩니다. 첫 번째 결과에서의 액세스가 제거되면 해당 결과는 확인 완료 상태로 업데이트됩니다.

결과를 아카이브하거나 결과를 생성한 액세스 권한을 제거할 때까지 모든 결과는 활성 상태로 유지됩니다. 액세스 권한을 제거하면 결과 상태가 확인 완료로 업데이트됩니다.

> **Note**
>
> Access Analyzer에 대한 정책을 수정한 후 리소스를 분석하고 결과를 업데이트하기까지 최대 30분이 걸릴 수 있습니다.

계정의 모든 결과를 검토하여 공유가 예상 및 승인되었는지 여부를 확인해야 합니다. 결과에서 식별된 공유가 예상되는 경우 결과를 아카이브할 수 있습니다. 결과를 아카이브하면 상태가 아카이브 완료로 변경되고 결과는 활성 결과 목록에서 제거됩니다. 결과는 삭제되지 않습니다. 아카이브된 결과를 언제든지 볼 수 있습니다. 활성 결과가 0이 될 때까지 계정의 모든 결과를 살펴봅니다. 결과가 0이 되면 새로 생성된 모든 활성 결과가 환경의 최근 변경에서 나온 것이라는 뜻입니다.

결과 검토

Access Analyzer를 활성화 (p. 519)한 후 다음 단계 결과를 검토하여 결과에서 식별된 액세스가 의도적인지 아닌지 여부를 확인하는 것입니다. 또한 결과를 검토하여 의도된 액세스에 대한 공통 결과를 확인한 다음, 해당 결과를 자동으로 아카이브하도록 아카이브 규칙을 생성 (p. 526)할 수 있습니다. 아카이브 및 확인이 완료된 결과를 검토할 수도 있습니다.

결과를 검토하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. Access analyzer(액세스 분석기)를 선택합니다.

> **Note**
>
> 분석기에 대한 결과를 볼 수 있는 권한이 있는 경우에만 결과가 표시됩니다.

분석기에서는 모든 활성 결과가 표시됩니다. 분석기에서 생성된 다른 결과를 보려면 해당 탭을 선택합니다.

- 분석기에서 생성된 모든 활성 결과를 보려면 활성화를 선택합니다.
- 아카이브가 완료된 분석기에서 생성된 결과만 보려면 아카이브 완료를 선택합니다. 자세한 내용은 결과 아카이브 (p. 525) 단원을 참조하십시오.
- 확인이 완료된 분석기에서 생성된 결과만 보려면 Resolved(확인 완료)를 선택합니다. 결과를 생성한 문제를 수정하면 결과 상태가 확인 완료로 변경됩니다.

  Important

  확인 완료된 결과는 결과를 마지막으로 업데이트하고 90일 후에 삭제됩니다. 활성화 및 아카이브 완료 상태의 결과는 결과를 생성한 분석기를 삭제하지 않는 한 삭제되지 않습니다.
- 상태에 관계 없이 분석기에서 생성된 모든 결과를 보려면 모두를 선택합니다.

Findings(결과) 페이지에는 결과를 생성한 공유 리소스 및 정책 설명에 대해 다음과 같은 세부 정보가 표시됩니다.

결과 ID

결과에 할당된 고유 ID입니다. 결과를 생성한 리소스 및 정책 설명에 대한 추가적인 세부 정보를 표시하려면 결과 ID를 선택합니다.

리소스

신뢰 영역 내에 있지 않은 외부 엔터티에 액세스 권한을 부여하는 정책이 적용된 리소스의 유형 및 이름의 일부입니다.

외부 보안 주체

신뢰 영역 내에 있지 않지만 분석된 정책에서 액세스 권한을 부여하는 보안 주체입니다. 유효한 값으로는 다음이 포함됩니다.

- AWS 계정 –해당 계정의 관리자로부터 권한을 부여 받은 나열된 AWS 계정의 모든 보안 주체는 리소스에 액세스할 수 있습니다.
- Any principal(모든 보안 주체) – 조건 열에 포함된 조건을 충족하는 AWS 계정의 모든 보안 주체는 리소스에 액세스할 수 있는 권한을 가집니다. 예를 들어 VPC가 나열되어 있을 경우 나열된 VPC에 액세스할 수 있는 권한이 있는 계정의 모든 보안 주체가 리소스에 액세스할 수 있다는 뜻입니다.
- Canonical user(정식 사용자) – 나열된 정식 사용자 ID를 가진 AWS 계정의 모든 보안 주체는 리소스에 액세스할 수 있는 권한을 가집니다.
- IAM 역할 – 나열된 IAM 역할은 리소스에 액세스할 수 있는 권한을 가집니다.
- IAM 사용자 – 나열된 IAM 사용자는 리소스에 액세스할 수 있는 권한을 가집니다.

Condition

액세스 권한을 부여하는 정책 설명의 조건입니다. 예를 들어 조건 필드에 Source VPC(소스 VPC)가 포함되어 있으면 나열된 VPC에 대한 액세스 권한이 있는 보안 주체와 리소스를 공유한다는 뜻입니다. 조건에는 글로벌 조건과 서비스별 조건이 있습니다. Global condition keys(전역 조건 키)에는 `aws:` 접두사가 있습니다.

액세스 레벨

리소스 기반 정책의 작업에 의해 외부 엔터티에 부여된 액세스 수준입니다. 자세한 내용은 결과의 세부 정보를 참조하십시오. 액세스 수준 값은 다음과 같습니다.

- 목록 – 객체가 존재하는지 여부를 판단하도록 서비스 내 리소스를 나열할 수 있는 권한입니다. 이 액세스 레벨의 작업은 객체를 나열할 수 있으나 리소스의 내용을 확인할 수 없습니다.
- 읽기 – 서비스에서 리소스 내용과 속성을 읽을 수 있으나 편집할 수 없는 권한입니다.
- 쓰기 – 서비스에서 리소스를 생성, 삭제 또는 수정할 수 있는 권한입니다.
- 권한 – 서비스에서 리소스 권한을 부여하거나 수정할 수 있는 권한입니다.

- 태그 지정 – 리소스 태그의 상태를 변경만 하는 작업을 수행할 수 있는 권한입니다.

Updated

결과 상태를 가장 최근에 업데이트한 타임스탬프 또는 결과가 생성된 시간과 날짜(업데이트가 수행되지 않은 경우)입니다.

Note

Access Analyzer에서 정책을 수정한 후 리소스를 다시 분석한 후 결과를 업데이트하는 데 최대 30분이 걸릴 수 있습니다.

상태

결과의 상태는 활성화, 아카이브 완료, 확인 완료 중 하나입니다.

결과 필터링

페이지의 기본 필터링은 모든 활성 결과를 표시하는 것입니다. 아카이브가 완료된 결과를 보려면 아카이브 완료 탭을 선택합니다. Access Analyzer를 처음 사용하기 시작할 때는 아카이브된 검색 결과가 없습니다.

필터를 사용하여 특정 리소스, 계정, 보안 주체 또는 기타 값에 대한 결과만 표시합니다. 필터를 생성하려면 필터링할 속성을 선택한 다음 필터링할 속성 값을 선택합니다. 예를 들어 특정 AWS 계정에 대한 결과만 표시하는 필터를 생성하려면 속성에 대해 AWS 계정을 선택한 다음, 결과를 보려는 AWS 계정의 계정 번호를 입력합니다.

표시된 결과를 필터링하려면

1. 활성 결과 필터링 필드를 선택합니다.
2. 표시된 결과를 필터링하는 데 사용할 속성을 선택합니다.
3. 속성에 대해 일치시킬 값을 선택합니다. 결과에 해당 값을 가진 결과만 표시됩니다.

   예를 들어 속성을 리소스 를 선택한 경우, 버킷 이름의 일부 또는 전체를 입력한 다음 Enter 키를 누릅니다. 파일러 기준과 일치하는 버킷에 대한 결과만 표시됩니다.

속성을 추가하여 표시된 결과를 추가로 필터링할 수 있습니다. 속성을 추가하면 필터의 모든 조건과 일치하는 결과만 표시됩니다. 특정 속성 또는 다른 속성과 일치하는 결과를 표시하도록 필터를 정의하는 것은 지원되지 않습니다.

다음 속성은 필터를 정의하는 데 사용할 수 있습니다.

- 리소스 – 리소스를 기준으로 필터링 하려면 리소스 이름의 전체 또는 일부를 입력합니다.
- 리소스 유형 – 리소스 유형을 기준으로 필터링하려면 표시된 목록에서 유형을 선택합니다.
- AWS 계정 – AWS 계정을 기준으로 필터링하려면 현재 계정의 리소스에 액세스할 수 있는 외부 AWS 계정의 12자리 AWS 계정 ID 전체 또는 일부를 입력합니다.
- Canonical User(정식 사용자) – 정식 사용자를 기준으로 필터링하려면 S3 버킷에 정의된 정식 사용자 ID를 입력합니다. 자세한 내용은 AWS 계정 식별자를 참조하십시오.
- Federated User(연합된 사용자) – 연합된 사용자를 기준으로 필터링하려면 연동 ID의 ARN 전체 또는 일부를 입력합니다. 자세한 내용은 ID 공급자 및 연동을 참조하십시오.
- Principal ARN(보안 주체 ARN) – 보안 주체의 ARN입니다(IAM 사용자, 역할 또는 그룹). 보안 주체 ARN을 기준으로 필터링하려면 결과에 보고된 외부 AWS 계정에서 IAM 사용자, 역할 또는 그룹의 ARN 전체 또는 일부를 입력합니다.
- Principal OrgID(보안 주체 OrgID) – 보안 주체 OrgID를 기준으로 필터링하려면 결과에 조건으로 지정된 AWS 조직에 속하는 외부 보안 주체와 연결된 조직 ID 전체 또는 일부를 입력합니다. 자세한 내용은 AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

- Principal Org Paths(보안 주체 조직 경로) – 보안 주체 조직 경로를 기준으로 필터링하려면 정책의 조건으로 지정된 조직 또는 조직 단위(OU)의 계정 구성원인 모든 외부 보안 주체에 액세스할 수 있는 AWS 조직 또는 OU의 ID 전체 또는 일부를 입력합니다. 자세한 내용은 AWS 글로벌 조건 컨텍스트 키를 참조하십시오.
- Source Account(소스 계정) – 소스 계정을 기준으로 필터링하려면 AWS의 일부 교차 서비스 권한에서 사용된 대로 리소스와 연결된 AWS 계정 ID 전체 또는 일부를 입력합니다.
- Source ARN(소스 ARN) – 소스 ARN을 기준으로 필터링하려면 결과에 조건으로 지정된 ARN 전체 또는 일부를 입력합니다. 자세한 내용은 "보안 주체 조직 경로를 기준으로 필터링하려면 정책의 조건으로 지정된 조직 또는 조직 단위(OU)의 계정 구성원인 모든 외부 보안 주체에 액세스할 수 있는 AWS 조직 또는 OU의 ID 전체 또는 일부를 입력합니다"를 참조하십시오. 자세한 내용은 AWS 글로벌 조건 컨텍스트 키를 참조하십시오.
- Source IP(소스 IP) – 소스 IP를 기준으로 필터링하려면 지정된 IP 주소를 사용할 때 외부 엔터티가 현재 계정의 리소스에 액세스할 수 있도록 허용하는 IP 주소의 전체 또는 일부를 입력합니다. 자세한 내용은 AWS 글로벌 조건 컨텍스트 키를 참조하십시오.
- Source VPC(소스 VPC) – 소스 VPC를 기준으로 필터링하려면 지정된 VPC를 사용할 때 외부 엔터티가 현재 계정의 리소스에 액세스할 수 있도록 허용하는 VPC ID의 전체 또는 일부를 입력합니다. 자세한 내용은 AWS 글로벌 조건 컨텍스트 키를 참조하십시오.
- Source VPCE(소스 VPCE) – 소스 VPCE를 기준으로 필터링하려면 지정된 VPC 엔드포인트를 사용할 때 외부 엔터티가 현재 계정의 리소스에 액세스할 수 있도록 허용하는 VPC 엔드포인트 ID의 전체 또는 일부를 입력합니다. 자세한 내용은 AWS 글로벌 조건 컨텍스트 키를 참조하십시오.
- 사용자 ID – 사용자 ID를 기준으로 필터링하려면 현재 계정의 리소스에 대한 액세스가 허용되는 외부 AWS 계정에서 IAM 사용자의 ID 전체 또는 일부를 입력합니다. 자세한 내용은 AWS 글로벌 조건 컨텍스트 키를 참조하십시오.
- KMS Key ID(KMS 키 ID) – KMS 키 ID를 기준으로 필터링하려면 현재 계정에서 KMS 암호화 S3 객체 액세스의 조건으로 지정된 KMS 키의 ID 전체 또는 일부를 입력합니다.
- Google Audience(Google 대상) – Google 대상을 기준으로 필터링하려면 현재 계정에서 IAM 역할 액세스 조건으로 지정된 Google 애플리케이션 ID의 전체 또는 일부를 입력합니다. 자세한 내용은 IAM 및 AWS STS 조건 컨텍스트 키를 참조하십시오.
- Cognito Audience(Cognito 대상) – Cognito 대상을 기준으로 필터링하려면 현재 계정에서 IAM 역할 액세스 조건으로 지정된 Amazon Cognito 자격 증명 풀 ID의 전체 또는 일부를 입력합니다. 자세한 내용은 IAM 및 AWS STS 조건 컨텍스트 키를 참조하십시오.
- Caller Account(호출자 계정) – IAM 역할, 사용자 또는 계정 루트 사용자와 같이 호출 엔터티를 소유하거나 포함하는 계정의 AWS 계정 ID입니다. 이 기능은 KMS를 호출하는 서비스에서 사용됩니다. 호출자 계정을 기준으로 필터링하려면 AWS 계정 ID의 전체 또는 일부를 입력합니다.
- Facebook App ID(Facebook 앱 ID) – Facebook 앱 ID를 기준으로 필터링하려면 현재 계정의 IAM 역할에 대한 Facebook 연동 액세스 권한을 이용하여 로그인을 할 수 있도록 조건으로 지정된 Facebook 애플리케이션 ID(또는 사이트 ID)의 전체 또는 일부를 입력합니다. 자세한 내용은 IAM 및 AWS STS 조건 컨텍스트 키를 참조하십시오.
- Amazon App ID(Amazon 앱 ID) – Amazon 앱 ID를 기준으로 필터링하려면 현재 계정의 IAM 역할에 대한 Amazon 연동 액세스 권한을 이용하여 로그인을 할 수 있도록 조건으로 지정된 Amazon 애플리케이션 ID(또는 사이트 ID)의 전체 또는 일부를 입력합니다. 자세한 내용은 IAM 및 AWS STS 조건 컨텍스트 키를 참조하십시오.
- Lambda Event Source Token(Lambda 이벤트 소스 토큰) – Alexa 통합 시 전달된 Lambda 이벤트 소스 토큰을 기준으로 필터링하려면 토큰 문자열 전체 또는 일부를 입력합니다.

결과 아카이브

승인된 워크플로에서 여러 명이 사용하는 IAM 역할과 같이 의도적인 리소스 액세스에 대한 결과를 얻으면 결과를 아카이브할 수 있습니다. 결과를 아카이브하면 활성 결과 목록에서 지워지므로 확인해야 하는 결과에 집중할 수 있습니다. 보관된 결과는 삭제되지 않습니다. 아카이브된 결과를 표시하도록 Findings(결과) 페이지를 필터링할 수 있고, 언제든지 아카이브를 취소할 수 있습니다.

Findings(결과) 페이지에서 결과를 아카이브하려면

1. 아카이브할 하나 이상의 결과 옆에 있는 확인란을 선택합니다.
2. Archive(아카이브)를 선택합니다.

   화면 상단에 확인 메시지가 표시됩니다.

Findings Details(결과 세부 정보) 페이지에서 결과를 아카이브하려면

1. 아카이브할 결과에 대한 Finding ID(결과 ID)를 선택합니다.
2. Archive(아카이브)를 선택합니다.

   화면 상단에 확인 메시지가 표시됩니다.

결과의 아카이브를 해제하려면 앞의 단계를 반복하되 Archive(아카이브) 대신 Unarchive(아카이브 해제)를 선택합니다. 결과의 아카이브를 해제하면 상태가 활성으로 설정됩니다.

결과 확인

허용할 생각이 없었던 액세스 권한으로부터 생성된 결과를 확인하려면 식별된 리소스에 대한 액세스를 허용하는 권한을 제거하도록 정책 설명을 수정합니다. 예를 들어 S3 버킷에 대한 결과의 경우 Amazon S3 콘솔을 사용하여 버킷에 대한 권한을 구성합니다. IAM 역할의 경우 IAM 콘솔을 사용하여 나열된 IAM 역할에 대해 신뢰 정책을 수정합니다. 이 콘솔을 사용하여 지원되는 다른 리소스에서 생성된 결과를 초래한 정책 설명을 수정합니다.

IAM 역할에 적용된 정책을 수정하는 등 결과를 확인하기 위해 변경을 수행한 후 Access Analyzer에서 리소스를 다시 검색합니다. 리소스가 신뢰 영역 외부에서 더 이상 공유되지 않으면 결과 상태가 확인 완료로 변경됩니다. 결과는 더 이상 Active findings(활성 결과) 테이블에 표시되지 않고 대신에 Resolved findings(확인된 결과) 테이블에 표시됩니다.

수행한 변경으로 인해 리소스가 신뢰 영역 외부에서 공유되지만 다른 보안 주체 또는 다른 권한에서와 같이 다른 방식으로 공유되는 경우, Access Analyzer에서 활성 결과가 새로 생성됩니다.

> **Note**
>
> Access Analyzer에서 정책을 수정한 후 리소스를 다시 분석한 후 결과를 업데이트하는 데 최대 30분이 걸릴 수 있습니다. 확인된 결과는 결과 상태를 마지막으로 업데이트하고 90일 후에 삭제됩니다.

아카이브 규칙

아카이브 규칙은 규칙을 생성할 때 정의한 기준을 충족하는 새 결과를 자동으로 아카이브합니다. 예를 들어, 정기적으로 액세스 권한을 부여한 특정 S3 버킷에 대한 결과를 자동으로 아카이브하는 아카이브 규칙을 생성할 수 있습니다. 또는 특정 보안 주체에게 여러 리소스에 대한 액세스 권한을 부여하는 경우 해당 보안 주체에게 부여된 액세스 권한에 대해 생성된 새로운 결과를 자동으로 아카이브하는 규칙을 생성할 수 있습니다. 이렇게 하면 보안 위험성이 있는 활성 상태의 결과에만 집중할 수 있습니다.

결과 세부 사항에서 제공된 정보를 사용하여 규칙을 생성하거나 편집할 때 사용할 특정 리소스 및 외부 엔터티를 식별합니다. 아카이브 규칙을 생성하면 규칙 기준과 일치하는 새로운 결과만 자동으로 보관됩니다. 기존 결과는 자동으로 아카이브되지 않습니다.

> **Note**
>
> 아카이브 규칙을 생성하거나 편집할 때 Access Analyzer은 규칙에 대한 필터에 포함되는 값의 유효성을 검사하지 않습니다. 예를 들어, AWS 계정과 일치하는 규칙을 추가하는 경우 Access Analyzer는 유효한 AWS 계정 번호가 아니더라도 필드의 모든 값을 허용합니다.

아카이브 규칙을 생성하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. Access analyzer(액세스 분석기)를 선택한 다음 Archive rules(아카이브 규칙)를 선택합니다.
3. Create archive rule(아카이브 규칙 생성)을 선택합니다.
4. 기본 이름을 변경하려면 규칙 이름을 입력합니다.
5. 규칙 섹션의 Criteria(조건)에서 규칙에 대해 일치시킬 속성을 선택합니다.
6. 속성 값에 대한 연산자(예: contains)를 선택합니다.

   사용 가능한 연산자는 선택한 속성에 따라 다릅니다.
7. 선택에 따라 속성에 대해 값을 추가하거나 규칙에 대한 기준을 추가합니다.

   기준에 다른 값을 추가하려면 Add another value(다른 값 추가)를 선택합니다. 규칙에 대해 다른 기준을 추가하려면 추가 버튼을 선택합니다.
8. 기준과 값을 추가했으면 Create archive rule(아카이브 규칙 생성)을 선택합니다.

예를 들어 S3 버킷에 대한 결과를 자동으로 아카이브하는 규칙을 생성하려면 리소스 유형을 선택한 다음 연산자로 is를 선택합니다. 그런 다음 리소스 유형 선택 목록에서 S3 버킷을 선택한 다음 추가를 선택합니다.

조건을 계속 정의하여 사용자 환경에 적합한 규칙을 사용자 지정한 다음 Create archive rule(아카이브 규칙 생성)을 선택합니다.

새 규칙을 생성하고 여러 조건을 추가하는 경우 Remove this criterion(이 조건 제거)를 선택하여 규칙에서 단일 기준을 제거할 수 있습니다. Remove value(값 제거)를 선택하여 기준에 대해 추가된 값을 제거할 수 있습니다.

아카이브 규칙을 편집하려면

1. 이름에서 편집할 규칙의 이름을 선택합니다.

   한 번에 하나의 아카이브 규칙만 편집할 수 있습니다.
2. 새 기준을 추가하거나 각 기준에 대한 기존 기준 및 값을 제거합니다.
3. Save changes(변경 사항 저장)를 선택합니다.

아카이브 규칙을 삭제하려면

1. 삭제할 규칙의 확인란을 선택합니다.

   한 개, 여러 개 또는 모든 규칙을 동시에 삭제할 수 있습니다.
2. 삭제를 선택합니다.
3. Delete archive rule(아카이브 규칙 삭제) 확인 대화 상자에 **`delete`**을 입력한 다음, 삭제를 선택합니다.

규칙은 현재 리전의 분석기에서만 삭제됩니다. 다른 리전에서 생성한 각 분석기에 대해 아카이브 규칙을 별도로 삭제해야 합니다.

Amazon EventBridge를 사용하여 AWS IAM Access Analyzer 모니터링

이 항목의 정보를 이용해 Amazon EventBridge를 사용하여 Access Analyzer 결과를 모니터링 하는 방법을 알아봅니다. EventBridge은 Amazon CloudWatch Events의 새 버전입니다.

결과 이벤트

Access Analyzer은 기존 결과의 상태 변경 시, 그리고 검색 결과가 삭제될 때 생성된 각각의 결과에 대해 EventBridge 이벤트를 전송합니다. 결과와 결과에 대한 알림을 받으려면 Amazon EventBridge에서 이벤트 규칙을 생성해야 합니다. 이벤트 규칙을 생성할 때 규칙에 따라 트리거할 대상 동작을 지정할 수도 있습니다. 예를 들어 Access Analyzer에서 새 결과에 대한 이벤트를 수신할 때 Amazon SNS 항목을 트리거하는 이벤트 규칙을 생성할 수 있습니다.

이벤트 알림 빈도

Access Analyzer는 계정에서 이벤트가 발생한 시점으로부터 약 1시간 이내에 새 결과와 EventBridge로 상태가 업데이트된 결과에 대해 이벤트를 전송합니다. Access Analyzer는 보존 기간이 만료되어 확인된 결과가 삭제될 때도 EventBridge에 이벤트를 전송합니다. 결과를 생성한 분석기가 삭제되었기 때문에 삭제가 된 결과의 경우, 분석기가 삭제된 후 약 24시간 내에 EventBridge로 이벤트가 전송됩니다. 결과가 삭제될 때 검색 상태는 변경되지 않습니다. 대신 `isDeleted` 속성이 `true`로 설정됩니다.

예제 이벤트

다음은 EventBridge로 전소오딘 Access Analyzer 이벤트의 예제입니다. 나열된 `id`은 EventBridge의 이벤트 ID입니다. 자세한 내용은 EventBridge의 이벤트 및 이벤트 패턴을 참조하십시오.

`detail` 객체에서 `accountId` 및 `region` 속성의 값은 결과에 보고된 계정 및 리전을 나타냅니다. `isDeleted` 속성은 이벤트가 삭제 중인 결과에서 발생했는지 여부를 나타냅니다.

```
{
  "id": "22222222-dcba-4444-dcba-333333333333",
  "detail-type": "Access Analyzer Finding",
  "source": "aws.access-analyzer",
  "account": "111122223333",
  "time": "2019-11-21T01:22:33Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:access-analyzer:us-west-2:111122223333:analyzer/MyAnalyzer"
  ],
  "detail": {
      "version": "1.0",
      "accountId": "111122223333",
      "region": "us-west-2",
      "isDeleted": false,
      COMPLETE_ACCESS_ANALYZER_GET_FINDING_RESPONSE
    }
}
```

`"id"`은 결과 ID입니다. `"resources"` 배열은 결과를 생성한 분석기의 ARN이 있는 singleton입니다.

다음 예제의 전체 목록은 Access Analyzer API의 `GetFinding` 작업에서 EventBridge로 전송되는 이벤트에 대한 데이터를 보여 줍니다.

```
"version": "0",
  "id": "22222222-dcba-4444-dcba-333333333333",
  "status": "ACTIVE",
  "resourceType": "AWS::S3::Bucket",
  "resource": "arn:aws:s3:::my-bucket",
  "createdAt": "2019-11-20T04:58:50Z",
  "analyzedAt": "2019-11-21T01:22:22Z",
  "updatedAt": "2019-11-21T01:14:07Z",
  "principal": {"AWS": "999988887777"},
  "action": ["s3:GetObject"],
```

```
  "condition": {},
  "isPublic": false
```

Access Analyzer는 오류 결과에 대해 EventBridge에 이벤트를 전송합니다. 오류 결과는 Access Analyzer에서 분석하려는 리소스에 액세스할 수 없을 때 생성되는 결과입니다. 오류 결과를 위한 이벤트에는 다음 예제에서와 같이 `error` 속성이 포함됩니다.

```
"id": "22222222-dcba-4444-dcba-333333333333",
"status": "ACTIVE",
"resourceType": "AWS::S3::Bucket",
"resource": "arn:aws:s3:::my-bucket",
"error": "ACCESS_DENIED",
"createdAt": "2019-10-16T19:21:44.244Z",
"analyzedAt": "2019-10-16T19:21:44.244Z",
"updatedAt": "2019-10-16T19:21:44.244Z"
```

대상이 있는 이벤트 규칙 생성

다음 절차에서는 콘솔을 사용하여 이벤트를 생성하는 방법을 설명합니다.

https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.

1. [Create rule]을 선택합니다.
2. 이름에 값을 입력하고 선택에 따라 설명에 값을 입력합니다.
3. Define pattern(패턴 정의)에서 이벤트 패턴을 선택한 다음 Custom pattern(사용자 정의 패턴)을 선택합니다.
4. 다음 예제를 복사하여 이벤트 패턴 상자에 붙여 넣습니다.

   ```
   {
     "source": [
       "aws.access-analyzer"
     ],
     "detail-type": [
       "Access Analyzer Finding"
     ]
   }
   ```
5. 저장을 선택합니다.
6. Select targets(대상 선택)에서 규칙에 대한 대상 작업(예: Amazon SNS 항목 또는 AWS Lambda 함수)을 선택합니다, .
7. 대상이 트리거될 때 사용할 특정 SNS 항목 또는 Lambda 함수를 선택합니다.

   규칙에 정의된 이벤트 패턴과 일치하는 이벤트를 수신할 때 대상이 트리거됩니다.
8. 저장을 선택하여 규칙을 생성합니다.

규칙 생성에 대한 자세한 내용은 AWS 리소스에서 이벤트에서 트리거하는 EventBridge 규칙 생성을 참조하십시오.

CLI를 사용하여 규칙 생성

1. 다음을 통해 AWS CLI를 사용하여 Amazon EventBridge에 대한 규칙을 생성합니다. 규칙 이름 *TestRule*을 자신의 규칙 이름으로 바꿉니다.

   ```
   aws events put-rule --name TestRule --event-pattern "{\"source\":[\"aws.access-analyzer
   \"]}"
   ```

2. 특정 속성을 가진 결과와 같이 생성된 결과의 하위 집합에 대해서만 대상 작업을 트리거하도록 규칙을 사용자 정의할 수 있습니다. 다음 예제에서는 활성 상태인 결과에 대해서만 대상 작업을 트리거하는 규칙을 생성하는 방법을 보여 줍니다.

```
aws events put-rule --name TestRule --event-pattern "{\"source\":[\"aws.access-analyzer
\"],\"detail-type\":[\"Access Analyzer Finding\"],\"detail\":{\"status\":[\"ACTIVE
\"]}}"
```

3. Lambda 함수를 생성한 규칙의 대상으로 정의하려면 다음 예제 명령을 사용합니다. ARN의 리전 및 함수 이름을 사용자 환경에 맞게 바꿉니다.

```
aws events put-targets --rule TestRule --targets Id=1,Arn=arn:aws:lambda:us-
east-1:111122223333:function:MyFunction
```

4. 규칙 대상을 호출하는 데 필요한 권한을 추가합니다. 다음 예제에서는 앞의 예에 따라 Lambda 함수에 권한을 부여하는 방법을 보여 줍니다.

```
aws lambda add-permission --function-name MyFunction --statement-id 1 --action
 'lambda:InvokeFunction' --principal events.amazonaws.com
```

AWS CloudTrail를 사용하여 Access Analyzer API 호출 로깅

Access Analyzer는 Access Analyzer에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail와 통합됩니다. CloudTrail는 Access Analyzer에 대한 모든 API를 이벤트로 캡처합니다. 캡처되는 호출에는 Access Analyzer 콘솔로부터의 호출과 Access Analyzer API 작업에 대한 코드 호출이 포함됩니다.

트레일을 생성하면 Access Analyzer에 대한 이벤트를 비롯하여 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 전송할 수 있습니다. 추적을 구성하지 않은 경우 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수도 있습니다.

CloudTrail에서 수집한 정보를 사용하여 Access Analyzer에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail User Guide을 참조하십시오.

CloudTrail의 Access Analyzer 정보

CloudTrail은 계정 생성 시 AWS 계정에서 활성화됩니다. Access Analyzer에서 활동이 수행되면 해당 활동은 Event history(이벤트 기록)에서 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록에서 이벤트 보기를 참조하십시오.

Access Analyzer에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 트레일을 생성합니다. 추적은 CloudTrail이 Amazon S3 버킷으로 로그 파일을 전송할 수 있도록 합니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 정보는 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합

- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Access Analyzer 작업이 CloudTrail에서 로깅되고 IAM Access Analyzer API Reference에 문서화됩니다. 예를 들어 `CreateAnalyzer`, `CreateArchiveRule` 및 `ListFindings` 작업을 호출하면 CloudTrail 로그 파일에서 항목이 생성됩니다.

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

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

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

Access Analyzer 로그 파일 항목 이해

추적은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 제공할 수 있도록 해 주는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함됩니다. 이벤트는 어떤 소스로부터의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 포함되어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

다음 예제에는 “2018년 6월 14일”에 “Alice”라는 사용자가 수행한 `CreateAnalyzer` 작업을 보여 주는 CloudTrail 로그 항목이 나와 있습니다.


```
{
  "eventVersion": "1.05",
  "userIdentity":   {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-06-14T22:54:20Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "userName": "Alice"
      }
    }
  },
  "eventTime": "2018-06-14T22:57:36Z",
  "eventSource": "access-analyzer.amazonaws.com",
  "eventName": "CreateAnalyzer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.179",
  "userAgent": "aws-cli/1.16.205 Python/2.7.16 Darwin/17.7.0 botocore/1.12.195",
  "requestParameters": {
    "analyzerName": "test",
    "type": "ACCOUNT",
    "clientToken": "11111111-abcd-2222-abcd-222222222222"
```

```
  },
  "responseElements": {
    "arn": "arn:aws:access-analyzer:us-west-2:111122223333:analyzer/test"
  },
  "requestID": "22222222-dcba-4444-dcba-333333333333",
  "eventID": "33333333-bcde-5555-bcde-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

IAM 문제 해결

AWS Identity and Access Management(IAM) 작업 시 액세스 거부 또는 이와 유사한 문제가 발생하면 이 섹션의 주제를 참조하십시오.

주제

일반적인 문제 해결

여기에 있는 정보를 사용하면 IAM(AWS Identity and Access Management) 작업 시 액세스 거부 또는 기타 일반적인 문제를 진단하고 해결할 수 있습니다.

주제

액세스 키를 분실했습니다

액세스 키는 다음 두 부분으로 구성됩니다.

- 액세스 키 식별자. 이 식별자는 비밀이 아니며 사용자 요약 페이지 등 IAM 콘솔에서 액세스 키가 나열되어 있는 곳 어디서나 확인할 수 있습니다.
- 보안 액세스 키. 액세스 키 페어를 처음 만들 때 제공됩니다. 암호와 마찬가지로 나중에 검색할 수 없습니다. 하지만 보안 액세스 키를 분실한 경우에는 새로운 액세스 키 페어를 생성해야 합니다. 이미 액세스 키의 최대 수 (p. 569)인 경우 기존 페어를 삭제해야만 다른 페어를 생성할 수 있습니다.

자세한 내용은 분실하거나 잊어버린 암호 또는 액세스 키 재설정 (p. 118) 단원을 참조하십시오.

예전 계정에 액세스해야 합니다

AWS 계정을 처음 생성할 때 이메일 주소와 암호를 입력했습니다. 그 주소와 암호가 바로 AWS 계정 루트 사용자 자격 증명입니다. 암호를 잊거나 분실하여 더 이상 액세스할 수 없게 된 AWS 계정이 있다면 암호를 복

구하면 됩니다. 자세한 정보는 분실하거나 잊어버린 암호 또는 액세스 키 재설정 (p. 118) 단원을 참조하십시오.

그 이메일에 더 이상 액세스할 수 없는 경우, 먼저 이메일에 대한 액세스부터 복구해 보아야 합니다. 복구에 실패하면 AWS 고객 서비스에 문의하십시오.

다음 옵션 중 하나를 사용하여 이메일에 대한 액세스 권한을 복구해 볼 수 있습니다.

- 이메일 주소의 호스팅 도메인이 본인 소유인 경우, 그 이메일 주소를 다시 이메일 서버에 추가하면 됩니다. 아니면 이메일 계정에 대한 완전 포착(catch-all) 조건을 설정할 수 있습니다. 도메인에 설정된 완전 포착(catch-all) 조건은 메일 서버에 존재하지 않는 이메일 주소로 전송된 "모든 메시지를 포착(catches all)"합니다. 그리고 그러한 메시지를 특정 이메일 주소로 리디렉션합니다. 예를 들어 AWS 계정 루트 사용자 이메일 주소가 `paulo@sample-domain.com`이지만 유일한 도메인 이메일 주소를 `paulo.santos@sample-domain.com`으로 변경한다고 가정합니다. 이 경우 새 이메일을 catch-all로 설정할 수 있습니다. 그러면 AWS 같은 곳에서 `paulo@sample-domain.com` 또는 다른 `text@sample-domain.com`으로 메시지를 보내면 사용자는 `paulo.santos@sample-domain.com` 주소로 그 메시지를 받게 됩니다.
- 계정의 이메일 주소가 회사 이메일 시스템에 속한 경우라면 IT 시스템 관리자에게 문의하는 것이 좋습니다. 시스템 관리자가 이메일 주소에 대한 액세스 권한을 다시 받을 수 있도록 도와 줄 것입니다.

그래도 AWS 계정에 액세스할 수 없는 경우, 문의처에서 현재 AWS 고객이며, 결제 또는 계정 지원이 필요합니다(I'm an AWS customer and I'm looking for billing or account support) 메뉴를 확장하여 다른 지원 옵션을 찾아볼 수 있습니다. AWS Support에 문의할 때는 다음 정보를 제공해야 합니다.

- 본인 이름, 전화번호, 주소, 이메일 주소, 신용카드의 마지막 네 자리 번호 등 계정에 나열되어 있는 모든 세부 정보. AWS Support에 문의할 목적으로 새 AWS 계정을 생성해야 할 수도 있습니다. 이는 요청 조사를 지원하는 데 있어 필수입니다.
- 암호 재설정 지침을 받아야 하는데 이메일 계정에 액세스할 수 없는 이유.
- 계정을 복구한 후에는 사용하지 않는 모든 계정을 닫으십시오. 요금이 부과될 가능성이 있으므로 본인 이름으로 계정을 열어 두지 않는 것이 좋습니다. 자세한 내용은 Billing and Cost Management 사용 설명서의 계정 닫기를 참조하십시오.

내 계정에 로그인할 수 없음

AWS 계정을 처음 생성할 때 이메일 주소와 암호를 입력했습니다. 그 주소와 암호가 바로 AWS 계정 루트 사용자 자격 증명입니다. 암호를 잊거나 분실하여 더 이상 액세스할 수 없게 된 계정이 있다면 해당 암호를 복구하면 됩니다. 자세한 정보는 분실하거나 잊어버린 암호 또는 액세스 키 재설정 (p. 118) 단원을 참조하십시오.

계정 이메일 주소와 암호를 입력한 경우 AWS는 일회성 확인 코드를 입력해야 하는 경우도 있습니다. 확인 코드를 검색하려면 AWS 계정과 연결된 이메일에서 Amazon Web Services의 메시지를 확인합니다. 이메일 주소는 @amazon.com 또는 @aws.amazon.com으로 끝납니다. 메시지의 지침을 따릅니다. 계정으로 메시지가 오지 않았으면 스팸 폴더를 점검합니다. 그 이메일에 더 이상 액세스할 수 없는 경우에는 예전 계정에 액세스해야 합니다 (p. 533) 단원을 참조하십시오.

AWS 서비스에 요청하면 "액세스 거부"가 발생합니다

- 요청한 작업 및 리소스를 호출할 자격 증명 기반 정책 권한이 있는지 확인합니다. 조건이 설정된 경우 요청을 보낼 때 그러한 조건 또한 충족해야 합니다. IAM 사용자, 그룹 또는 역할에 대한 정책을 보거나 수정하는 방법에 대한 자세한 정보는 IAM 정책 관리 (p. 435) 단원을 참조하십시오.
- 리소스 기반 정책 (p. 372)을 지원하는 서비스(예: Amazon S3, Amazon SNS 또는 Amazon SQS)에 액세스하려 합니까? 그러한 경우 정책에서 사용자를 보안 주체로 지정하고 액세스 권한을 부여하는지 확인하십시오. 자신의 계정 내에서 서비스를 요청하는 경우 자격 증명 기반 정책이나 리소스 기반 정책에서 요청자에게 권한을 부여할 수 있습니다. 다른 계정에서 서비스를 요청하는 경우 자격 증명 기반 정책 및 리소스

기반 정책 모두에서 요청자에게 권한을 부여해야 합니다. 리소스 기반 정책을 지원하는 서비스를 보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

- 정책에 키–값 페어가 있는 조건이 포함된 경우 이를 주의하여 검토하십시오. `aws:RequestTag/tag-key` (p. 650) 전역 조건 키, AWS KMS `kms:EncryptionContext:encryption_context_key` 및 여러 서비스에서 지원하는 `ResourceTag/tag-key` 조건 키가 그 예입니다. 키 이름이 여러 개의 결과와 일치하지 않도록 하십시오. 조건 키 이름이 대/소문자를 구분하지 않으므로 이름이 `foo`인 키를 검사하는 조건은 `foo`, `Foo` 또는 `FOO`와 일치합니다. 대/소문자로만 구분되는 키 이름을 가진 여러 키–값 페어가 요청에 포함된 경우 액세스가 예기치 않게 거부될 수 있습니다. 자세한 정보는 IAM JSON 정책 요소: Condition (p. 598) 단원을 참조하십시오.
- 권한 경계 (p. 363)가 있다면, 권한 경계에 사용된 정책이 요청을 허용하는지 확인합니다. 자격 증명 기반 정책에서는 요청이 허용되지만 권한 경계에서는 허용되지 않는 경우 요청이 거부됩니다. 이 권한 경계는 IAM 보안 주체(사용자나 역할)에 부여할 수 있는 최대 권한을 제어합니다. 리소스 기반 정책은 권한 경계에 제한을 받지 않습니다. 권한 경계는 일반적이지 않습니다. AWS 평가 정책에 대한 자세한 정보는 정책 평가 로직 (p. 622)을 참조하십시오.
- (AWS SDK를 사용하지 않고) 요청에 수동으로 서명할 경우, 요청에 올바르게 서명했는지 확인합니다.

임시 보안 자격 증명으로 요청하면 "액세스 거부"가 발생합니다

- 우선, 임시 자격 증명과 무관한 이유로 액세스가 거부되지는 않았는지 확인합니다. 자세한 정보는 AWS 서비스에 요청하면 "액세스 거부"가 발생합니다 (p. 534) 단원을 참조하십시오.
- IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하여 서비스에서 임시 보안 자격 증명을 허용하는지 확인합니다.
- 요청에 올바르게 서명했고 요청이 잘 구성되었는지 확인합니다. 자세한 정보는 도구 키트 문서 또는 AWS 리소스에서 임시 자격 증명 사용 (p. 313) 단원을 참조하십시오.
- 임시 보안 자격 증명이 만료되지 않았는지 확인합니다. 자세한 정보는 임시 보안 자격 증명 (p. 302) 단원을 참조하십시오.
- IAM 사용자 또는 역할 권한이 올바른지 확인합니다. 임시 보안 자격 증명에 대한 권한은 IAM 사용자 또는 역할에서 파생됩니다. 결과적으로 위임한 역할(임시 자격 증명이 제공됨)에 부여된 권한으로 제한됩니다. 임시 보안 자격 증명의 권한이 결정되는 방법에 대한 자세한 정보는 사용자 임시 보안 자격 증명에 대한 권한 제어 (p. 316) 단원을 참조하십시오.
- 역할을 수임한 경우 역할 세션이 세션 정책에 의해 제한되었을 수 있습니다. AWS STS 사용을 통해 프로그래밍 방식으로 임시 보안 자격 증명을 요청 (p. 304)한 경우 인라인 또는 관리형 세션 정책 (p. 351)을 전달할 수 있습니다. 세션 정책은 역할 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. `Policy` 파라미터를 사용하여 단일 JSON 인라인 세션 정책 문서를 전달할 수 있습니다. `PolicyArns` 파라미터를 사용하여 최대 10개까지 관리형 세션 정책을 지정할 수 있습니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 자격 증명 기반 정책의 교집합과 세션 정책입니다. 또는 관리자 또는 사용자 프로그램에서 임시 자격 증명을 제공한 경우 세션 정책에 포함되어 액세스를 제한했을 수 있습니다.
- 연동 사용자인 경우 세션이 세션 정책에 의해 제한되었을 수 있습니다. IAM 사용자로 AWS에 로그인하여 연동 사용자가 된 후 연동 토큰을 요청합니다. 연동 사용자에 대한 자세한 내용은 GetFederationToken—사용자 지정 자격 증명 브로커를 통한 연동 (p. 308) 단원을 참조하십시오. 사용자 또는 사용자의 자격 증명 브로커가 연동 토큰을 요청하는 동안 세션 정책을 전달한 경우 세션이 이러한 정책에 의해 제한됩니다. 결과적으로 얻는 세션의 권한은 IAM 사용자 자격 증명 기반 정책의 교집합과 세션 정책입니다. 세션 정책에 대한 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오.
- 역할을 사용하여 리소스 기반 정책이 있는 리소스에 액세스할 경우, 해당 정책에서 역할에 권한을 부여하는지 확인합니다. 예를 들어, 다음과 같은 정책에서는 계정 `MyRole`의 `111122223333`이 `MyBucket`에 액세스하도록 허용합니다.

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

```
    "Sid": "S3BucketPolicy",
    "Effect": "Allow",
    "Principal": {"AWS": ["arn:aws:iam::111122223333:role/MyRole"]},
    "Action": ["s3:PutObject"],
    "Resource": ["arn:aws:s3:::MyBucket/*"]
  }]
}
```

정책 변수가 작동하지 않습니다

- 변수가 포함된 모든 정책에 버전 번호 `"Version": "2012-10-17"`이 있는지 확인하십시오. 올바른 버전 번호가 없으면 평가 도중에 변수가 대체되지 않습니다. 대신 변수는 문자 그대로 평가됩니다. 최신 버전 번호를 포함시키더라도 변수를 포함하지 않은 정책은 계속 작동합니다.

  `Version` 정책 요소는 정책 버전과 다릅니다. `Version` 정책 요소는 정책 내에서 사용되며 정책 언어의 버전을 정의합니다. 반면에 정책 버전은 IAM에서 고객 관리형 정책을 변경할 때 생성됩니다. 변경된 정책은 기존 정책을 덮어쓰지 않습니다. 대신 IAM에서 관리형 정책의 새 버전을 만듭니다. `Version` 정책 요소에 대한 자세한 정보는 IAM JSON 정책 요소: Version (p. 587)을 참조하십시오. 정책 버전에 대한 자세한 정보는 the section called “IAM 정책 버전 관리” (p. 458) 단원을 참조하십시오.
- 정책 변수가 올바른지 확인합니다. 자세한 정보는 IAM 정책 요소: 변수 및 태그 (p. 615) 단원을 참조하십시오.

변경 사항이 매번 즉시 표시되는 것은 아닙니다

사용자들이 전세계 데이터 센터의 컴퓨터들을 통해 액세스하는 서비스인 IAM은 최종 일관성이라고 하는 분산 컴퓨팅 모델을 사용합니다. IAM(또는 다른 AWS 서비스)에서 변경한 사항을, 있을 수 있는 모든 엔드포인트에서 보게 될 때까지는 시간이 걸립니다. 일부 지연은 서버에서 서버로, 복제 영역에서 복제 영역으로, 전세계의 리전에서 리전으로 데이터를 보내는 데 걸리는 시간으로 인해 발생합니다. 또한 IAM는 캐싱을 사용하여 성능을 개선하지만 이 경우 중 몇몇 경우는 더 많은 시간이 소요될 수 있습니다. 이전에 캐시된 데이터가 시간 초과될 때까지 변경 사항이 표시되지 않을 수 있기 때문입니다.

이러한 잠재적 지연을 고려하도록 전역 애플리케이션을 설계해야 합니다. 한 위치에서 변경한 내용이 다른 위치에서 즉시 보이지 않을 때조차도 예상대로 작동하는지 확인합니다. 그러한 변경 사항에는 사용자, 그룹, 역할 또는 정책을 만들거나 업데이트한 것이 포함됩니다. 그러한 IAM 변경 사항을 애플리케이션의 중요한 고가용성 코드 경로에 포함시키지 않는 것이 좋습니다. 대신 자주 실행하지 않는 별도의 초기화 루틴이나 설정 루틴에서 IAM을 변경하십시오. 또한 프로덕션 워크플로우에서 변경 사항을 적용하기 전에 변경 사항이 전파되었는지 확인하십시오.

이로 인해 일부 다른 AWS 서비스가 받게 되는 영향에 대한 자세한 정보는 다음 자료를 참고하십시오.

- Amazon DynamoDB: DynamoDB FAQ에서 Amazon DynamoDB의 일관성 모델이란 무엇입니까? 및 Amazon DynamoDB 개발자 안내서에서의 읽기 일관성이란 무엇입니까?
- Amazon EC2: Amazon EC2 API Reference에서의 EC2 최종 일관성.
- Amazon EMR: 빅 데이터 블로그에서 AWSETL 워크플로우에 대해 Amazon S3 및 Amazon Elastic MapReduce 사용 시 일관성 유지
- Amazon Redshift: Amazon Redshift Database Developer Guide에서 데이터 일관성 관리
- Amazon S3: Amazon Simple Storage Service 개발자 가이드에서의 Amazon S3 데이터 일관성 모델

iam:DeleteVirtualMFADevice를 수행할 권한이 없음

본인 또는 다른 사용자를 위해 가상 MFA 디바이스를 할당하거나 제거하려고 하면 다음과 같은 오류가 발생할 수 있습니다.

```
User: arn:aws:iam::123456789012:user/Diego is not authorized to perform:
 iam:DeleteVirtualMFADevice on resource: arn:aws:iam::123456789012:mfa/Diego with an
 explicit deny
```

이는 IAM 콘솔에서 이전에 다른 누군가가 가상 MFA 디바이스를 사용자에게 할당하기 시작했다가 프로세스를 취소한 경우 발생할 수 있습니다. 이렇게 하면 IAM에서 사용자를 위한 MFA 디바이스가 생성되지만 활성화되지는 않습니다. 새 디바이스를 사용자와 연결하려면 먼저 기존 MFA 디바이스를 삭제해야 합니다.

AWS에서는 사용자가 MFA를 사용하여 인증된 경우에만 자신의 가상 MFA 디바이스를 삭제할 수 있도록 허용하는 정책을 권장합니다. 자세한 내용은 AWS: MFA 인증 IAM 사용자가 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 자격 증명을 관리할 수 있도록 허용합니다. (p. 391) 단원을 참조하십시오.

이 문제를 해결하려면 관리자가 정책 권한을 편집하지 않아야 합니다. 대신 관리자는 AWS CLI 또는 AWS API를 사용하여 비활성화된 기존 디바이스를 제거해야 합니다.

비활성화된 기존 MFA 디바이스를 삭제하려면

1. 계정에서 가상 MFA 디바이스를 확인합니다.
   - AWS CLI: aws iam list-virtual-mfa-devices
   - AWS API: ListVirtualMFADevices
2. 응답에서 수정하려는 사용자의 가상 디바이스 ARN을 찾습니다.
3. 디바이스를 삭제합니다.
   - AWS CLI: aws iam delete-virtual-mfa-device
   - AWS API: DeleteVirtualMFADevice

IAM 정책 문제 해결

정책 (p. 349)은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 AWS의 엔터티입니다. AWS는 사용자와 같은 보안 주체가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지 여부를 결정합니다. 정책은 JSON 문서로 AWS에 저장되며 자격 증명 기반 정책으로 보안 주체에 연결되거나 리소스 기반 정책으로 리소스에 연결됩니다. 자격 증명 기반 정책을 IAM 그룹, 사용자 또는 역할과 같은 보안 주체(또는 자격 증명)에 연결할 수 있습니다. 자격 증명 기반 정책에는 AWS 관리형 정책, 고객 관리형 정책 및 인라인 정책이 포함됩니다. AWS Management 콘솔에서 Visual editor(시각적 편집기) 탭 또는 JSON 탭을 통해 고객 관리형 정책을 생성하고 편집할 수 있습니다. AWS Management 콘솔에서 정책을 볼 때 정책에서 부여된 권한의 요약을 볼 수 있습니다. 시각적 편집기 및 정책 요약을 사용하여 IAM 정책을 관리하는 동안 발생한 일반 오류를 진단하고 해결할 수 있습니다.

모든 IAM 정책은 JavaScript Object Notation(JSON) 규칙으로 시작하는 구문을 사용하여 저장됩니다. 정책을 생성 또는 관리하기 위해 이 구문을 이해할 필요가 없습니다. AWS Management 콘솔에서 시각적 편집기를 사용하여 정책을 생성하고 편집할 수 있습니다. IAM 정책의 JSON 구문에 대한 자세한 정보는 IAM JSON 정책 언어의 문법 (p. 637) 단원을 참조하십시오.

IAM 정책 주제 문제 해결

시각적 편집기를 사용하여 문제 해결

고객 관리형 정책을 생성 또는 편집할 때 Visual editor(시각적 편집기) 탭의 정보를 사용하여 정책의 오류를 해결할 수 있습니다. 시각적 편집기를 사용하여 정책을 생성하는 예제를 보려면 the section called “자격 증명에 대한 액세스 제어” (p. 376) 단원을 참조하십시오.

정책 재구성

정책을 생성할 때 AWS는 정책을 검증, 처리 및 변환한 후 저장합니다. AWS가 사용자 쿼리에 응답하여 정책을 반환하거나 콘솔에 표시할 경우 AWS는 정책에서 부여한 권한을 변경하지 않고 해당 정책을 사람이 읽을 수 있는 형식으로 다시 변환합니다. 이렇게 하면 정책 시각적 편집기 또는 JSON 탭에 표시되는 사항이 달라질 수 있습니다. 시각적 편집기 권한 블록이 추가, 제거 또는 재정렬될 수 있으며 블록 내의 내용이 최적화될 수 있습니다. JSON 탭에서 사소한 공백은 제거되며, JSON 맵 내의 요소는 재정렬될 수 있습니다. 또한 보안 주체 요소 내의 AWS 계정 ID는 AWS 계정 루트 사용자의 ARN으로 교체할 수 있습니다. 이러한 변경 가능성 때문에 JSON 정책 문서를 문자열로 비교하면 안 됩니다.

AWS Management 콘솔에서 고객 관리형 정책을 생성할 때 JSON 탭에서 완전히 작업하도록 선택할 수 있습니다. Visual editor(시각적 편집기)탭에서 변경을 수행하지 않고 JSON 탭에서 정책 검토를 선택하면 정책을 재구성할 가능성이 적습니다. 그러나 정책을 생성하고 Visual editor(시각적 편집기) 탭을 사용하여 수정한 경우 또는 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에서 모양을 최적화하기 위해 정책을 재구성할 수 있습니다.

이러한 재구성은 편집 세션에만 존재하며 자동으로 저장되지 않습니다.

편집 세션에서 정책이 재구성되면 IAM이 다음 상황에 따라 재구성을 저장할지 여부를 결정합니다.

이 탭에서	정책을 편집한 경우	그런 다음 이 탭에서 정책 검토를 선택한 경우	변경 사항 저장을 선택한 경우
Visual editor(시각적 편집기)	편집됨	Visual editor(시각적 편집기)	정책이 재구성됨
Visual editor(시각적 편집기)	편집됨	JSON	정책이 재구성됨
Visual editor(시각적 편집기)	편집되지 않음	Visual editor(시각적 편집기)	정책이 재구성됨
JSON	편집됨	Visual editor(시각적 편집기)	정책이 재구성됨

이 탭에서	정책을 편집한 경우	그런 다음 이 탭에서 정책 검토를 선택한 경우	변경 사항 저장을 선택한 경우
JSON	편집됨	JSON	정책 구성이 변경되지 않음
JSON	편집되지 않음	JSON	정책 구성이 변경되지 않음

IAM은 여러 서비스, 리소스 유형 또는 조건 키를 허용하는 문이나 권한 블록이 있는 정책 또는 복잡한 정책을 재구성할 수 있습니다.

시각적 편집기에서 리소스 ARN 선택

시각적 편집기를 사용하여 정책을 생성하거나 편집할 때 먼저 서비스를 선택한 다음 해당 서비스에서 작업을 선택해야 합니다. 선택한 서비스 및 작업이 특정 리소스 (p. 381) 선택을 지원하는 경우에는 시각적 편집기에 지원되는 리소스 유형이 나열됩니다. 그런 다음 Add ARN(ARN 추가)를 선택하여 리소스에 대한 세부 정보를 제공합니다. 리소스 유형에 대한 ARN을 추가하기 위해 다음 옵션에서 선택할 수 있습니다.

- ARN 빌더 사용 – 리소스 유형에 따라 ARN을 빌드하는 여러 필드가 표시될 수 있습니다. 모두 선택을 선택하여 지정된 설정의 값에 대한 권한을 제공할 수도 있습니다. 예를 들어, Amazon EC2 읽기 액세스 레벨 그룹을 선택하면 정책의 작업이 `instance` 리소스 유형을 지원합니다. 리소스에 대해 리전, 계정 및 InstanceId 값을 제공해야 합니다. 계정 ID를 제공하지만 리전 및 인스턴스 ID에 대해 모두 선택을 선택한 경우 정책은 계정의 모든 인스턴스에 대해 권한을 부여합니다.
- ARN 입력 또는 붙여넣기 – Amazon 리소스 이름(ARN) (p. 564)별로 리소스를 지정할 수 있습니다. ARN의 필드(각 콜론 쌍 사이)에 와일드카드 문자(*)를 포함할 수 있습니다. 자세한 정보는 IAM JSON 정책 요소: Resource (p. 597) 단원을 참조하십시오.

시각적 편집기에서 권한 거부

기본적으로 시각적 편집기를 사용하여 생성하는 정책은 사용자가 선택하는 작업을 허용합니다. 대신 선택한 작업을 거부하려면 Switch to deny permissions(권한 거부로 전환)을 선택합니다. 요청은 기본적으로 거부되므로 사용자에게 필요한 작업과 리소스에만 권한을 허용하는 것이 보안 모범 사례입니다. 이것을 "화이트리스트"라고 부르기도 합니다. 다른 문이나 정책에서 허용되는 권한을 별도로 재정의하려는 경우에만 권한을 거부("블랙리스트")하기 위한 문을 생성해야 합니다. 권한 거부의 수가 늘어나면 권한 문제를 해결하기가 더 어려워질 수 있기 때문에 그 수를 최소한으로 제한하는 것이 좋습니다. IAM이 정책 로직을 평가하는 방법에 대한 자세한 정보는 정책 평가 로직 (p. 622) 단원을 참조하십시오.

> **Note**
>
> 기본적으로 AWS 계정 루트 사용자만 해당 계정의 모든 리소스에 액세스할 수 있습니다. 따라서 루트 사용자로 로그인하지 않은 경우 정책이 부여한 권한이 있어야 합니다.

시각적 편집기에서 여러 서비스 지정

시각적 편집기를 사용하여 정책을 생성할 때 한 번에 서비스 하나만 선택할 수 있습니다. 시각적 편집기는 해당 서비스 하나에 대한 작업에서 선택할 수 있도록 허용하므로 이렇게 하는 것이 모범 사례입니다. 그런 다음 해당 서비스 및 선택한 작업에서 지원되는 리소스 중에서 선택합니다. 이렇게 하면 정책을 쉽게 생성하고 문제를 해결할 수 있습니다.

JSON 구문에 대해 잘 알고 있는 경우 와일드카드 문자(*)를 사용하여 여러 서비스를 수동으로 지정할 수도 있습니다. 예를 들어, **`Code*`**를 입력하여 `CodeBuild` 및 `CodeCommit`과 같이 `Code`로 시작하는 모든 서비스에 대한 권한을 제공합니다. 그러나 정책을 완료하려면 작업 및 리소스 ARN을 입력해야 합니다. 또한 정책을 저장하면 각 서비스를 별도의 권한 블록에 포함하도록 정책이 재구성 (p. 538)될 수 있습니다.

또는 서비스에 대해 JSON 구문(예: 와일드카드)을 사용하기 위해 JSON 탭을 통해 정책을 생성, 편집 및 저장합니다.

시각적 편집기에서 정책의 크기 줄이기

시각적 편집기를 사용하여 정책을 생성할 때 IAM은 정책을 저장하기 위해 JSON 문서를 생성합니다. JSON 탭으로 전환하여 이 문서를 볼 수 있습니다. 이 JSON 문서가 정책의 크기 제한을 초과할 경우, 시각적 편집기에 오류 메시지가 표시되며 정책을 검토하거나 저장할 수 없습니다. 관리형 정책의 크기에 대한 IAM 제한을 보려면 IAM 및 STS 문자 제한 (p. 571) 단원을 참조하십시오.

시각적 편집기에서 정책의 크기를 줄이려면 정책을 편집하거나 권한 블록을 다른 정책으로 옮깁니다. 오류 메시지에는 정책 문서에 포함된 문자 수가 포함되며, 이 정보를 통해 정책의 크기를 줄일 수 있습니다.

시각적 편집기에서 인식할 수 없는 서비스, 작업 또는 리소스 유형 수정

시각적 편집기에서 정책을 생성하거나 편집할 때 정책에 인식할 수 없는 서비스, 작업 또는 리소스 유형이 포함되어 있다는 경고가 표시될 수 있습니다.

> Note
>
> IAM은 정책 요약을 지원하는 서비스의 이름, 작업 및 리소스 유형을 검토합니다. 그러나 존재하지 않는 리소스 값이나 조건이 정책 요약에 포함될 수 있습니다. 항상 정책 시뮬레이터 (p. 441)로 정책을 테스트합니다.

정책에 인식할 수 없는 서비스, 작업 또는 리소스 유형이 포함되는 경우 다음 오류 중 하나가 발생한 것입니다.

- 미리 보기 서비스 – 미리 보기에 있는 서비스는 시각적 편집기를 지원하지 않습니다. 미리 보기에 참여하고 있는 경우 경고를 무시하고 계속 진행할 수 있지만, 정책을 완료하려면 작업 및 리소스 ARN을 수동으로 입력해야 합니다. 또는 JSON 탭을 선택하여 JSON 정책 문서를 입력하거나 붙여 넣을 수 있습니다.
- 사용자 지정 서비스 – 사용자 지정 서비스는 시각적 편집기를 지원하지 않습니다. 사용자 지정 서비스를 사용하고 있는 경우 경고를 무시하고 계속 진행할 수 있지만, 정책을 완료하려면 작업 및 리소스 ARN을 수동으로 입력해야 합니다. 또는 JSON 탭을 선택하여 JSON 정책 문서를 입력하거나 붙여 넣을 수 있습니다.
- 시각적 편집기를 지원하지 않는 서비스 – 정책에 시각적 편집기를 지원하지 않는 정식 버전(GA) 서비스가 포함되어 있는 경우 경고를 무시하고 계속 진행할 수 있지만, 정책을 완료하려면 작업 및 리소스 ARN을 수동으로 입력해야 합니다. 또는 JSON 탭을 선택하여 JSON 정책 문서를 입력하거나 붙여 넣을 수 있습니다.

  일반적으로 사용할 수 있는 서비스는 공개적으로 출시된 서비스이며 프리뷰 또는 사용자 지정 서비스가 아닙니다. 인식할 수 없는 서비스를 일반적으로 사용할 수 있고 이름을 올바르게 입력한 경우 서비스는 시각적 편집기를 지원하지 않습니다. GA 서비스에 대한 시각적 편집기 또는 정책 요약 지원을 요청하는 방법을 알아보려면 서비스가 IAM 정책 요약을 지원하지 않음 (p. 542) 단원을 참조하십시오.
- 시각적 편집기를 지원하지 않는 작업 – 지원되지 않는 작업과 함께 지원되는 서비스가 정책에 포함되어 있는 경우 경고를 무시하고 계속 진행할 수 있지만, 정책을 완료하려면 리소스 ARN을 수동으로 입력해야 합니다. 또는 JSON 탭을 선택하여 JSON 정책 문서를 입력하거나 붙여 넣을 수 있습니다.

  지원되지 않는 작업과 함께 지원되는 서비스가 정책에 포함되어 있으면 서비스가 시각적 편집기를 완전히 지원하지 않습니다. GA 서비스에 대한 시각적 편집기 또는 정책 요약 지원을 요청하는 방법을 알아보려면 서비스가 IAM 정책 요약을 지원하지 않음 (p. 542) 단원을 참조하십시오.
- 시각적 편집기를 지원하지 않는 리소스 유형 – 지원되지 않는 리소스 유형과 함께 지원되는 작업이 정책에 포함되어 있는 경우 경고를 무시하고 계속 진행할 수 있습니다. 그러나 IAM은 선택한 모든 작업에 대한 리소스를 포함했는지 여부를 확인할 수 없으며, 추가 경고가 표시될 수 있습니다.
- 오타 – 시각적 편집기에 서비스, 작업 또는 리소스를 수동으로 입력할 경우 오타가 포함된 정책이 생성될 수 있습니다. 시각적 편집기를 사용하여 서비스 및 작업 목록에서 선택한 다음 표시되는 메시지에 따라 리

소스 섹션을 완료하는 것이 모범 사례입니다. 그러나 서비스가 시각적 편집기를 완전히 지원하지 않는 경우 정책의 부분을 수동으로 입력해야 할 수 있습니다.

정책에 위와 같은 오류가 없다는 것을 확신한다면 오타가 포함된 것일 수 있습니다. 서비스, 작업 및 리소스 유형 이름에 오탈자가 있는지 확인합니다. 예를 들어 `s2` 대신 `s3`를 사용하고, `ListMyBuckets` 대신 `ListAllMyBuckets`을 사용할 수 있습니다. 또 다른 일반적인 작업 오타는 ARN에 불필요한 텍스트를 추가(예: `arn:aws:s3: : :*`)하거나 작업에서 콜론을 누락(예: `AWSAuthRuntimeService.AuthenticatePassword`)하는 것입니다. 정책 검토를 선택하여 정책 요약을 검토하고 정책이 의도한 권한을 제공하는지 여부를 확인하여 정책에 오타가 있는지를 평가할 수 있습니다.

정책 요약을 사용하여 문제 해결

정책 요약과 관련된 문제를 진단하고 해결할 수 있습니다.

정책 요약 누락

IAM 콘솔에는 정책에서 각 서비스에 대해 허용되거나 거부되는 액세스 레벨, 리소스, 조건을 설명하는 정책 요약 테이블이 포함되어 있습니다. 정책은 3가지 테이블, 즉 정책 요약 (p. 484), 서비스 요약 (p. 493), 작업 요약 (p. 497)으로 요약됩니다. 정책 요약 테이블에는 서비스 목록과 선택한 정책에 의해 정의된 권한의 요약이 포함되어 있습니다. 사용자 페이지에서 사용자에게 연결된 정책에 대한 정책 요약 (p. 483)을 볼 수 있습니다. 정책 페이지에서 관리형 정책에 대한 정책 요약을 볼 수 있습니다. AWS가 정책 요약을 렌더링할 수 없는 경우 요약 대신 JSON 정책 문서가 제공되며 다음 오류가 표시됩니다.

A summary for this policy cannot be generated. You can still view or edit the JSON policy document.

정책이 요약을 포함하지 않을 경우 다음 오류 중 하나가 발생한 것입니다.

- 지원되지 않는 정책 요소 – IAM은 다음 정책 요소 (p. 586) 중 하나를 포함하는 정책에 대해 정책 요약 생성을 지원하지 않습니다.
  - `Principal`
  - `NotPrincipal`
  - `NotResource`
- 정책 권한 없음 – 정책이 유효한 권한을 제공하지 않을 경우 정책 요약을 생성할 수 없습니다. 예를 들어 정책이 요소 `"NotAction": "*"`과 함께 단일 명령문을 포함하는 경우 이 정책은 "모든 작업"(*)을 제외한 모든 작업에 대한 액세스 권한을 부여합니다. 즉 어떤 작업에 대해서도 `Deny` 또는 `Allow` 액세스 권한을 부여하지 않습니다.

  Note

  `NotPrincipal`, `NotAction`, `NotResource` 등의 이러한 정책 요소를 사용할 때는 주의해야 합니다. 정책 요소 사용에 대한 자세한 정보는 IAM JSON 정책 요소 참조 (p. 586) 단원을 참조하십시오.

  일치하지 않는 서비스와 리소스를 제공하는 경우 유효한 권한을 제공하지 않는 정책을 생성할 수 있습니다. 이는 한 서비스의 작업과 다른 서비스의 리소스를 지정하는 경우에 발생할 수 있습니다. 이 경우에는 정책 요약이 나타납니다. 요약의 리소스 열에 다른 서비스의 리소스를 포함할 수 있는 경우에만 문제가 있다는 표시가 나타납니다. 이 열에 일치하지 않는 리소스가 포함되어 있으면 정책에 오류가 있는지 검토해야 합니다. 정책을 더 잘 이해하려면 항상 정책 시뮬레이터 (p. 441)로 테스트합니다.

정책 요약에 인식할 수 없는 서비스, 작업 또는 리소스 유형 포함됨

IAM 콘솔에서 정책 요약 (p. 483)에 경고 기호()가 있으면 정책 요약에 인식할 수 없는 서비스, 작업 또는 리소스 유형이 포함되었을 수 있습니다. 정책 요약 내의 경고에 대해 알아보려면 정책 요약(서비스 목록) (p. 484)을 참조하십시오.

Note

IAM은 정책 요약을 지원하는 서비스의 이름, 작업 및 리소스 유형을 검토합니다. 그러나 존재하지 않는 리소스 값이나 조건이 정책 요약에 포함될 수 있습니다. 항상 정책 시뮬레이터 (p. 441)로 정책을 테스트합니다.

정책에 인식할 수 없는 서비스, 작업 또는 리소스 유형이 포함되는 경우 다음 오류 중 하나가 발생한 것입니다.

- 미리 보기 서비스 – 미리 보기에 있는 서비스는 정책 요약을 지원하지 않습니다.
- 사용자 지정 서비스 – 사용자 지정 서비스는 정책 요약을 지원하지 않습니다.
- 서비스가 요약을 지원하지 않음 – 정책 요약을 지원하지 않는 정식 버전(GA) 서비스가 정책에 포함되어 있으면 서비스가 정책 요약 테이블의 Unrecognized services(알 수 없는 서비스) 섹션에 포함됩니다. 일반적으로 사용할 수 있는 서비스는 공개적으로 출시된 서비스이며 프리뷰 또는 사용자 지정 서비스가 아닙니다. 인식할 수 없는 서비스가 정식 버전이고 이름을 올바르게 입력한 경우에는 서비스에서 IAM 정책 요약을 지원하지 않습니다. GA 서비스에 대한 정책 요약 지원을 요청하는 방법을 알아보려면 서비스가 IAM 정책 요약을 지원하지 않음 (p. 542)을 참조하십시오.
- 작업이 요약을 지원하지 않음 – 지원되지 않는 작업과 함께 지원되는 서비스가 정책에 포함되어 있으면 작업이 서비스 요약 테이블의 Unrecognized actions(알 수 없는 작업) 섹션에 포함됩니다. 서비스 요약 내의 경고에 대해 알아보려면 서비스 요약(작업 목록) (p. 493)을 참조하십시오.
- 리소스 유형이 요약을 지원하지 않음 – 정책에 지원되지 않는 리소스 유형을 가진 지원되는 작업이 포함된 경우, 서비스 요약 테이블의 Unrecognized resource types(인식되지 않은 리소스 유형) 섹션에 리소스가 포함됩니다. 서비스 요약 내의 경고에 대해 알아보려면 서비스 요약(작업 목록) (p. 493)을 참조하십시오.
- 오타 – AWS의 정책 검증기는 JSON의 구문이 정확한지 여부만 검사하므로 생성한 정책에 오타가 포함될 수 있습니다. 정책에 위와 같은 오류가 없다는 것을 확신한다면 오타가 포함된 것일 수 있습니다. 서비스, 작업 및 리소스 유형 이름에 오탈자가 있는지 확인합니다. 예를 들어 `s2` 대신 `s3`를 사용하고, `ListMyBuckets` 대신 `ListAllMyBuckets`을 사용할 수 있습니다. 또 다른 일반적인 작업 오타는 ARN에 불필요한 텍스트를 추가(예: `arn:aws:s3: : :*`)하거나 작업에서 콜론을 누락(예: `AWSAuthRuntimeService.AuthenticatePassword`)하는 것입니다. 정책 검증기 (p. 441)를 사용하여 정책이 의도된 권한을 제공하는지 여부를 확인하여 정책에 오타가 있는지 검사할 수 있습니다.

서비스가 IAM 정책 요약을 지원하지 않음

정식 버전(GA) 서비스 또는 작업이 IAM 정책 요약 또는 시각적 편집기에서 인식되지 않으면 서비스가 이러한 기능을 지원하지 않을 수 있습니다. 일반적으로 사용할 수 있는 서비스는 공개적으로 출시된 서비스이며 프리뷰 또는 사용자 지정 서비스가 아닙니다. 인식할 수 없는 서비스를 일반적으로 사용할 수 있고 이름을 올바르게 입력한 경우 서비스는 이러한 기능을 지원하지 않습니다. 지원되지 않는 작업과 함께 지원되는 서비스가 정책에 포함되어 있으면 서비스가 IAM 정책 요약을 완전히 지원하지 않습니다.

서비스에서 IAM 정책 요약 또는 시각적 편집기 지원을 추가하도록 요청하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 지원되지 않는 서비스가 포함된 정책을 찾습니다.
   - 그 정책이 관리형 정책인 경우, 탐색 창에서 정책을 선택합니다. 정책 목록에서 보려는 정책의 이름을 선택합니다.
   - 사용자에게 연결된 인라인 정책인 경우, 탐색 창에서 사용자를 선택합니다. 사용자 목록에서 정책을 보려는 사용자의 이름을 선택합니다. 사용자에 대한 정책 테이블에서 보려는 정책 요약의 헤더를 확장합니다.
3. 왼쪽의 AWS Management 콘솔 바닥글에서 의견을 선택합니다. Tell us about your experience(귀하의 작업 환경에 대해 말씀해 주십시오) 상자에 **`I request that the <ServiceName> service add support for IAM policy summaries and the visual editor`**를 입력하십시오. 요약 지원을

바라는 서비스가 두 개 이상인 경우 **`I request that the <ServiceName1>, <ServiceName2>, and <ServiceName3> services add support for IAM policy summaries and the visual editor`**라고 입력합니다

서비스에서 누락된 작업에 대한 IAM 정책 요약 지원을 추가하도록 요청하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 지원되지 않는 서비스가 포함된 정책을 찾습니다.
   - 그 정책이 관리형 정책인 경우, 탐색 창에서 정책을 선택합니다. 정책 목록에서 보려는 정책의 이름을 선택합니다.
   - 사용자에게 연결된 인라인 정책인 경우, 탐색 창에서 사용자를 선택합니다. 사용자 목록에서 정책을 보려는 사용자의 이름을 선택합니다. 사용자에 대한 정책 표에서 보려는 정책의 이름을 선택하여 정책 요약을 펼칩니다.
3. 정책 요약에서 지원되지 않는 작업을 포함하는 서비스의 이름을 선택합니다.
4. 왼쪽의 AWS Management 콘솔 바닥글에서 의견을 선택합니다. Tell us about your experience(귀하의 작업 환경에 대해 말씀해 주십시오) 상자에 **`I request that the <ServiceName> service add IAM policy summary and the visual editor support for the <ActionName> action`**를 입력하십시오. 지원되지 않는 작업을 두 개 이상 보고하는 경우 **`I request that the <ServiceName> service add IAM policy summary and the visual editor support for the <ActionName1>, <ActionName2>, and <ActionName3> actions`**라고 입력합니다

다른 서비스에 누락된 작업을 포함하도록 요청하려면 마지막 세 단계를 반복합니다.

정책이 필요한 권한을 부여하지 않음

사용자, 그룹, 역할 또는 리소스에 권한을 할당하려면 권한을 정의하는 문서인 정책을 생성해야 합니다. 정책 문서에는 다음 요소가 포함됩니다.

- Effect – 정책에서 액세스를 허용하는지 또는 거부하는지 여부
- Action – 정책에서 허용하거나 거부하는 작업 목록
- Resource – 작업이 발생할 수 있는 리소스 목록
- 조건(선택 사항) – 정책에서 권한을 부여하는 상황

이러한 요소와 기타 정책 요소에 대한 자세한 정보는 IAM JSON 정책 요소 참조 (p. 586) 단원을 참조하십시오.

액세스 권한을 부여하려면 정책이 지원되는 리소스를 가진 작업을 정의해야 합니다. 정책에 조건도 있는 경우 이 조건은 전역 조건 키 (p. 650)를 포함해야 하거나, 작업에 적용해야 합니다. 작업에서 어떤 리소스를 지원하는지 확인하려면 해당 서비스의 AWS 설명서를 참조하십시오. 작업에서 어떤 조건을 지원하는지 확인하려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

정책에서 권한을 부여하지 않는 작업, 리소스 또는 조건을 정의하는지 확인하려면 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 사용하여 해당 정책의 정책 요약 (p. 484)을 보십시오. 정책 요약을 사용하여 정책의 문제를 식별하고 수정할 수 있습니다.

IAM 정책에 정의되었는데도 요소가 권한을 부여하지 않는 몇 가지 이유는 다음과 같습니다.

- 적용 가능한 리소스 없이 작업이 정의된 경우 (p. 544)
- 적용 가능한 작업 없이 리소스가 정의된 경우 (p. 544)
- 적용 가능한 작업 없이 조건이 정의된 경우 (p. 545)

경고를 포함하는 정책 요약의 예를 보려면 the section called “정책 요약(서비스 목록)” (p. 484) 단원을 참조하십시오.

적용 가능한 리소스 없이 작업이 정의된 경우

아래 정책은 모든 `ec2:Describe*` 작업과 특정 리소스를 정의합니다. 이러한 작업 중에서 리소스 수준 권한을 지원하는 작업이 없기 때문에 어떤 `ec2:Describe` 작업도 부여되지 않습니다. 리소스 수준 권한이란 작업이 정책의 `Resource` (p. 597) 요소에 있는 ARN (p. 564)을 사용하여 리소스를 지원함을 의미합니다. 작업이 리소스 수준 권한을 지원하지 않는 경우에는 정책의 이 명령문에서 `*` 요소에 와일드카드(`Resource`)를 사용해야 합니다. 리소스 수준 권한을 서비스에 대해 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "ec2:Describe*",
        "Resource": "arn:aws:ec2:us-east-2:ACCOUNT-ID:instance/*"
    }]
}
```

이 정책은 어떤 권한도 제공하지 않으며, 정책 요약에는 다음 오류가 포함됩니다.

```
This policy does not grant any permissions. To grant access, policies must have
an action that has an applicable resource or condition.
```

정책을 수정하려면 `*` 요소에 `Resource`를 사용해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "ec2:Describe*",
        "Resource": "*"
    }]
}
```

적용 가능한 작업 없이 리소스가 정의된 경우

아래 정책은 Amazon S3 버킷 리소스를 정의하지만, 해당 리소스에서 수행할 수 있는 S3 작업을 포함하지 않습니다. 이 정책은 또한 모든 Amazon CloudFront 작업에 대한 전체 액세스 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "cloudfront:*",
        "Resource": [
            "arn:aws:cloudfront:*",
            "arn:aws:s3:::examplebucket"
        ]
    }]
}
```

이 정책은 모든 CloudFront 작업에 대한 권한을 제공합니다. 하지만 정책에서 S3 작업을 정의하지 않고 S3 `examplebucket` 리소스를 정의하기 때문에 정책 요약에 다음 경고가 표시됩니다.

```
This policy defines some actions, resources, or conditions that do not provide
permissions. To grant access, policies must have an action that has an
applicable resource or condition.
```

이 정책을 수정하여 S3 버킷 권한을 제공하려면 버킷 리소스에서 수행할 수 있는 S3 작업을 정의해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "cloudfront:*",
            "s3:CreateBucket",
            "s3:ListBucket*",
            "s3:PutBucket*",
            "s3:GetBucket*"
        ],
        "Resource": [
            "arn:aws:cloudfront:*",
            "arn:aws:s3:::examplebucket"
        ]
    }]
}
```

또는 이 정책을 수정하여 CloudFront 권한만 제공하려면 S3 리소스를 삭제하십시오.

적용 가능한 작업 없이 조건이 정의된 경우

아래 정책은 S3 접두사가 `custom`이고 버전 ID가 `1234`일 경우 모든 S3 리소스에 대해 2개의 Amazon S3 작업을 정의합니다. 하지만 `s3:VersionId` 조건 키가 객체 버전 태그 지정에 사용되었으며, 정의된 버킷 작업이 이 조건 키를 지원하지 않습니다. 작업에서 어떤 조건을 지원하는지 알아보려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하고, 링크를 클릭하여 조건 키에 대한 서비스 설명서를 보십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucketVersions",
                "s3:ListBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "custom"
                    ],
                    "s3:VersionId": [
                        "1234"
                    ]
                }
            }
        }
    ]
}
```

이 정책은 버킷 이름에 `s3:ListBucketVersions` 접두사가 있는 경우 `s3:ListBucket` 작업 및 `custom` 작업에 대한 권한을 제공합니다. 하지만 정의된 작업 중 `s3:VersionId` 조건을 지원하는 작업이 없기 때문에 정책 요약에 다음 오류가 표시됩니다.

```
This policy does not grant any permissions. To grant access, policies must have
an action that has an applicable resource or condition.
```

이 정책을 수정하여 S3 객체 버전 태그 지정을 사용하려면, `s3:VersionId` 조건 키를 지원하는 S3 작업을 정의해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:GetObjectVersion"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "custom"
                    ],
                    "s3:VersionId": [
                        "1234"
                    ]
                }
            }
        }
    ]
}
```

이 정책은 정책의 모든 작업과 조건에 대한 권한을 제공합니다. 하지만 하나의 작업이 모든 조건을 충족하는 경우가 없기 때문에 어떤 권한도 제공하지 않습니다. 이렇게 하는 대신, 적용할 조건을 갖는 작업만 각각 포함하도록 두 개의 구문을 별도로 작성해야 합니다.

이 정책을 수정하려면 두 개의 구문을 작성합니다. 첫째 구문에는 `s3:prefix` 조건을 지원하는 작업이 포함되고, 둘째 구문에는 `s3:VersionId` 조건을 지원하는 작업이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucketVersions",
                "s3:ListBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:prefix": "custom"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObjectVersion",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:VersionId": "1234"
                }
            }
        }
    ]
}
```

정책 관리 문제 해결

정책 관리와 관련된 문제를 진단하고 해결할 수 있습니다.

IAM 계정에서 정책 연결 또는 분리

일부 AWS 관리형 정책은 서비스에 연결되어 있습니다. 이러한 정책은 해당 서비스에 대한 서비스 연결 역할 (p. 175)에서만 사용됩니다. IAM 콘솔에서 정책의 요약 페이지를 보면 페이지에 정책이 서비스에 연결되어 있음을 나타내는 배너가 포함되어 있습니다. 이 정책을 IAM 내의 사용자, 그룹 또는 역할에 연결할 수 없습니다. 서비스에 대한 서비스 연결 역할을 생성하면 이 정책이 새 역할에 자동으로 연결됩니다. 정책이 필요하므로 서비스 연결 역할에서 정책을 분리할 수 없습니다.

작업 기반 IAM 자격 증명 관련 정책 변경

작업에 따라 IAM 자격 증명(사용자, 그룹 및 역할)에 대한 정책을 업데이트할 수 있습니다. 이 작업을 수행하려면 CloudTrail 이벤트 이력에서 계정의 이벤트를 확인합니다. CloudTrail 이벤트 로그에는 정책의 권한을 변경하는 데 사용할 수 있는 자세한 이벤트 정보가 포함되어 있습니다. 사용자 또는 역할이 AWS에서 작업을 수행하려 하고 요청이 거부된 것을 알 수 있습니다. 이러한 경우 사용자 또는 역할에 작업을 수행할 권한이 있어야 하는지 여부를 고려할 수 있습니다. 권한을 부여해야 하는 경우 해당 작업과 이들이 액세스하려고 했던 리소스의 ARN도 정책에 추가할 수 있습니다. 또는, 사용자나 역할에 사용하지 않는 권한이 있는 경우 정책에서 그러한 권한을 제거하는 것을 고려할 수도 있습니다. 정책은 필요한 작업을 수행하는 데 필요한 최소 권한 (p. 61)만 부여해야 합니다. CloudTrail 사용에 대한 자세한 정보는 AWS CloudTrail 사용 설명서의 CloudTrail 콘솔에서 CloudTrail 이벤트 보기 단원을 참조하십시오.

JSON 정책 문서 문제 해결

JSON 정책 문서와 관련된 문제를 진단하고 해결할 수 있습니다.

JSON 정책 객체가 둘 이상인 경우

IAM 정책은 단 하나의 JSON 객체로 구성되어야 합니다. 객체는 중괄호 { }로 묶어 표시합니다. 대괄호 [ ] 안에 중괄호 { }를 추가로 삽입하여 JSON 객체 내에 다른 객체를 중첩시킬 수도 있지만 정책에 따라 중괄호 { }를 묶는 대괄호 [ ]는 하나로 제한됩니다. 다음 예제는 최상위 레벨에 객체 2개가 추가되었기 때문에 올바르지 않습니다(###으로 표시).

```
{
      "Version": "2012-10-17",
      "Statement":
      {
         "Effect":"Allow",
         "Action":"ec2:Describe*",
         "Resource":"*"
      }
   }
   {
     "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::my-bucket/*"
     }
   }
```

하지만 올바른 정책 문법을 사용하여 위 예제의 의도를 만족하는 방법도 있습니다. 2개의 정책 객체에 `Statement` 요소를 각각 추가하지 않고 두 블록을 단일 `Statement` 요소로 결합하면 됩니다. 그러면 다음 예제와 같이 `Statement` 요소가 두 객체의 배열을 값으로 인식합니다(굵은체로 표시).

```
{
```

```
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Action": "ec2:Describe*",
          "Resource":" *"
        },
        {
          "Effect": "Allow",
          "Action": "s3:*",
          "Resource": "arn:aws:s3:::my-bucket/*"
        }
      ]
    }
```

JSON Statement 요소가 둘 이상인 경우

이 오류는 처음에는 위 오류의 변형으로 보일 수도 있습니다. 하지만 구문으로 보면 다른 유형의 오류입니다. 다음 예제에는 중괄호 {} 한 쌍이 최상위 레벨로 정책 객체 하나만 표시하고 있습니다. 하지만 객체에 포함된 `Statement` 요소는 2개입니다.

IAM 정책에서는 콜론 왼쪽의 이름(`Statement`)과 오른쪽의 값으로 구성된 `Statement` 요소 1개만 추가할 수 있습니다. 그리고, `Statement` 요소의 값은 `Effect` 요소 1개와 `Action` 요소 1개, 그리고 `Resource` 요소 1개가 중괄호 {}로 묶여 구성된 객체가 되어야 합니다. 다음 예제는 정책 객체에 `Statement` 요소가 2개 포함되었기 때문에 올바르지 않습니다(###으로 표시).

```
{
      "Version": "2012-10-17",
      "Statement": {
        "Effect": "Allow",
        "Action": "ec2:Describe*",
        "Resource": "*"
      },
      "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::my-bucket/*"
      }
    }
```

값 객체는 여러 값 객체의 배열일 수 있습니다. 이 문제를 해결하려면, 다음 예제와 같이 객체 배열을 사용하여 2개의 `Statement` 요소를 하나로 결합합니다(굵은체로 표시).

```
{
      "Version": "2012-10-17",
      "Statement": [    {
          "Effect": "Allow",
          "Action": "ec2:Describe*",
          "Resource":"*"
        },
        {
          "Effect": "Allow",
          "Action": "s3:*",
          "Resource": "arn:aws:s3:::my-bucket/*"
        }
     ]
    }
```

`Statement` 요소 값이 객체 배열이 되었습니다. 이제 위 예제의 배열은 두 객체로 구성되며, 각 객체 자체가 정확한 `Statement` 요소 값으로 인식됩니다. 배열을 구성하는 각 객체는 쉼표로 구분합니다.

JSON Statement 요소의 Effect, Action 또는 Resource 요소가 둘 이상인 경우

Statement 이름/값 쌍에서 값 부분을 보면 객체가 Effect 요소 1개, Action 요소 1개, 그리고 Resource 요소 1개로 구성되어야 합니다. 다음은 Effect의 값 객체에 Statement 요소가 2개이기 때문에 잘못된 정책입니다.

```
{
      "Version": "2012-10-17",
      "Statement": {
        "Effect": "Deny",
        "Effect": "Allow",
        "Action": "ec2:* ",
        "Resource": "*"
      }
    }
```

Note

정책 엔진은 새로운 정책이나 편집된 정책에서 이러한 오류를 허용하지 않습니다. 하지만 정책 엔진은 엔진 업데이트 이전에 저장된 정책은 계속 허용합니다. 오류와 관련한 기존 정책 특성은 아래와 같습니다.

- Effect 요소가 다수일 때: 마지막 Effect 요소만 따릅니다. 나머지 요소는 모두 무시됩니다.
- Action 요소가 다수일 때: Action 요소가 모두 내부적으로 결합되어 마치 단일 목록인 것처럼 처리됩니다.
- Resource 요소가 다수일 때: Resource 요소가 모두 내부적으로 결합되어 마치 단일 목록인 것처럼 처리됩니다.

정책 엔진은 구문 오류 정책을 저장하도록 허용하지 않습니다. 따라서 저장하기 전에 정책 오류를 정정해야 합니다. 정책 검사기 (p. 441)는 이전 정책 오류를 찾는 데 효과적일 뿐만 아니라 정정 방법까지 알려주는 도구입니다.

모든 경우 해결책은 잘못 추가된 요소를 삭제하는 것입니다. Effect 요소일 때는 삭제 방법이 간단합니다. 앞의 예제에서 Amazon EC2 인스턴스에 대한 권한을 거부하고 싶다면 다음과 같이 정책에서 "Effect": "Allow", 라인을 삭제하면 됩니다.

```
{
      "Version": "2012-10-17",
      "Statement": {
        "Efect": "Deny",
        "Action": "ec2:* ",
        "Resource": "*"
      }
    }
```

하지만 중복 요소가 Action 또는 Resource인 경우에는 해결 방법이 더욱 복잡합니다. 권한을 허용(또는 거부)하려는 작업이 다수일 수도 있고, 여러 리소스에 대한 액세스를 제어할 수도 있기 때문입니다. 예를 들어 다음 예제는 Resource 요소가 여러 개이기 때문에 올바르지 않습니다(###으로 표시).

```
{
      "Version": "2012-10-17",
      "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
```

```
        "Resource": "arn:aws:s3:::my-bucket",
        "Resource": "arn:aws:s3:::my-bucket/*"
      }
    }
```

Statement 요소의 값 객체에서 필요한 요소는 각각 한 번만 표시할 수 있습니다. 해결책은 객체 배열에 값을 하나씩만 지정하는 것입니다. 다음 예제는 배열을 값 객체로 사용하여 2개의 리소스 요소를 1개의 Resource 요소로 결합함으로써 이를 설명합니다(굵은체로 표시).

```
{
      "Version": "2012-10-17",
      "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": [
          "arn:aws:s3:::my-bucket",
          "arn:aws:s3:::my-bucket/*"
        ]
      }
    }
```

JSON 버전 요소 누락

Version 정책 요소는 정책 버전과 다릅니다. Version 정책 요소는 정책 내에서 사용되며 정책 언어의 버전을 정의합니다. 반면에 정책 버전은 IAM에서 고객 관리형 정책을 변경할 때 생성됩니다. 변경된 정책은 기존 정책을 덮어쓰지 않습니다. 대신 IAM에서 관리형 정책의 새 버전을 만듭니다. Version 정책 요소에 대한 자세한 정보는 IAM JSON 정책 요소: Version (p. 587)을 참조하십시오. 정책 버전에 대한 자세한 정보는 the section called “IAM 정책 버전 관리” (p. 458) 단원을 참조하십시오.

AWS 기능이 점차 진화하면서 IAM 정책에도 이를 지원할 수 있도록 새로운 기능이 추가되었습니다. 간혹 정책 구문이 업데이트될 때마다 새로운 버전 번호가 추가됩니다. 정책 문법에서 최신 기능을 사용하는 경우에는 정책 구문 분석 엔진에게 사용 버전을 알려주어야 합니다. 기본 정책 버전은 "2008-10-17"입니다. 이때 이후 추가된 정책 기능을 사용하려면 원하는 기능을 지원하는 버전 번호를 지정해야 합니다. 따라서 항상 최신 정책 구문 버전 번호("Version": "2012-10-17")를 추가할 것을 권장합니다. 예를 들어 다음 정책은 리소스에 대해 ARN의 ${...} 변수를 사용하기 때문에 올바르지 않습니다. 정책 변수를 지원하는 정책 구문 버전을 지정하는 데 실패합니다(*red*에서 호출).

```
{
  "Statement":
  {
    "Action": "iam:*AccessKey*",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::123456789012:user/${aws:username}"
  }
}
```

다음과 같이 정책 상단에 정책 변수를 지원하는 첫 번째 IAM API 버전인 2012-10-17 값과 함께 Version 요소를 추가하면 이 문제가 해결됩니다(굵은체로 표시).

```
{
  "Version": "2012-10-17",
  "Statement":
  {
    "Action": "iam:*AccessKey*",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::123456789012:user/${aws:username}"
  }
}
```

U2F 보안 키 문제 해결

여기 정보를 사용하여 U2F 보안 키 작업 시 공통적으로 발생할 수 있는 문제를 진단하십시오.

주제

U2F 보안 키를 활성화할 수 없습니다.

IAM 사용자인지 시스템 관리자인지 자신의 상태에 따라 다음 해결 방법을 문의하십시오.

IAM 사용자

U2F 보안 키가 활성화되지 않으면 다음 사항을 확인하십시오.

- 지원되는 구성을 사용 중입니까?

  U2F 및 AWS에 사용할 수 있는 디바이스 및 브라우저 정보는 U2F 보안 키 사용에 지원되는 구성 (p. 129)을 확인하십시오.
- Mozilla Firefox를 사용 중입니까?

  U2F를 지원하는 대부분의 Firefox 버전은 기본적으로 지원을 활성화하지 않습니다. Firefox에서 U2F 지원을 활성화하려면 다음과 같이 하십시오.

  1. Firefox 주소 표시줄에 **`about:config`**를 입력합니다.
  2. 열리는 화면의 검색줄에 기본 **`u2f`**를 입력합니다.
  3. security.webauth.u2f를 선택하고 값을 true로 변경합니다.
- 브라우저 플러그인을 사용 중입니까?

  AWS는 플러그인 사용을 통한 U2F 브라우저 지원 추가를 지원하지 않습니다. 대신 U2F 표준을 기본적으로 지원하는 브라우저를 사용하십시오.

  지원되는 브라우저를 사용하더라도 U2F와 호환되지 않는 플러그인이 있을 수 있습니다. 호환되지 않는 플러그인이 있으면 U2F 보안 키를 활성화하고 사용하지 못할 수 있습니다. 호환되지 않는 플러그인을 모두 비활성화하고 브라우저를 새로 시작해야 합니다. 그런 다음 U2F 보안 키를 다시 활성화해 보십시오.
- 적절한 권한이 있습니까?

  위 호환성 문제가 없는 경우 적절한 권한이 없는 경우일 수 있습니다. 시스템 관리자에게 문의하십시오.

시스템 관리자

본인이 관리자이고 IAM 사용자가 지원되는 구성을 사용 중인데도 U2F 보안 키를 활성화할 수 없다면 그 사용자에게 적절한 권한이 있는지 확인하십시오. 자세한 예제는 자습서: 사용자들이 자신의 자격 증명 및 MFA 설정을 구성할 수 있도록 하기 (p. 55) 단원을 참조하십시오.

U2F 보안 키를 사용해 로그인할 수 없습니다.

IAM 사용자인데 U2F를 사용해서 AWS Management 콘솔에 로그인할 수 없는 경우 먼저 U2F 보안 키 사용에 지원되는 구성 (p. 129)을 확인하십시오. 지원되는 구성을 사용하는데 로그인이 안 되면 시스템 관리자에게 연락해 도움을 받으십시오.

U2F 키를 분실했거나 고장 났습니다.

한 사용자에게는 한 번에 하나의 MFA 디바이스(가상, U2F 보안 키 또는 하드웨어)만 할당됩니다. U2F 보안 키의 교체는 하드웨어 MFA 디바이스의 교체와 비슷합니다. 어떤 유형의 MFA 디바이스를 분실했거나 고장 난 경우 해결 방법은 MFA 디바이스 분실 또는 작동 중단 시 문제 해결 (p. 144)을 참조하십시오.

기타 문제

여기에 나오지 않은 U2F 보안 키의 문제는 다음 중 하나를 수행해 보십시오.

- IAM 사용자: 시스템 관리자에게 문의하십시오.
- AWS 계정 루트 사용자: AWS 지원에 문의하십시오.

IAM 역할 문제 해결

여기 정보를 사용하여 IAM 역할 작업 시 공통적으로 발생할 수 있는 문제를 진단 및 수정하십시오.

주제

역할을 위임할 수 없음

다음을 확인하십시오.

- 역할 이름은 대소문자를 구분하므로 역할 이름을 정확하게 사용하십시오.
- 해당 IAM 정책에서 사용자가 위임하려는 역할에 대해 `sts:AssumeRole`을 호출할 수 있는 권한을 부여하는지 확인하십시오. IAM 정책의 `Action` 요소는 `AssumeRole` 액션을 호출할 수 있어야 합니다. 또한 IAM 정책의 `Resource` 요소는 위임하려는 역할을 지정해야 합니다. 예를 들어 `Resource` 요소는 ARN(Amazon Resource Name) 또는 와일드카드(*)를 통해 역할을 지정할 수 있습니다. 예를 들어 사용자에게 적용되는 하나 이상의 정책은 다음과 유사한 권한을 부여해야 합니다.

```
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::account_id_number:role/role-name-you-want-to-assume"
```

- IAM 자격 증명에 IAM 정책에 필요한 태그가 있는지 확인하십시오. 예를 들어 다음 정책 권한에서 `Condition` 요소는 역할을 위임하도록 요청할 보안 주체에게 특정 태그가 있어야 한다는 것을 요구합니다. `department = HR` 또는 `department = CS` 태그가 지정되어 있어야 합니다. 그렇지 않으면 역할을 위임할 수 없습니다. IAM 사용자 및 역할 태그 지정에 대한 자세한 내용은 the section called “사용자 및 역할 태그 지정” (p. 290) 단원을 참조하십시오.

```
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "*",
    "Condition": {"StringEquals": {"aws:PrincipalTag/department": [
```

```
            "HR",
            "CS"
        ]}}
```

- 역할의 신뢰 정책에 지정된 모든 조건을 만족하고 있는지 확인하십시오. `Condition` 요소는 만료 날짜와 외부 ID를 지정하거나, 반드시 특정 IP 주소를 이용해야만 요청이 가능하도록 지정할 수 있습니다. 다음 예제를 고려하십시오. 현재 날짜가 지정된 날짜 이후의 시간이면 이 정책은 일치하지 않으며 해당 역할을 수임할 권한을 사용자에게 부여할 수 없습니다.

```
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::account_id_number:role/role-name-you-want-to-assume"
    "Condition": {
        "DateLessThan" : {
            "aws:CurrentTime" : "2016-05-01T12:00:00Z"
        }
    }
```

- `AssumeRole`을 호출하는 AWS 계정이 위임하려는 역할에 대해 신뢰할 수 있는 엔터티인지 확인하십시오. 신뢰할 수 있는 대상이라면 역할의 신뢰 정책에 `Principal`로 정의되어 있습니다. 다음은 수임할 역할에 연결된 신뢰 정책의 예입니다. 이 예에서 IAM 사용자가 로그인한 계정 ID는 123456789012여야 합니다. 계정 번호가 역할의 신뢰 정책의 `Principal` 요소에 명시되어 있지 않은 경우 해당 역할을 수임할 수 없습니다. 액세스 정책에서 어떤 권한이 부여되었는지는 중요하지 않습니다. 예제 정책은 2017년 7월 1일부터 2017년 12월 31일(UTC)까지 발생한 작업에 대한 권한을 제한합니다. 이 날짜 전이나 후에 로그인한 경우에는 정책이 일치하지 않기 때문에 해당 역할을 수행할 수 없습니다.

```
    "Effect": "Allow",
    "Principal": { "AWS": "arn:aws:iam::123456789012:root" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "DateGreaterThan": {"aws:CurrentTime": "2017-07-01T00:00:00Z"},
      "DateLessThan": {"aws:CurrentTime": "2017-12-31T23:59:59Z"}
    }
```

내 AWS 계정에 표시되는 새 역할

일부 AWS 서비스에서는 해당 서비스에 직접 연결된 고유한 유형의 서비스 역할을 사용해야 합니다. 이 서비스 연결 역할 (p. 175)은 해당 서비스에서 사전 정의하며 해당 서비스에 필요한 모든 권한을 포함합니다. 필요한 권한을 수동으로 추가할 필요가 없으므로 서비스를 더 쉽게 설정할 수 있습니다. 서비스 연결 역할에 대한 일반적인 내용은 서비스 연결 역할 사용 (p. 218) 단원을 참조하십시오.

서비스 연결 역할을 지원하려 할 때 이미 서비스를 사용 중일 수 있습니다. 그런 경우 계정의 새 역할에 대해 알리는 이메일을 받을 수 있습니다. 이 역할에는 서비스에서 사용자를 대신하여 작업을 수행하는 데 필요한 모든 권한이 포함되어 있습니다. 따라서 이 역할을 지원하기 위해 별도의 조치를 취할 필요가 없습니다. 그러나 계정에서 역할을 삭제하면 안 됩니다. 그렇게 하면 서비스가 AWS 리소스에 액세스하는 데 필요한 권한을 제거할 수 있습니다. IAM 콘솔의 IAM 역할 페이지에서 계정의 서비스 연결 역할을 볼 수 있습니다. 서비스 연결 역할은 테이블의 Trusted entities(신뢰할 수 있는 개체) 열에 (Service-linked role)((서비스 연결 역할))로 표시됩니다.

서비스 연결 역할을 지원하는 서비스에 대한 자세한 내용은 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 서비스의 서비스 연결 역할 사용에 대한 정보를 보려면 예]링크를 선택합니다.

AWS 계정에서 역할을 편집하거나 삭제할 수 없음

IAM에서 서비스 연결 역할 (p. 175)에 대한 권한을 삭제하거나 편집할 수 없습니다. 이러한 역할에는 사용자 대신 작업을 수행하기 위해 서비스에 필요한 신뢰 및 권한이 미리 지정되어 포함됩니다. IAM 콘솔, AWS CLI,

API 등을 사용하여 서비스 연결 역할의 설명만 편집할 수 있습니다. 콘솔의 IAM 역할 페이지에서 계정의 서비스 연결 역할을 볼 수 있습니다. 서비스 연결 역할은 테이블의 신뢰할 수 있는 개체(Trusted entities) 열에 (서비스 연결 역할)((Service-linked role))로 표시됩니다. 역할의 요약 페이지 배너에도 해당 역할이 서비스 역할임이 표시됩니다. 이러한 역할은 해당 서비스가 관리 및 삭제 작업을 지원할 경우 연결 서비스를 통해서만 관리하고 삭제할 수 있습니다. 서비스 연결 역할을 수정하거나 삭제하면 서비스에서 AWS 리소스에 액세스하는 데 필요한 권한이 제거될 수 있으므로 주의하십시오.

서비스 연결 역할을 지원하는 서비스에 대한 자세한 내용은 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다.

iam:PassRole을 수행하도록 인증되지 않음

서비스 연결 역할을 생성하는 경우 해당 역할을 서비스에 전달할 권한이 있어야 합니다. 일부 서비스는 서비스에서 작업을 수행할 때 계정에 서비스 연결 역할을 자동으로 생성합니다. 예를 들어 Amazon EC2 Auto Scaling에서는 사용자가 Auto Scaling 그룹을 처음으로 생성할 때 사용자를 대신해 `AWSServiceRoleForAutoScaling` 서비스 연결 역할을 생성합니다. `PassRole` 권한 없이 Auto Scaling 그룹을 생성하려고 하면 다음 오류가 발생합니다.

```
ClientError: An error occurred (AccessDenied) when calling the
PutLifecycleHook operation: User: arn:aws:sts::111122223333:assumed-role/
Testrole/Diego is not authorized to perform: iam:PassRole on resource:
arn:aws:iam::111122223333:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling
```

이 오류를 해결하려면 관리자에게 `iam:PassRole` 권한을 추가해 달라고 요청합니다.

서비스 연결 역할을 지원하는 서비스를 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 서비스가 자동으로 서비스 연결 역할을 생성하는지 여부를 알아보려면 예 링크를 선택하여 해당 서비스의 서비스 연결 역할 설명서 단원을 참조하십시오.

12시간 길이 세션을 선택한 경우 역할을 위임할 수 없는 이유(AWS CLI, AWS API)

AWS STS `AssumeRole*` API 또는 `assume-role*` CLI 작업을 사용하여 역할을 위임하는 경우 `DurationSeconds` 파라미터에 대한 값을 지정할 수 있습니다. 이 값의 범위는 900초(15분)에서 해당 역할에 대한 최대 CLI/API 세션 기간 설정까지 지정할 수 있습니다. 이 설정보다 높게 값을 지정하면 작업에 실패합니다. 이 설정의 최댓값은 12시간입니다. 예를 들어 세션 기간으로 12시간을 지정했는데 관리자가 최대 세션 기간으로 6시간을 설정하면 작업에 실패합니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오.

역할 함께 묶기 (p. 176)(역할을 사용하여 두 번째 역할 위임)를 사용하는 경우 세션은 최대 1시간으로 제한됩니다. 그런 다음 `DurationSeconds` 파라미터를 사용하여 1시간보다 큰 값을 입력하면 이 작업에 실패합니다.

역할에 작업 수행을 허용하는 정책이 있지만 “액세스 거부”가 표시됩니다.

역할 세션이 세션 정책에 의해 제한되었을 수 있습니다. AWS STS 사용을 통해 프로그래밍 방식으로 임시 보안 자격 증명을 요청 (p. 304)한 경우 인라인 또는 관리형 세션 정책 (p. 351)을 전달할 수 있습니다. 세션 정책은 역할 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. `Policy` 파라미터를 사용하여 단일 JSON 인라인 세션 정책 문서를 전달할 수 있습니다. `PolicyArns` 파라미터를 사용하여 최대 10개까지 관리형 세션 정책을 지정할 수 있습니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 자격 증명 기반 정책의 교집합과 세션 정책입니다. 또는 관리자 또는 사용자 프로그램에서 임시 자격 증명을 제공한 경우 세션 정책에 포함되어 액세스를 제한했을 수 있습니다.

Amazon EC2 및 IAM 문제 해결

이 문서의 정보를 사용하여 Amazon EC2 및 IAM 작업 시 발생할 수 있는 액세스 거부 또는 기타 문제를 해결할 수 있습니다.

주제

인스턴스를 시작하려고 할 때 Amazon EC2 콘솔 IAM 역할 목록에서 보여야 할 역할이 보이지 않습니다.

다음을 확인하십시오.

- IAM 사용자로 로그인한 경우, `ListInstanceProfiles`를 호출할 권한이 있는지 확인하십시오. 역할 사용 시 필요한 권한에 대한 자세한 내용은 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265)의 "Amazon EC2로 역할을 사용하는 데 필요한 권한"을 참조하십시오. 사용자에게 권한을 추가하는 방법에 대한 자세한 내용은 IAM 정책 관리 (p. 435)을 참조하십시오.

  권한을 수정할 수 없는 경우, IAM을 사용할 수 있는 관리자에게 문의하여 권한을 업데이트해야 합니다.
- IAM CLI 또는 API를 사용하여 역할을 만든 경우, 인스턴스 프로파일을 만들고 이 인스턴스 프로파일에 해당 역할을 추가했는지 확인하십시오. 또한 역할과 인스턴스 프로필의 이름을 다르게 설정한 경우, Amazon EC2 콘솔의 IAM 역할 목록에서 올바른 역할 이름을 볼 수 없습니다. Amazon EC2 콘솔의 IAM 역할 목록에는 역할 이름이 아니라 인스턴스 프로필 이름이 나열되어 있습니다. 원하는 역할을 포함한 인스턴스 프로필 이름을 선택해야 합니다. 인스턴스 프로파일에 대한 자세한 내용은 인스턴스 프로파일 사용 (p. 271)을 참조하십시오.

  > **Note**
  >
  > IAM 콘솔을 사용하여 역할을 만드는 경우, 인스턴스 프로파일을 사용하지 않아도 됩니다. 인스턴스 프로파일은 IAM 콘솔에서 만드는 각 역할과 동일한 이름으로 생성되며, 역할은 해당 인스턴스 프로파일에 자동으로 추가됩니다. 하나의 인스턴스 프로파일은 하나의 IAM 역할만 포함할 수 있으며 이 제한은 늘릴 수 없습니다.

제 인스턴스에 있는 자격 증명의 역할이 잘못되었습니다.

인스턴스 프로파일의 역할이 최근에 교체되었을 수 있습니다. 그러한 경우 다음에 예정된 자동 자격 증명 교체 이후에 역할의 자격 증명을 사용할 수 있습니다.

`AddRoleToInstanceProfile`을 호출하려고 하면 `AccessDenied` 오류가 발생합니다.

IAM 사용자로 요청을 하는 경우, 다음과 같은 권한이 있는지 확인하십시오.

- 인스턴스 프로파일 ARN과 일치하는 리소스가 포함된 `iam:AddRoleToInstanceProfile`(예: `arn:aws:iam::999999999999:instance-profile/ExampleInstanceProfile`).

역할 사용에 필요한 권한에 대한 자세한 내용은 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265)의 "어떻게 시작할 수 있습니까?"를 참조하십시오. 사용자에게 권한을 추가하는 방법에 대한 자세한 내용은 IAM 정책 관리 (p. 435) 단원을 참조하십시오.

Amazon EC2: 역할로 인스턴스를 시작하려고 하면 AccessDenied 오류가 발생합니다.

다음을 확인하십시오.

- 인스턴스 프로필 없이 인스턴스를 시작합니다. 이를 통해 문제가 Amazon EC2 인스턴스의 IAM 역할로 제한되어 있는지 확인할 수 있습니다.
- IAM 사용자로 요청을 하는 경우, 다음과 같은 권한이 있는지 확인하십시오.
  - 와일드카드 리소스("*")가 포함된 `ec2:RunInstances`
  - 역할 ARN과 일치하는 리소스가 포함된 `iam:PassRole`(예: `arn:aws:iam::999999999999:role/ExampleRoleName`)
- IAM `GetInstanceProfile` 작업을 호출하여 올바른 인스턴스 프로필 이름 또는 올바른 인스턴스 프로필 ARN을 사용 중인지 확인하십시오. 자세한 내용은 Amazon EC2 인스턴스로 IAM 역할 사용 단원을 참조하십시오.
- IAM `GetInstanceProfile` 작업을 호출하여 인스턴스 프로필에 역할이 있는지 확인하십시오. 인스턴스 프로파일이 비어 있으면 `AccessDenied` 오류가 발생합니다. 역할 만들기에 대한 자세한 내용은 IAM 역할 생성 (p. 225) 단원을 참조하십시오.

역할 사용에 필요한 권한에 대한 자세한 내용은 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265)의 "어떻게 시작할 수 있습니까?"를 참조하십시오. 사용자에게 권한을 추가하는 방법에 대한 자세한 내용은 IAM 정책 관리 (p. 435) 단원을 참조하십시오.

제 EC2 인스턴스의 임시 보안 자격 증명에 액세스할 수 없습니다.

EC2 인스턴스에서 임시 보안 자격 증명에 액세스하려면 먼저 IAM 콘솔을 사용하여 역할을 생성해야 합니다. 그런 다음 해당 역할을 사용하는 EC2 인스턴스를 시작하고 실행 중인 인스턴스를 검사합니다. 자세한 내용은 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265)의 어떻게 시작합니까?를 참조하십시오.

그래도 EC2 인스턴스에서 임시 보안 자격 증명에 액세스할 수 없는 경우 다음을 확인하십시오.

- Instance Metadata Service(IMDS)의 다른 부분에는 액세스할 수 있습니까? 액세스할 수 없는 경우 IMDS로의 요청에 대한 액세스를 차단하는 방화벽 규칙이 없는지 확인하십시오.

```
[ec2-user@domU-12-31-39-0A-8D-DE ~]$ GET http://169.254.169.254/latest/meta-data/
hostname; echo
```

- IMDS의 `iam` 하위 트리가 있습니까? 그렇지 않은 경우 EC2 `DescribeInstances` API 작업을 호출하거나 aws ec2 `describe-instances` CLI 명령을 사용하여 인스턴스에 IAM 인스턴스 프로필이 연결되어 있는지 확인합니다.

```
[ec2-user@domU-12-31-39-0A-8D-DE ~]$ GET http://169.254.169.254/latest/meta-data/iam;
 echo
```

- 오류가 있는지 IAM 하위 트리의 info 문서를 확인하십시오. 오류가 있는 경우 자세한 내용은 IAM 하위 트리에서 info 문서의 오류란 무엇인가요? (p. 557) 단원을 참조하십시오.

```
[ec2-user@domU-12-31-39-0A-8D-DE ~]$ GET http://169.254.169.254/latest/meta-data/iam/
info; echo
```

IAM 하위 트리에서 info 문서의 오류란 무엇인가요?

iam/info 문서는 "Code":"InstanceProfileNotFound"를 나타냅니다.

IAM 인스턴스 프로필이 삭제되었으므로 Amazon EC2에서 더 이상 인스턴스에 자격 증명을 제공할 수 없습니다. Amazon EC2 인스턴스에 올바른 인스턴스 프로파일을 연결해야 합니다.

해당 이름의 인스턴스 프로파일이 있는 경우, 원래 인스턴스 프로파일이 삭제되고 동일한 이름의 다른 인스턴스가 생성된 것이 아닌지 확인하십시오.

1. IAM GetInstanceProfile 작업을 호출하여 InstanceProfileId를 가져옵니다.
2. Amazon EC2 DescribeInstances 작업을 호출하여 인스턴스의 IamInstanceProfileId를 가져옵니다.
3. IAM 작업의 InstanceProfileId와 Amazon EC2 작업의 IamInstanceProfileId가 일치하는지 확인합니다.

ID가 다르면 인스턴스에 연결된 인스턴스 프로파일이 더 이상 유효하지 않습니다. 인스턴스에 올바른 인스턴스 프로파일을 연결해야 합니다.

iam/info 문서는 성공을 나타내지만 "Message":"Instance Profile does not contain a role..."을 나타냅니다.

역할이 IAM RemoveRoleFromInstanceProfile 작업에 의해 인스턴스 프로필에서 제거되었습니다. IAM AddRoleToInstanceProfile 작업을 사용하여 인스턴스 프로필에 역할을 연결할 수 있습니다. 역할의 자격 증명에 액세스하려면 다음에 예정된 새로 고침까지 기다려야 합니다.

iam/security-credentials/[role-name] 문서는 "Code":"AssumeRoleUnauthorizedAccess"를 나타냅니다.

Amazon EC2에는 역할을 위임할 권한이 없습니다. 다음 예와 같이 역할을 수임할 권한은 해당 역할에 연결된 신뢰 정책에서 관리합니다. IAM UpdateAssumeRolePolicy API를 사용하여 신뢰 정책을 업데이트합니다.

```
{"Version": "2012-10-17","Statement": [{"Effect": "Allow","Principal": {"Service":
 ["ec2.amazonaws.com"]},"Action": ["sts:AssumeRole"]}]}
```

역할의 자격 증명에 액세스하려면 다음에 예정된 자동 새로 고침까지 기다려야 합니다.

Amazon S3 및 IAM 문제 해결

이 문서의 정보를 사용하여 Amazon S3 및 IAM 작업 시 발생할 수 있는 문제를 해결하십시오.

Amazon S3 버킷에 대한 익명 액세스 권한을 부여하는 방법은 무엇입니까?

`principal` 요소에 와일드카드(*)를 지정하는 Amazon S3 버킷 정책을 사용합니다. 이는 누구나 버킷에 액세스할 수 있다는 의미입니다. 익명 액세스를 통하면 누구나(AWS 계정이 없는 사용자 포함) 버킷에 액세스할 수 있게 됩니다. 샘플 정책은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 버킷 정책 사례를 참조하십시오.

AWS 계정의 루트 사용자로 로그인했는데 내 계정으로 Amazon S3 버킷에 액세스할 수 없는 이유가 무엇입니까?

IAM 및 Amazon S3에 대해 모든 권한을 가진 IAM 사용자가 있기도 합니다. IAM 사용자가 Amazon S3 버킷에 버킷 정책을 할당하고 AWS 계정 루트 사용자를 보안 주체로 지정하지 않으면 루트 사용자의 버킷 액세스가 거부됩니다. 하지만 루트 사용자로 계속 버킷에 액세스할 수 있습니다. 이를 위해 버킷 정책을 수정하여 Amazon S3 콘솔 또는 AWS CLI에서 루트 사용자 액세스를 허용합니다.

AWS로 SAML 2.0 연동 문제 해결

이 문서의 정보를 사용하여 IAM 연동 및 SAML 2.0 작업 시 발생할 수 있는 문제를 진단하고 해결할 수 있습니다.

주제

오류: 요청에 잘못된 SAML 응답이 포함되어 있습니다. 로그아웃하려면 여기를 클릭하십시오.

이 오류는 자격 증명 공급자의 SAML 응답에 `Name`이 `https://aws.amazon.com/SAML/Attributes/Role`로 설정된 속성이 포함되지 않은 경우 발생할 수 있습니다. 이 속성은 하나 이상의 `AttributeValue` 요소를 포함해야 하며, 각 요소에 다음과 같은 문자열 쌍이 쉼표로 구분되어 있어야 합니다.

- 사용자를 매핑할 수 있는 역할의 ARN

- SAML 공급자의 ARN

자세한 내용은 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오. 브라우저에서 SAML 응답을 보려면 문제 해결을 위해 브라우저에서 SAML 응답을 보는 방법 (p. 561)의 단계를 따르십시오.

오류: AuthnResponse에 RoleSessionName 필요(서비스: AWSSecurityTokenService, 상태 코드: 400, 오류 코드: InvalidIdentityToken)

이 오류는 자격 증명 공급자의 SAML 응답에 `Name`이 `https://aws.amazon.com/SAML/Attributes/RoleSessionName`로 설정된 속성이 포함되지 않은 경우 발생할 수 있습니다. 속성 값은 사용자의 식별자이며, 일반적으로 사용자 ID 또는 이메일 주소입니다.

자세한 내용은 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오. 브라우저에서 SAML 응답을 보려면 문제 해결을 위해 브라우저에서 SAML 응답을 보는 방법 (p. 561)의 단계를 따르십시오.

오류: sts:AssumeRoleWithSAML을 수행할 권한 없음(서비스: AWSSecurityTokenService, 상태 코드: 403, 오류 코드: AccessDenied)

이 오류는 SAML 응답에 지정된 IAM 역할이 잘못 기재되었거나 존재하지 않는 경우 발생할 수 있습니다. 역할 이름은 대소문자를 구분하므로 역할 이름을 정확하게 사용하십시오. SAML 서비스 공급자 구성의 역할 이름을 올바르게 수정하십시오.

역할 신뢰 정책에 `sts:AssumeRoleWithSAML` 작업이 포함된 경우에만 액세스가 허용됩니다. `PrincipalTag` 속성 (p. 206)을 사용하도록 SAML 어설션이 구성된 경우 신뢰 정책에도 `sts:TagSession` 작업이 포함되어야 합니다. 세션 태그에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

이 오류는 연동 사용자가 역할을 수임할 권한이 없는 경우에도 발생할 수 있습니다. 역할에는 IAM SAML 자격 증명 공급자의 ARN을 `Principal`로 지정하는 신뢰 정책이 있어야 합니다. 또한 역할에는 어떤 사용자가 해당 역할을 수임할 수 있는지 제어하는 조건이 포함됩니다. 사용자는 조건의 요구 사항을 준수해야 합니다.

이 오류는 SAML 응답에 `Subject`가 포함된 `NameID`가 없는 경우에도 발생할 수 있습니다.

자세한 내용은 Establish Permissions in AWS for Federated Users 및 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오. 브라우저에서 SAML 응답을 보려면 문제 해결을 위해 브라우저에서 SAML 응답을 보는 방법 (p. 561)의 단계를 따르십시오.

오류: AuthnResponse의 RoleSessionName은 [a-zA-Z_0-9+=,.@-]{2,64}와 일치해야 함(서비스: AWSSecurityTokenService, 상태 코드: 400, 오류 코드: InvalidIdentityToken)

이 오류는 `RoleSessionName` 속성 값이 너무 길거나 유효하지 않은 문자가 포함된 경우 발생할 수 있습니다. 유효한 최대 길이는 64자입니다.

자세한 내용은 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오. 브라우저에서 SAML 응답을 보려면 문제 해결을 위해 브라우저에서 SAML 응답을 보는 방법 (p. 561)의 단계를 따르십시오.

오류: 유효하지 않은 응답 서명(서비스: AWSSecurityTokenService, 상태 코드: 400, 오류 코드: InvalidIdentityToken)

이 오류는 자격 증명 공급자의 연동 메타데이터가 IAM 자격 증명 공급자의 메타데이터와 일치하지 않는 경우 발생할 수 있습니다. 예를 들어, 만료된 인증서를 업데이트하기 위해 자격 증명 서비스 공급자의 메타데이터 파일이 변경되었을 수 있습니다. 이 경우, 자격 증명 서비스 공급자의 업데이트된 SAML 메타데이터 파일을 다운로드합니다. 그런 다음 `aws iam update-saml-provider` 크로스플랫폼 CLI 명령 또는 `Update-IAMSAMLProvider` PowerShell cmdlet을 통해 IAM에서 정의한 AWS 자격 증명 공급자 엔터티에 이를 업데이트합니다.

오류: 역할을 수임하지 못함: 지정한 공급자에 발행자가 없음(서비스: AWSOpenIdDiscoveryService, 상태 코드: 400, 오류 코드: AuthSamlInvalidSamlResponseException)

이 오류는 업로드한 연동 메타데이터 파일에 선언되어 있는 발행자와 SAML 응답의 발행자가 일치하지 않는 경우 발생할 수 있습니다. 메타데이터 파일은 IAM에서 자격 증명 공급자를 생성할 때 AWS에 업로드되었습니다.

오류: 메타데이터를 구문 분석할 수 없습니다.

이 오류는 메타데이터 파일이 적절한 형식이 아닌 경우에 발생할 수 있습니다.

AWS Management 콘솔에서 SAML 자격 증명 공급자를 생성하거나 관리할 때 (p. 199), 사용자의 자격 증명 공급자에서 SAML 메타데이터 문서를 가져와야 합니다. 이 메타데이터 파일에는 발급자 이름, 만료 정보 및 IdP에서 가져온 SAML 인증 응답(어설션)을 확인하는 데 사용할 수 있는 키가 포함되어 있습니다. 메타데이터 파일은 바이트 순서 표시(BOM)가 없는 UTF-8 형식으로 인코딩되어야 합니다. 또한 SAML 메타데이터 문서의 일부로 포함된 x.509 인증서는 1,024비트 이상의 키를 사용해야 합니다. 키 크기가 이보다 작으면 "메타데이터를 구문 분석할 수 없음" 오류로 인해 IdP 생성에 실패합니다. BOM을 제거하려면 Notepad++와 같은 텍스트 편집 도구를 사용해 파일을 UTF-8로 인코딩합니다.

오류: 지정된 공급자가 존재하지 않습니다.

이 오류는 SAML 어설션에서 지정한 공급자의 이름이 IAM에 구성된 공급자의 이름과 일치하지 않는 경우 발생할 수 있습니다. 공급자 이름 보기에 대한 자세한 내용은 IAM SAML 자격 증명 공급자 생성 (p. 198) 단원을 참조하십시오.

오류: 요청된 DurationSeconds가 이 역할에 대해 설정된 MaxSessionDuration을 초과합니다.

이 오류는 AWS CLI 또는 API에서 역할을 위임한 경우 발생할 수 있습니다.

assume-role-with-saml CLI 또는 AssumeRoleWithSAML API 작업을 사용하여 역할을 위임하는 경우 `DurationSeconds` 파라미터의 값을 지정할 수 있습니다. 이 값의 범위는 900초(15분)에서 해당 역할에 대한 최대 세션 기간 설정까지 지정할 수 있습니다. 이 설정보다 높게 값을 지정하면 작업에 실패합니다. 예를 들어 세션 기간으로 12시간을 지정했는데 관리자가 최대 세션 기간으로 6시간을 설정하면 작업에 실패합니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오.

문제 해결을 위해 브라우저에서 SAML 응답을 보는 방법

다음 절차는 SAML 2.0 관련 문제를 해결할 경우 브라우저에서 서비스 공급자로부터의 SAML 응답을 보는 방법을 설명합니다.

브라우저에서 문제를 재현할 수 있는 페이지로 이동합니다. 그런 다음 해당 브라우저의 단계를 따릅니다.

주제

Google Chrome

Chrome에서 SAML 응답을 보려면

이 단계는 54.0.2840.87m 버전을 사용하여 테스트했습니다. 다른 버전을 사용할 경우 그에 맞게 단계를 적용해야 할 수 있습니다.

1. F12를 눌러 개발자 콘솔을 시작합니다.
2. 네트워크 탭을 선택한 후 로그 보관(Preserve log)을 선택합니다.
3. 문제를 재현합니다.
4. 개발자 콘솔 창에서 SAML 게시물(SAML Post)을 확인합니다. 해당 행을 선택하고 하단에서 헤더(Headers) 탭을 봅니다. 인코딩된 요청을 포함하는 SAMLResponse 속성을 확인합니다.

Mozilla Firefox

Firefox에서 SAML 응답을 보려면

이 절차는 37.0.2 of Mozilla Firefox에서 테스트했습니다. 다른 버전을 사용할 경우 그에 맞게 단계를 적용해야 할 수 있습니다.

1. F12를 눌러 개발자 콘솔을 시작합니다.
2. 개발자 콘솔 창 상단 오른쪽에서 옵션(작은 기어 모양 아이콘)을 클릭합니다. 공통 기본 설정(Common Preferences)에서 지속적 로그 활성화(Enable persistent logs)를 선택합니다.
3. 네트워크 탭을 선택합니다.
4. 문제를 재현합니다.
5. 테이블에서 POST SAML을 확인합니다. 해당 행을 선택합니다. 오른쪽의 양식 데이터(Form Data) 창에서 Params 탭을 선택하고 SAMLResponse 요소를 확인합니다.

Apple Safari

Safari에서 SAML 응답을 보려면

이 단계는 8.0.6(10600.6.3) 버전을 사용하여 테스트했습니다. 다른 버전을 사용할 경우 그에 맞게 단계를 적용해야 할 수 있습니다.

1. Safari에서 Web Inspector를 사용하도록 설정합니다. 기본 설정 창을 열고 고급 탭을 선택한 후 메뉴 표시줄에 Develop 메뉴 표시(Show Develop menu in the menu bar)를 선택합니다.
2. 이제 Web Inspector를 열 수 있습니다. Develop을 클릭한 후 웹 검사기 표시(Show Web Inspector)를 선택합니다.
3. 리소스 탭을 선택합니다.
4. 문제를 재현합니다.
5. saml-signin.aws.amazon.com 요청을 찾습니다.
6. 아래로 스크롤하여 `Request Data`라는 `SAMLResponse`를 확인합니다. 연결된 값은 Base64 인코딩 응답입니다.

Microsoft Internet Explorer

Internet Explorer에서 SAML 응답을 보려면

Internet Explorer의 네트워크 트래픽을 분석하는 가장 좋은 방법은 타사 도구를 사용하는 것입니다.

- http://social.technet.microsoft.com/wiki/contents/articles/3286.ad-fs-2-0-how-to-use-fiddler-web-debugger-to-analyze-a-ws-federation-passive-sign-in.aspx의 단계에 따라 Fiddler를 다운로드하여 설치한 후 데이터를 수집하십시오.

Base64 인코딩 SAML 응답에 대해 해야 할 작업

브라우저에서 Base64 인코딩 SAML 응답 요소를 확인했으면 복사한 후 Base-64 디코딩 도구에서 사용하여 XML 태그 응답을 추출합니다.

> 보안 팁
>
> 표시되는 SAML 응답 데이터에는 중요한 보안 데이터가 포함되어 있을 수 있으므로 온라인 base64 디코더를 사용하지 않을 것을 권장합니다. 대신 로컬 컴퓨터에 설치된 도구를 사용하십시오. 로컬 컴퓨터에 설치된 도구는 네트워크를 통해 SAML 데이터를 전송하지 않습니다.

Windows 시스템용 내장 옵션(PowerShell):

```
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("base64encodedtext"))
```

MacOS 및 Linux 시스템용 내장 옵션:

```
$ echo "base64encodedtext" | base64 --decode
```

AWS Identity and Access Management에 대한 참조 정보

이 단원의 주제를 통해 IAM 및 AWS STS의 다양한 측면에 대한 자세한 참조 자료를 찾아보십시오.

주제

IAM 식별자

IAM은(는) 사용자, 그룹, 역할, 정책 및 서버 인증서에 대해 몇 가지 다른 식별자를 사용합니다. 이 단원에서는 그러한 식별자와 각 식별자를 사용하는 경우를 설명합니다.

주제

표시 이름 및 경로

사용자, 역할, 그룹 또는 정책을 만들거나 서버 인증서를 업로드할 때 표시 이름을 지정합니다. 예를 들면 Bob, TestApp1, Developers, ManageCredentialsPermissions 또는 ProdServerCert입니다.

IAM API 또는 AWS Command Line Interface(AWS CLI)를 사용하여 IAM 엔터티를 생성하는 경우, 해당 엔터티에 선택적 경로를 부여할 수도 있습니다. 하나의 경로를 사용하거나, 하나의 폴더 구조인 것처럼 여러 경로를 중첩할 수 있습니다. 예를 들면 중첩된 경로 `/division_abc/subdivision_xyz/product_1234/engineering/`를 사용하여 귀하 회사의 조직 구조를 일치시킬 수 있습니다. 그런 다음 정책을 생성하여 그 경로의 모든 사용자가 정책 시뮬레이터 API에 액세스할 수 있도록 허용할 수 있습니다. 정책을 보려면 IAM: 사용자 경로를 바탕으로 정책 시뮬레이터 API 액세스 (p. 422) 단원을 참조하십시오. 경로를 사용하는 방법의 추가 예제는 IAM ARN (p. 564) 단원을 참조하십시오.

AWS CloudFormation을 사용하여 리소스를 생성할 때 사용자, 그룹 및 역할에 대한 경로를 지정할 수 있지만 정책은 지정할 수 없습니다.

어떤 사용자 및 그룹에 동일한 경로를 부여했다고 해서 해당 사용자가 그룹에 자동으로 추가되지는 않습니다. 예를 들어, Developers 그룹을 생성하고 이 그룹의 경로를 /division_abc/subdivision_xyz/product_1234/engineering/으로 지정할 수 있습니다. Bob이라는 사용자를 만들고 그에게 동일한 경로를 부여했다고 해서 Bob이 Developers 그룹에 자동으로 추가되지는 않습니다. IAM는 경로를 기반으로 사용자 또는 그룹 간에 경계를 적용하지 않습니다 경로가 다른 사용자가 (해당 리소스에 대한 권한이 있다는 가정하에) 동일한 리소스를 사용할 수 있습니다. 이름의 제한 사항에 대한 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오.

IAM ARN

대부분의 리소스에는 표시 이름이 있습니다(예를 들어, `Bob`이라는 사용자 또는 `Developers`라는 그룹). 그러나 권한 정책 언어에는 다음과 같은 Amazon 리소스 이름(ARN) 형식을 사용하여 하나 이상의 리소스를 지정해야 합니다.

```
arn:partition:service:region:account:resource
```

여기서 각 항목은 다음과 같습니다.

- `partition`은 리소스가 위치하는 파티션을 식별합니다. 표준 AWS 리전에서 파티션은 `aws`입니다. 리소스가 다른 파티션에 있는 경우 파티션은 `aws-partitionname`입니다. 예를 들어 중국(베이징) 리전에 있는 리소스의 파티션은 `aws-cn`입니다. 다른 파티션의 계정 간에 액세스 권한을 위임 (p. 288)할 수 없습니다.
- `service`에서는 AWS 제품을 식별합니다. IAM 리소스의 경우 항상 `iam`입니다.
- `region`은 리소스가 상주하는 리전입니다. IAM 리소스의 경우 항상 공백입니다.
- `account`는 AWS 계정 ID이며 하이픈은 제외합니다(예: 123456789012).
- `resource`는 특정 리소스를 이름으로 식별하는 부분입니다.

다음 구문을 사용하여 IAM 및 AWS STS ARN을 지정할 수 있습니다. IAM 리소스가 글로벌이기 때문에 ARN의 리전 부분은 공백입니다.

구문:

```
arn:aws:iam::account-id:root
arn:aws:iam::account-id:user/user-name-with-path
arn:aws:iam::account-id:group/group-name-with-path
arn:aws:iam::account-id:role/role-name-with-path
arn:aws:iam::account-id:policy/policy-name-with-path
arn:aws:iam::account-id:instance-profile/instance-profile-name-with-path
arn:aws:sts::account-id:federated-user/user-name
arn:aws:sts::account-id:assumed-role/role-name/role-session-name
arn:aws:iam::account-id:mfa/virtual-device-name-with-path
arn:aws:iam::account-id:u2f/u2f-token-id
arn:aws:iam::account-id:server-certificate/certificate-name-with-path
arn:aws:iam::account-id:saml-provider/provider-name
arn:aws:iam::account-id:oidc-provider/provider-name
```

다음과 같은 많은 예에는 ARN의 리소스 부분에 경로가 포함됩니다. AWS Management 콘솔에서는 경로를 생성하거나 조작할 수 없습니다. 경로를 사용하려면 AWS API나 AWS CLI 또는 Windows PowerShell용 도구을(를) 사용하여 리소스 작업을 해야 합니다.

예제:

```
arn:aws:iam::123456789012:root
arn:aws:iam::123456789012:user/JohnDoe
arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/JaneDoe
arn:aws:iam::123456789012:group/Developers
arn:aws:iam::123456789012:group/division_abc/subdivision_xyz/product_A/Developers
arn:aws:iam::123456789012:role/S3Access
arn:aws:iam::123456789012:role/application_abc/component_xyz/S3Access
arn:aws:iam::123456789012:policy/UsersManageOwnCredentials
arn:aws:iam::123456789012:policy/division_abc/subdivision_xyz/UsersManageOwnCredentials
arn:aws:iam::123456789012:instance-profile/Webserver
arn:aws:sts::123456789012:federated-user/JohnDoe
arn:aws:sts::123456789012:assumed-role/Accounting-Role/JaneDoe
arn:aws:iam::123456789012:mfa/JaneDoeMFA
```

```
arn:aws:iam::123456789012:u2f/user/JohnDoe/default (U2F security key)
arn:aws:iam::123456789012:server-certificate/ProdServerCert
arn:aws:iam::123456789012:server-certificate/division_abc/subdivision_xyz/ProdServerCert
arn:aws:iam::123456789012:saml-provider/ADFSProvider
arn:aws:iam::123456789012:oidc-provider/GoogleProvider
```

다음 예제에서는 다양한 유형의 IAM 및 AWS STS 리소스에 대한 ARN 형식을 이해하는 데 도움이 되는 자세한 정보를 제공합니다.

- 계정의 IAM 사용자:

```
arn:aws:iam::123456789012:user/JohnDoe
```

- 조직 차트를 반영하는 경로를 갖는 다른 사용자:

```
arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/JaneDoe
```

- IAM 그룹:

```
arn:aws:iam::123456789012:group/Developers
```

- 경로를 포함하는 IAM 그룹:

```
arn:aws:iam::123456789012:group/division_abc/subdivision_xyz/product_A/Developers
```

- IAM 역할:

```
arn:aws:iam::123456789012:role/S3Access
```

- 관리형 정책:

```
arn:aws:iam::123456789012:policy/ManageCredentialsPermissions
```

- EC2 인스턴스와 연결될 수 있는 인스턴스 프로파일:

```
arn:aws:iam::123456789012:instance-profile/Webserver
```

- IAM에서 "Paulo"로 식별되는 연동 사용자:

```
arn:aws:sts::123456789012:federated-user/Paulo
```

- 역할 세션 이름 'Mary'로 역할 'Accounting-Role'을 수임하는 누군가의 활성 세션:

```
arn:aws:sts::123456789012:assumed-role/Accounting-Role/Mary
```

- 사용자 이름 Jorge에 할당된 멀티 팩터 인증 디바이스:

```
arn:aws:iam::123456789012:mfa/Jorge
```

- 서버 인증서:

```
arn:aws:iam::123456789012:server-certificate/ProdServerCert
```

- 조직 차트를 반영하는 경로를 갖는 서버 인증서:

```
arn:aws:iam::123456789012:server-certificate/division_abc/subdivision_xyz/ProdServerCert
```

- 자격 증명 공급자(SAML 및 OIDC):

```
arn:aws:iam::123456789012:saml-provider/ADFSProvider
arn:aws:iam::123456789012:oidc-provider/GoogleProvider
```

또 다른 중요한 ARN은 루트 사용자 ARN입니다. IAM 리소스는 아니지만 이 ARN의 형식을 잘 알고 있어야 합니다. 이 ARN은 종종 정책의 `Principal` 요소 (p. 589)에 사용됩니다.

- AWS 계정 - 계정 자체:

```
arn:aws:iam::123456789012:root
```

다음 예제에서는 Richard가 자신의 액세스 키를 관리할 수 있도록 그에게 할당할 수 있는 정책을 보여줍니다. 리소스는 IAM 사용자 Richard입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageRichardAccessKeys",
            "Effect": "Allow",
            "Action": [
                "iam:*AccessKey*",
                "iam:GetUser"
            ],
            "Resource": "arn:aws:iam::*:user/division_abc/subdivision_xyz/Richard"
        },
        {
            "Sid": "ListForConsole",
            "Effect": "Allow",
            "Action": "iam:ListUsers",
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> ARN을 사용하여 IAM 정책의 리소스를 식별하는 경우 정책 변수를 포함할 수 있습니다. 정책 변수에는 ARN의 일부로 런타임 정보(예: 사용자 이름)에 대한 자리표시자가 포함될 수 있습니다. 자세한 내용은 IAM 정책 요소: 변수 및 태그 (p. 615) 단원을 참조하십시오.

ARN의 *###* 부분에 와일드카드를 사용하여 여러 사용자, 그룹 또는 정책을 지정할 수 있습니다. 예를 들어, product_1234를 작업하는 모든 사용자를 지정하려면 다음을 사용합니다.

```
arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/product_1234/*
```

이름이 `app_` 문자열로 시작하는 사용자가 여럿 있다고 가정해 봅시다. 다음과 같은 ARN을 사용하여 이들 모두를 언급할 수 있습니다.

```
arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/product_1234/app_*
```

AWS 계정의 모든 사용자, 그룹 또는 정책을 지정하려면, ARN의 `user/`, `group/` 또는 `policy` 부분 다음에 각각 와일드카드를 사용합니다.

```
arn:aws:iam::123456789012:user/*
```

```
arn:aws:iam::123456789012:group/*
arn:aws:iam::123456789012:policy/*
```

ARN의 `user/`, `group/` 또는 `policy` 부분에 와일드카드를 사용하지 마십시오. 예를 들어 다음은 허용되지 않습니다.

```
arn:aws:iam::123456789012:u*
```

Example 프로젝트 기반 그룹의 경로 및 ARN 사용

AWS Management 콘솔에서는 경로를 생성하거나 조작할 수 없습니다. 경로를 사용하려면 AWS API나 AWS CLI 또는 Windows PowerShell용 도구을(를) 사용하여 리소스 작업을 해야 합니다.

이 예제에서 Marketing_Admin 그룹의 Jules가 /marketing/ 경로에 프로젝트 기반 그룹을 생성합니다. Jules는 회사의 다른 파트에 있는 사용자를 해당 그룹에 할당합니다. 이 예는 사용자의 경로가 그가 속한 그룹과 관련되지 않는다는 점을 보여줍니다.

마케팅 그룹에는 이들이 출시할 신제품이 있으므로 Jules는 /marketing/ 경로에 Widget_Launch라는 새 그룹을 생성합니다. 그런 다음 Jules는 해당 그룹에 다음과 같은 정책을 할당합니다. 이 정책은 그룹에 이 특정 출시에 지정된 `example_bucket` 부분의 객체에 대한 액세스 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::example_bucket/marketing/newproductlaunch/widget/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket*",
      "Resource": "arn:aws:s3:::example_bucket",
      "Condition": {"StringLike": {"s3:prefix": "marketing/newproductlaunch/widget/*"}}
    }
  ]
}
```

그런 다음 Jules는 해당 그룹에 이 출시와 관련된 사용자를 할당합니다. 여기에는 /marketing/ 경로의 Patricia와 Eli가 포함됩니다. 또한 /sales/ 경로의 Chris와 Chloe, /legal/ 경로의 Alice와 Jim이 포함됩니다.

고유 식별자

IAM에서 사용자, 그룹, 역할, 정책, 인스턴스 프로파일 또는 서버 인증서를 생성할 때, 각 엔터티에 다음과 같은 고유 ID를 할당합니다.

```
AIDAJQABLZS4A3QDU576Q
```

대부분의 경우 IAM 엔터티로 작업할 때 표시 이름과 ARN (p. 564)을 사용합니다. 이렇게 하면 특정 엔터티의 고유 ID를 알아야 할 필요가 없습니다. 그러나 표시 이름을 사용하는 것이 적절치 않은 경우에는 고유 ID를 사용하는 것이 유용합니다.

한 예로써 AWS 계정에서 표시 이름을 재사용하는 경우를 살펴보겠습니다. 계정 내에서 사용자, 그룹 또는 정책의 표시 이름은 고유해야 합니다. 예를 들어, David라는 IAM 사용자를 생성할 수 있습니다. 회사에서 Amazon S3를 사용하고 있고 각 직원에 대한 폴더가 포함된 버킷이 있습니다. 이 버킷에는 사용자가 버킷에서 자신의 폴더에만 액세스할 수 있도록 리소스 기반 정책(버킷 정책)이 있습니다. David라는 직원이 퇴사하여 해당하는 IAM 사용자를 삭제한다고 가정해 봅시다. 그러나 이후 David라는 또 다른 직원이 입사하여 David라는 새 IAM 사용자를 생성합니다. 버킷 정책에서 `David` IAM 사용자를 지정하는 경우 이 정책은 새 David가 이전 David가 남긴 정보에 액세스할 수 있도록 허용합니다.

그러나 이전에 삭제한 표시 이름을 재사용하는 새 IAM 사용자를 생성한다 하더라도 모든 IAM 사용자는 고유 ID를 갖습니다. 이 예에서 이전 IAM 사용자 David와 새 IAM 사용자 David는 서로 다른 고유 ID를 갖습니다. 사용자 이름뿐만 아니라 고유 ID별로 액세스 권한을 부여하는 Amazon S3 버킷에 대한 리소스 정책을 생성할 수 있습니다. 이렇게 하면 직원에게 없어야 하는 정보에 대한 액세스 권한을 실수로 부여할 가능성이 줄어듭니다.

사용자 ID가 유용한 또 다른 예는 IAM 사용자 정보의 데이터베이스(또는 다른 저장소)를 유지하는 경우입니다. 고유 ID는 사용자가 생성하는 각 IAM 사용자에 대해 고유 식별자를 제공할 수 있습니다. 이전 예제에서와 같이 시간이 지남에 따라 이름을 재사용하는 IAM 사용자가 있는 경우에도 마찬가지입니다.

고유 ID 접두사에 대한 이해

IAM에서는 다음과 같은 접두사를 사용해 각 고유 ID가 적용되는 엔터티의 유형을 표시합니다.

접두사	엔터티 유형
AAGA	작업 그룹
ACCA	컨텍스트별 자격 증명
AGPA	그룹
AIDA	IAM user
AIPA	Amazon EC2 인스턴스 프로파일
AKIA	액세스 키
ANPA	관리형 정책
ANVA	관리 정책 내 버전
APKA	퍼블릭 키
AROA	역할
ASCA	Certificate
ASIA	임시(AWS STS) 키

고유 식별자 가져오기

IAM 엔터티의 고유 ID는 IAM 콘솔에서 제공되지 않습니다. 고유 ID를 가져오기 위해 다음과 같은 AWS CLI 명령 또는 IAM API 호출을 사용할 수 있습니다.

AWS CLI:

- get-caller-identity
- get-group
- get-role
- get-user
- get-policy
- get-instance-profile
- get-server-certificate

IAM API:

- GetCallerIdentity
- GetGroup
- GetRole
- GetUser
- GetPolicy
- GetInstanceProfile
- GetServerCertificate

IAM 및 STS 제한

AWS Identity and Access Management(IAM) 및 AWS Security Token Service(STS)의 객체에는 크기 제한이 있습니다. 또한 이러한 서비스는 객체의 이름을 지정하는 방법, 생성할 수 있는 객체 수 및 객체를 전달할 때 사용할 수 있는 문자 수를 제한합니다.

> Note
>
> IAM 사용량 및 할당량에 관한 계정 수준 정보를 가져오려면 GetAccountSummary API 작업 또는 get-account-summary AWS CLI 명령을 사용합니다.

IAM 이름 제한

다음은 IAM 이름에 대한 제한 사항입니다.

- 정책 설명서에는 수평 탭(U+0009), 라인 피드(U+000A), 캐리지 리턴(U+000D), 그리고 U+0020 ~ U+00FF 범위의 문자 등 유니코드 문자만 넣을 수 있습니다.
- 사용자, 그룹, 역할, 정책, 인스턴스 프로파일 및 서버 인증서 이름은 더하기(+), 등호(=), 콤마(,), 마침표(.), at(@), 밑줄(_), 하이픈(-)을 포함하는 영숫자여야 합니다.
- 사용자, 그룹, 역할 및 인스턴스 프로파일의 이름은 계정 내에서 고유해야 합니다. 대소문자는 구분하지 않습니다. 예를 들어 그룹 **`ADMINS`**와 그룹 **`admins`**를 모두 만들 수는 없습니다.
- 타사에서 역할을 맡기 위해 사용하는 외부 ID 값은 최소 2자 이상, 최대 1,224자 이상이어야 합니다. 이 값은 공백 없이 영숫자여야 합니다. 이 값은 더하기(+), 등호(=), 쉼표(,) 마침표(.), 기호(@), 콜론(:), 슬래시(/) 및 하이픈(-)과 같은 기호도 포함할 수 있습니다. 외부 ID에 대한 자세한 내용은 AWS 리소스에 대한 액세스를 타사에 부여할 때 외부 ID를 사용하는 방법 (p. 229)을 참조하십시오.
- 경로 이름은 슬래시(/)로 시작하고 끝나야 합니다.
- 인라인 정책 (p. 357)의 정책 이름은 이러한 정책이 포함된 사용자, 그룹 또는 역할에 대해 고유해야 합니다. 이름에는 라틴어 기본(ASCII) 문자가 포함될 수 있는데 예약된 문자인 역슬래시(\), 슬래시(/), 별표(*), 물음표(?), 공백이 없어야 합니다. 이러한 문자는 RFC 3986에 따라 설정됩니다.
- 사용자 암호(로그인 프로필)에는 라틴어 기본(ASCII) 문자가 포함될 수 있습니다.
- AWS 계정 ID 별칭은 AWS 제품 전체에서 고유해야 하며, 다음 DNS 명명 규칙을 따르는 영숫자여야 합니다. 별칭은 소문자여야 하며, 하이픈으로 시작하거나 끝나면 안 되고, 2개의 하이픈이 연속으로 있으면 안 되고, 12자리 숫자는 안 됩니다.

로마자 기본(ASCII) 문자 목록을 보려면 의회 도서관 로마자 기본(ASCII) 코드 표를 확인하십시오.

IAM 객체 제한

AWS를 이용하면 기본 IAM 엔터티 제한에 증가를 요청할 수 있습니다. 이러한 기본 제한에 대하여 한도 상승을 요청하는 방법에 대한 자세한 내용은 Amazon Web Services 일반 참조 설명서의 AWS 서비스 제한 단원을 참조하십시오.

IAM 엔터티에 대한 기본 제한:

리소스	기본 한도
AWS 계정 내 고객 관리형 정책	1500
AWS 계정 내 그룹	300
AWS 계정 내 역할	1000
IAM 역할에 연결된 관리형 정책	10
IAM 사용자에 연결된 관리형 정책	10
AWS 계정 내 가상 MFA 장치(할당된 또는 할당되지 않은 상태)	계정에 대한 사용자 할당량과 동일
AWS 계정 내 인스턴스 프로파일	1000
하나의 AWS 계정에 저장되는 서버 인증서	20

다음 제한에 대한 한도 상승을 요청할 수 없습니다.

IAM 엔터티에 대한 제한:

리소스	제한
한 명의 IAM 사용자에게 할당되는 액세스 키	2
AWS 계정 루트 사용자에 할당되는 액세스 키	2
AWS 계정당 별칭	1
IAM 사용자 한 명이 소속될 수 있는 그룹 수	10
그룹의 IAM 사용자 수	계정에 대한 사용자 할당량과 동일
AWS 계정 내 사용자	5000(다수의 사용자를 추가해야 한다면 임시 보안 자격 증명 (p. 302)의 사용을 고려할 수 있습니다.)
IAM SAML 공급자 객체와 연결된 자격 증명 공급자(IdP)	10
SAML 제공자당 키	10
IAM 사용자당 로그인 프로필	1
IAM 그룹에 연결된 관리형 정책	10
IAM 사용자에 대한 권한 경계	1
IAM 역할에 대한 권한 경계	1
한 명의 IAM 사용자가 사용하는 MFA 디바이스	1
AWS 계정 루트 사용자당 사용하는 MFA 디바이스:	1
인스턴스 프로파일 내 역할	1
AWS 계정당 SAML 제공자	100
한 명의 IAM 사용자에게 할당되는 서명 인증서	2

리소스	제한
한 명의 IAM 사용자에게 할당되는 SSH 퍼블릭 키	5
IAM 역할에 연결할 수 있는 태그	50
IAM 사용자에 연결할 수 있는 태그	50
저장할 수 있는 관리형 정책의 버전 수	5

IAM 및 STS 문자 제한

다음은 IAM 및 AWS STS에 대한 최대 문자 수 및 크기 제한입니다.

설명	한도
경로	512자
사용자 이름	64자
그룹 이름	128자
역할 이름	64자 **Important** AWS 콘솔에서 역할 전환 기능이 있는 역할을 사용하려면 `Path`와 `RoleName`을 합해 64자를 초과할 수 없습니다.
태그 키	128자 이 문자 제한은 사용자 태그, 역할 태그 및 세션 태그 (p. 294)에 적용됩니다.
태그 값	256자 이 문자 제한은 사용자 태그, 역할 태그 및 세션 태그 (p. 294)에 적용됩니다. 태그 값은 비워 둘 수 있습니다. 즉, 태그 값의 길이는 0자일 수 있습니다.
인스턴스 프로파일 이름	128자
IAM에서 생성된 고유 ID, 예: • `AIDA`로 시작되는 사용자 ID • `AGPA`로 시작되는 그룹 ID • `AROA`로 시작되는 역할 ID • `ANPA`로 시작되는 관리형 정책 ID • `ASCA`로 시작되는 서버 인증서 ID	128자

설명	한도
Note 이는 포괄적인 목록을 제공하기 위한 것이 아니며 특정 유형의 ID가 지정된 문자 조합으로만 시작됨을 보장하지도 않습니다.	
정책 이름	128자
로그인 프로필의 암호	1~128자
AWS 계정 ID의 별칭	3~63자
역할 신뢰 정책 JSON 텍스트(역할을 맡을 수 있는 사람을 결정하는 정책)	2,048자
역할 세션 이름	64자
역할 세션 기간	12시간 AWS CLI 또는 API에서 역할을 위임할 때 `duration-seconds` CLI 파라미터 또는 `DurationSeconds` API 파라미터를 사용해 더 긴 역할 세션을 요청할 수 있습니다. 이 값은 900초(15분)에서 역할에 대한 최대 세션 기간(1~12시간) 설정까지 지정할 수 있습니다. 최대 세션 기간 설정은 AWS 서비스에서 수임하는 세션을 제한하지 않습니다. 역할에 대한 최댓값을 확인하는 방법을 알아보려면 역할에 대한 최대 세션 기간 설정 보기 (p. 251) 단원을 참조하십시오. `DurationSeconds` 파라미터의 값을 지정하지 않으면 보안 자격 증명이 한 시간 동안 유효하게 됩니다.
역할 세션 정책 (p. 351)	• 역할 또는 연동 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 경우 하나의 JSON 정책 문서만 전달할 수 있습니다. • 전달된 JSON 정책 문서의 크기와 전달된 모든 관리형 정책 ARN 문자를 합친 크기는 2,048자를 초과할 수 없습니다. • 세션을 생성할 때 최대 10개의 관리형 정책 ARN을 전달할 수 있습니다. • AWS 변환은 전달된 세션 정책과 세션 태그를 별도의 제한이 있는 압축된 이진 형식으로 압축합니다. AWS CLI 또는 AWS API를 사용하여 세션 정책을 전달할 수 있습니다. `PackedPolicySize` 응답 요소는 요청에 대한 정책 및 태그가 상위 크기 제한과 얼마나 가까운지를 백분율로 나타냅니다.

설명	한도
역할 세션 태그 (p. 294)	• 세션 태그는 128자의 태그 키 제한과 256자의 태그 값 제한을 충족해야 합니다. • 최대 50개의 세션 태그를 전달할 수 있습니다. • AWS 변환은 전달된 세션 정책과 세션 태그를 별도의 제한이 있는 압축된 이진 형식으로 압축합니다. AWS CLI 또는 AWS API를 사용하여 세션 태그를 전달할 수 있습니다. `PackedPolicySize` 응답 요소는 요청에 대한 정책 및 태그가 상위 크기 제한과 얼마나 가까운지를 백분율로 나타냅니다.
인라인 정책 (p. 357):	원하는 만큼의 인라인 정책을 IAM 사용자, 역할 또는 그룹에게 추가할 수 있습니다. 단, 엔터티당 총 누적 정책 크기(모든 인라인 정책의 합)은 다음 한계를 초과할 수 없습니다. • 사용자 정책 크기는 2,048자를 초과할 수 없습니다. • 역할 정책 크기는 10,240자를 초과할 수 없습니다. • 그룹 정책 크기는 5,120자를 초과할 수 없습니다. Note IAM은 이러한 한계를 기준으로 정책의 크기를 계산할 때 공백을 계수하지 않습니다.
관리형 정책 (p. 357)	• IAM 사용자, 역할 또는 그룹당 최대 10개의 관리형 정책을 추가할 수 있습니다. • 각 관리 정책의 크기는 6,144자를 초과할 수 없습니다. Note IAM은 이 한계를 기준으로 정책의 크기를 계산할 때 공백을 계수하지 않습니다.

IAM로 작업하는 AWS 서비스

아래 나열된 AWS 서비스는 AWS 제품 범주에 의해 그룹화되며, 지원되는 IAM 기능에 대한 정보를 포함합니다.

- 서비스 – 서비스의 이름을 선택하여 해당 서비스의 IAM 권한 부여 및 액세스에 대한 AWS 문서를 볼 수 있습니다.
- 작업 – 정책에서 개별 작업을 지정할 수 있습니다. 서비스에서 이 기능을 지원하지 않는 경우 시각적 편집기(visual editor) (p. 437)의 모든 작업(All actions)이 선택됩니다. JSON 정책 문서의 * 요소에서 `Action`를 사용해야 합니다. 각 서비스의 작업 목록은 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.
- 리소스 수준 권한 – ARN (p. 564)을 사용하여 정책에서 개별 리소스를 지정할 수 있습니다. 서비스에서 이 기능을 지원하지 않는 경우 정책 시각적 편집기 (p. 437)에 모든 리소스(All resources)가 선택됩니다.

JSON 정책 문서의 * 요소에서 `Resource`를 사용해야 합니다. `List*` 작업과 같은 일부 작업은 ARN 지정을 지원하지 않습니다. 여러 리소스를 반환하기로 설계되었기 때문입니다. 서비스에서 일부 리소스에 대해서만 이 기능을 지원하지 않는 경우 표의 노란색 셀에 표시됩니다. 자세한 정보는 서비스에 대한 문서 단원을 참조하십시오.

- 리소스 기반 정책 – 리소스 기반 정책을 서비스 내 리소스에 연결할 수 있습니다. 리소스 기반 정책은 해당 리소스에 액세스할 수 있는 IAM 자격 증명을 지정하는 `Principal` 요소를 포함합니다. 자세한 정보는 자격 증명 기반 정책 및 리소스 기반 정책 (p. 372) 단원을 참조하십시오.
- 태그 기반 권한 부여 – 정책 조건에서 리소스 태그를 사용하여 서비스의 리소스에 대한 액세스를 제어할 수 있습니다. `aws:ResourceTag` (p. 659) 전역 조건 키 또는 서비스별 태그(예: `ec2:ResourceTag`)를 사용하여 이 작업을 수행합니다. 태그와 같은 속성을 기반으로 권한을 정의하는 방법에 대한 자세한 내용은 AWS용 ABAC란 무엇입니까? (p. 12) 단원을 참조하십시오.
- 임시 자격 증명 – 연동, 교차 계정 역할 또는 서비스 역할 (p. 175)을 사용하여 로그인한 사용자는 이 서비스에 액세스할 수 있습니다. AssumeRole 또는 GetFederationToken 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 가져옵니다. 자세한 정보는 임시 보안 자격 증명 (p. 302) 단원을 참조하십시오.
- 서비스 연결 역할 – 서비스 연결 역할 (p. 175)은 사용자를 대신하여 작업을 완료하기 위해 다른 서비스의 리소스에 액세스할 수 있는 서비스 권한을 부여합니다. 이러한 역할을 지원하는 서비스에 대한 설명서를 보려면 [`Yes`] 링크를 선택합니다. 자세한 정보는 서비스 연결 역할 사용 (p. 218) 단원을 참조하십시오.
- 추가 정보 – 서비스가 기능을 완전히 지원하지 않는 경우 항목에 대한 각주를 검토하여 제한 사항과 관련 정보의 링크를 볼 수 있습니다.

컴퓨팅 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Batch	예	예	아니요	아니요	예	아니요
Amazon Elastic Compute Cloud (Amazon EC2)	예	예	아니요	예	예	예[1]
Amazon EC2 Auto Scaling	예	예	아니요	예	예	예
Amazon EC2 이미지 빌더	예	예	아니요	예	예	아니요
AWS Elastic Beanstalk	예	예	아니요	예	예	예
Amazon Elastic Container Registry (Amazon ECR)	예	예	예	예	예	아니요
Amazon Elastic Container Service (Amazon ECS)	예	예[2]	아니요	예	예	예
Amazon Elastic Kubernetes Service (Amazon EKS)	예	예	아니요	예	예	예
Amazon Elastic Inference	예	예	예	아니요	아니요	아니요
Elastic Load Balancing	예	예	아니요	예	예	예
AWS Lambda	예	예	예	아니요	예	예[3]
Amazon Lightsail	예	예	아니요	예	예	아니요
AWS Outposts	예	예	아니요	예	예	아니요

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Serverless Application Repository	예	예	예	아니요	예	아니요

[1] Amazon EC2 서비스 연결 역할은 AWS Management 콘솔을 사용하여 생성할 수 없으며 예약된 인스턴스, 스팟 인스턴스 요청, 스팟 집합 요청 기능에 대해서만 사용할 수 있습니다.

[2] 일부 Amazon EC2 작업만 리소스 수준 권한을 지원합니다.

[3] AWS Lambda에는 서비스 연결 역할이 없지만 Lambda@Edge에는 있습니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 Lambda@Edge에 서비스 연결 역할 사용을 참조하십시오.

스토리지 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Backup	예	예	예	아니요	예	아니요
AWS Backup 스토리지	예	예	아니요	아니요	예	아니요
Amazon Elastic Block Store (Amazon EBS)	예	예	아니요	예	예	아니요
Amazon Elastic File System (Amazon EFS)	예	예	아니요	예	예	예
Amazon FSx	예	예	예	예	예	예
Amazon S3 Glacier	예	예	예	예	예	아니요
AWS Import/Export	예	아니요	아니요	아니요	예	아니요
AWS Migration Hub	예	예	아니요	아니요	예	아니요
Amazon Simple Storage Service (Amazon S3)	예	예	예	예[1]	예	아니요
AWS Snowball	예	아니요	아니요	아니요	예	아니요
AWS Snowball 엣지	예	아니요	아니요	아니요	아니요	아니요
AWS Storage Gateway	예	예	아니요	예	예	아니요

[1] Amazon S3에서는 객체 리소스에 대해서만 태그 기반 권한 부여를 지원합니다.

데이터베이스 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon DynamoDB	예	예	아니요	아니요	예	예
Amazon ElastiCache	예	아니요[1]	아니요	아니요	예	예
AWS Managed Apache Cassandra Service(MCS)	예	예	아니요	예	예	아니요
Amazon Quantum Ledger Database(Amazon QLDB)	예	예	아니요	예	예	아니요
Amazon Redshift	예	예	아니요	아니요	예	예
Amazon Relational Database Service (Amazon RDS)	예	예	아니요	예	예	예
Amazon RDS 데이터 API	예	아니요	아니요	아니요	예	아니요
Amazon SimpleDB	예	예	아니요	아니요	예	아니요

[1] 정책에서 ElastiCache 리소스 ARN을 지정할 수 없지만 클러스터 또는 복제를 시드할 때 ElastiCache 작업을 사용하여 Amazon S3 ARN을 지정할 수 있습니다. 그룹.

개발자 도구 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Cloud9	예	예	예	예	예	예
CodeBuild	예	예	예[1]	예[2]	예	아니요
CodeCommit	예	예	아니요	예	예	아니요
AWS CodeDeploy	예	예	아니요	아니요	예	아니요
CodePipeline	예	예	아니요	예	예	아니요
AWS CodeStar	예	예[1]	아니요	예	예	아니요
AWS CodeStar 알림	예	예	아니요	예	예	예
AWS X-Ray	예	예	아니요	아니요	예	아니요

[1] CodeBuild는 AWS RAM를 통해 교차 계정 리소스 공유를 지원합니다.

[2] CodeBuild는 프로젝트 기반 작업에 대한 태그를 기반으로 권한 부여를 지원합니다.

보안, 자격 증명 및 규정 준수 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Certificate Manager Private Certificate Authority (ACM)	예	예	아니요	예	예	아니요
AWS Artifact	예	예	아니요	아니요	예	아니요
AWS Certificate Manager (ACM)	예	예	아니요	예	예	아니요
AWS CloudHSM	예	예	아니요	예	예	예
AWS CloudHSM 클래식	예	아니요	아니요	아니요	아니요	아니요
Amazon Cognito	예	예	아니요	예	예	예
Amazon Detective	예	예	아니요	아니요	예	아니요
AWS Directory Service	예	예	아니요	예	예	아니요
AWS Firewall Manager	예	예	예	예	예	예
Amazon GuardDuty	예	예	아니요	아니요	예	예
AWS Identity and Access Management (IAM)	예	예	예[1]	예[2] (p. 382)	예[3]	아니요
IAM 액세스 분석기	예	예	아니요	예	예	예
Amazon Inspector	예	아니요	아니요	아니요	예	예
AWS Key Management Service (AWS KMS)	예	예	예	아니요	예	예
Amazon Macie	예	아니요	아니요	아니요	예	예
AWS 리소스 액세스 관리자(AWS RAM)	예	예	아니요	예	예	아니요
AWS Secrets Manager	예	예	예	예	예	아니요
AWS Security Hub	예	예	아니요	예	예	예
AWS Single Sign-On (AWS SSO)	예	아니요	아니요	아니요	예	예
AWS SSO 디렉터리	예	아니요	아니요	아니요	예	아니요
AWS Security Token Service (AWS STS)	예	예[4]	아니요	예	예[5]	아니요
AWS Shield Advanced	예	예	아니요	아니요	예	아니요
AWS WAF	예	예	아니요	아니요	예	예
AWS WAFV2	예	예	아니요	예	예	아니요

[1] IAM은 역할 신뢰 정책이라고 하는 리소스 기반 정책 유형 하나만 지원하며, 이 유형은 IAM 역할에 연결됩니다. 자세한 정보는 사용자에 대한 역할 전환 권한 부여 (p. 252) 단원을 참조하십시오.

[2] IAM에서는 사용자 및 역할 리소스에 대해서만 태그 기반 액세스 제어를 지원합니다.

[3] IAM에 대한 일부 API 작업만 임시 자격 증명으로 호출할 수 있습니다. 자세한 정보는 API 옵션 비교 단원을 참조하십시오.

[4] AWS STS는 "리소스"가 없지만 사용자에게 유사한 방식으로 액세스를 제한하는 것을 허용합니다. 자세한 정보는 이름을 사용한 임시 보안 자격 증명 액세스 거부 단원을 참조하십시오.

[5] AWS STS에 대한 일부 API만 임시 자격 증명을 이용한 호출을 지원합니다. 자세한 정보는 API 옵션 비교 단원을 참조하십시오.

Machine Learning 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon CodeGuru	예	아니요	아니요	아니요	예	예
Amazon CodeGuru 프로파일러	예	예	아니요	아니요	예	아니요
Amazon CodeGuru 검토자	예	예	아니요	예	예	예
Amazon Comprehend	예	예	아니요	예	예	아니요
AWS DeepComposer	예	예	아니요	아니요	예	아니요
AWS DeepRacer	예	아니요	아니요	아니요	예	예
Forecast	예	예	아니요	아니요	예	아니요
Amazon Fraud Detector	예	아니요	아니요	아니요	예	아니요
Ground Truth Labeling	예	아니요	아니요	아니요	예	아니요
Amazon Kendra	예	예	아니요	아니요	예	아니요
Amazon Lex	예	예	아니요	아니요	예	예
Amazon Machine Learning	예	예	아니요	예	예	아니요
Amazon Personalize	예	예	아니요	아니요	예	아니요
Amazon Polly	예	예	아니요	아니요	예	아니요
Amazon Rekognition	예	예	아니요	아니요	예	아니요
Amazon SageMaker	예	예	아니요	예	예	아니요
Amazon Textract	예	예	아니요	아니요	아니요	아니요
Amazon Transcribe	예	아니요	아니요	아니요	예	아니요
Amazon Translate	예	아니요	아니요	아니요	예	아니요

관리 및 거버넌스 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Application Auto Scaling	예	아니요	아니요	아니요	예	예
AWS AppConfig	예	예	아니요	예	예	아니요
AWS Auto Scaling	예	아니요	아니요	아니요	예	예
AWS 챗봇	예	예	아니요	아니요	예	예
AWS CloudFormation	예	예	아니요	예	예	아니요
AWS CloudTrail	예	예	아니요	아니요	예	아니요
Amazon CloudWatch	예	예	아니요	예	예	예[1]
Amazon CloudWatch Events	예	예	아니요	예	예	아니요
Amazon CloudWatch Logs	예	예	예	아니요	예	아니요
Amazon CloudWatch Synthetics	예	예	아니요	아니요	예	아니요
AWS Compute Optimizer	예	아니요	아니요	아니요	예	예
AWS Config	예	예[2]	아니요	예	예	예
Amazon 데이터 수명 주기 관리자	예	예	아니요	예	예	아니요
AWS Health	예	예	아니요	아니요	예	아니요
AWS OpsWorks	예	예	아니요	예	예	아니요
AWS OpsWorks for Chef Automate	예	예	아니요	예	예	아니요
AWS Organizations	예	예	아니요	아니요	예	예
AWS 리소스 그룹	예	예	아니요	예	예[3]	아니요
리소스 그룹 Tagging API	예	아니요	아니요	아니요	예	아니요
AWS Service Catalog	예	아니요	아니요	예[4]	예	아니요
AWS 시스템 관리자	예	예	아니요	예	예	예
AWS Trusted Advisor	예[5]	예	아니요	아니요	예	예
AWS Well-Architected Tool	예	예	아니요	아니요	예	아니요

[1] Amazon CloudWatch 서비스 연결 역할은 AWS Management 콘솔을 사용하여 생성할 수 없으며 경보 작업 기능만 지원합니다.

[2] AWS Config의 경우 다중 계정 다중 리전 데이터 집계 및 AWS Config 역할에 대한 리소스 수준 권한을 지원합니다. 지원되는 리소스 목록을 보려면 AWS Config API 가이드의 다중 계정 다중 리전 데이터 집계 섹션 및 AWS Config 역할 섹션을 참조하십시오.

[3] 사용자는 AWS 리소스 그룹 작업을 허용하는 정책이 있는 역할을 수임할 수 있습니다.

[4] AWS Service Catalog의 경우 API 작업을 입력에 있는 하나의 리소스와 일치시키는 작업에 대해서만 태그 기반 액세스 제어를 지원합니다.

[5] Trusted Advisor에 대한 API 액세스는 AWS Support API를 통해 이루어지며 AWS Support IAM 정책으로 제어합니다.

마이그레이션 및 전송 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Database Migration Service	예	아니요	아니요	아니요	예	아니요
AWS Application Discovery Service	예	아니요	아니요	아니요	아니요	예
AWS Database Migration Service	예	예	예[1]	예	예	아니요
AWS Migration Hub	예	예	아니요	아니요	예	아니요
AWS Server Migration Service	예	아니요	아니요	아니요	예	예

[1] 지원되는 대상 엔드포인트로 마이그레이션된 데이터를 암호화하도록 생성한 AWS KMS 암호화 키에 연결된 정책을 생성 및 수정할 수 있습니다. 지원되는 대상 엔드포인트에는 Amazon Redshift 및 Amazon S3 등이 있습니다. 자세한 내용은 AWS Database Migration Service 사용 설명서의 AWS KMS 키 생성 및 사용을 통한 Amazon Redshift 대상 데이터 암호화 및 AWS KMS 키 생성을 통한 Amazon S3 대상 객체 암호화를 참조하십시오.

모바일 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS 증폭	예	예	아니요	예	예	아니요
AWS Device Farm	예	예	아니요	예	예	아니요

네트워킹 및 콘텐츠 전송 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon API Gateway	예	예	예	예	예	예
AWS App Mesh	예	예	아니요	예	예	예
Amazon CloudFront	예[1]	예	아니요	예	예	예[4]
AWS Cloud Map	예	예	아니요	아니요	예	아니요

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Direct Connect	예	예	아니요	예	예	아니요
AWS Global Accelerator	예	예	아니요	예	예	예
Network Manager	예	예	예	예	예	예
Amazon Route 53	예	예	아니요	아니요	예	아니요
Amazon Route 53 해석기	예	예	아니요	예	예	아니요
Amazon Virtual Private Cloud (Amazon VPC)	예	예[2]	예[3]	아니요	예	아니요

[1] CloudFront는 CloudFront 키 페어 생성을 위한 작업 수준 권한을 지원하지 않습니다. AWS 계정 루트 사용자을(를) 사용하여 CloudFront 키 페어를 생성해야 합니다. 자세한 정보는 Amazon CloudFront 개발자 안내서의 신뢰할 수 있는 서명자에 대해 CloudFront 키 페어 생성 단원을 참조하십시오.

[2] IAM 사용자 정책에서는 특정 Amazon VPC 엔드포인트에 대해 권한을 제한할 수 없습니다. `Action` 또는 `ec2:*VpcEndpoint*` API 작업을 포함하는 모든 `ec2:DescribePrefixLists` 요소는 `""Resource": "*""`를 포함해야 합니다. 자세한 정보는 Amazon VPC 사용 설명서의 엔드포인트 사용 제어 단원을 참조하십시오.

[3] Amazon VPC에서는 단일 리소스 정책을 VPC 엔드포인트에 연결하여 해당 엔드포인트를 통해 액세스 가능한 대상을 제한할 수 있도록 지원합니다. 특정 Amazon VPC 엔드포인트의 리소스에 대한 액세스를 제어하기 위해 리소스 기반 정책을 사용하는 방법에 대한 자세한 정보는 Amazon VPC 사용 설명서의 엔드포인트 정책 사용 단원을 참조하십시오.

[4] Amazon CloudFront에는 서비스 연결 역할이 없지만 Lambda@Edge에는 있습니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 Lambda@Edge에 서비스 연결 역할 사용을 참조하십시오.

미디어 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon Elastic Transcoder	예	예	아니요	아니요	예	아니요
AWS Elemental MediaConnect	예	예	아니요	아니요	예	아니요
AWS Elemental MediaConvert	예	예	아니요	예	예	아니요
AWS Elemental MediaLive	예	예	예	예	예	아니요
AWS Elemental MediaPackage	예	예	아니요	예	예	아니요
AWS Elemental MediaStore	예	예	예	아니요	예	아니요
AWS Elemental MediaTailor	예	예	아니요	예	예	아니요
Kinesis 비디오 스트림	예	예	아니요	예	예	아니요

분석 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon Athena	예	예	아니요	예	예	아니요
Amazon CloudSearch	예	예	아니요	아니요	예	아니요
AWS Data Exchange	예	예	아니요	예	예	아니요
AWS Data Pipeline	예	아니요	아니요	예	예	아니요
Amazon Elasticsearch Service	예	예	예	아니요	예	예
Amazon EMR	예	예	아니요	예	예	예
AWS Glue	예	예	예	예	예	아니요
Amazon Kinesis Data Analytics	예	예	아니요	예	예	아니요
Amazon Kinesis Data Firehose	예	예	아니요	예	예	아니요
Amazon Kinesis Data Streams	예	예	아니요	아니요	예	아니요
AWS Lake Formation	예	아니요	아니요	아니요	예	예
Amazon Managed Streaming for Apache Kafka(MSK)	예	예	아니요	예	예	아니요
Amazon QuickSight	예	예	아니요	아니요	예	아니요

애플리케이션 통합 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon EventBridge	예	예	아니요	예	예	아니요
Amazon EventBridge 스키마	예	예	아니요	예	예	아니요
Amazon MQ	예	예	아니요	예	예	아니요
Amazon Simple Notification Service (Amazon SNS)	예	예	예	아니요	예	아니요
Amazon Simple Queue Service (Amazon SQS)	예	예	예	아니요	예	아니요
AWS Step Functions	예	예	아니요	예	예	아니요
Amazon Simple Workflow Service (Amazon SWF)	예	예	아니요	예	예	아니요

비즈니스 애플리케이션 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Alexa for Business	예	예	아니요	아니요	예	아니요
Amazon Chime	예	예	아니요	아니요	예	예
Amazon WorkMail	예	예	아니요	예	예	예

위성 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Ground Station	예	예	아니요	예	예	아니요

사물 인터넷 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS IoT Greengrass	예	예	아니요	예	예	아니요
AWS IoT	예	예	예[1]	예	예	아니요
AWS IoT Analytics	예	예	아니요	예	예	아니요
AWS IoT Device Tester	예	아니요	아니요	아니요	예	아니요
AWS IoT Events	예	예	아니요	예	예	아니요
AWS IoT Things Graph	예	아니요	아니요	아니요	예	아니요
AWS IoT SiteWise	예	예	아니요	아니요	예	아니요
FreeRTOS	예	예	아니요	예	예	아니요

[1] AWS IoT에 연결된 디바이스는 X.509 인증서 또는 Amazon Cognito 자격 증명을 통해 인증됩니다. AWS IoT 정책을 X.509 인증서 또는 Amazon Cognito 자격 증명에 연결하여 디바이스가 어떤 작업을 수행하도록 권한 부여할 것인지 제어할 수 있습니다. 자세한 정보는 AWS IoT 개발자 안내서의 AWS IoT의 보안 및 자격 증명 단원을 참조하십시오.

로봇 공학 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
RoboMaker	예	예	아니요	예	아니요	예

블록체인 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon Managed Blockchain	예	예	아니요	아니요	예	아니요

게임 개발 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon GameLift	예	예	아니요	아니요	예	아니요

AR 및 VR 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon Sumerian	예	예	아니요	아니요	예	아니요

고객 참여 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS IQ	아니요	아니요	아니요	아니요	예	아니요
AWS IQ 권한	아니요	아니요	아니요	아니요	예	아니요
AWS Support	예	아니요	아니요	아니요	예	예

고객 참여 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon Connect	예	예	아니요	아니요	예	예
Amazon Pinpoint	예	예	아니요	예	예	아니요
Amazon Simple Email Service (Amazon SES)	예	예[1]	예	예	예[2]	아니요

[1] `ses:SendEmail` 또는 `ses:SendRawEmail` 등과 같이 이메일 전송과 관련된 작업을 참조하는 정책 설명의 리소스 수준 권한만 사용할 수 있습니다. 기타 다른 작업을 참조하는 정책 설명의 경우 리소스 요소에 *만 포함될 수 있습니다.

[2] Amazon SES API만이 임시 보안 자격 증명을 지원합니다. Amazon SES SMTP 인터페이스는 임시 보안 자격 증명에서 파생된 SMTP 자격 증명을 지원하지 않습니다.

최종 사용자 컴퓨팅 서비스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
Amazon AppStream	예	아니요	아니요	아니요	예	아니요
Amazon AppStream 2.0	예	예	아니요	예	예	아니요
Amazon WAM	예	아니요	아니요	아니요	예	아니요
Amazon WorkDocs	예	아니요	아니요	아니요	예	아니요
Amazon WorkLink	예	예	예	아니요	예	예
Amazon WorkSpaces	예	예	아니요	예	예	아니요

추가 리소스

서비스	작업	리소스 수준 권한	리소스 기반 정책	태그 기반 권한 부여	2013년 5월 22일	서비스 연결 역할
AWS Billing and Cost Management	예	아니요	아니요	아니요	예	아니요
AWS Marketplace	예	아니요	아니요	아니요	예	아니요
AWS Marketplace Catalog	예	예	아니요	아니요	예	아니요
AWS Private Marketplace	예	아니요	아니요	아니요	아니요	아니요

IAM JSON 정책 참조

이 단원에서는 IAM에서 JSON 정책의 자세한 구문과 설명, 요소의 예, 변수, 평가 로직을 설명합니다. 더 일반적인 내용은 JSON 정책 개요 (p. 354) 단원을 참조하십시오.

본 참조는 다음 섹션을 포함합니다:

- IAM JSON 정책 요소 참조 (p. 586) — 정책을 생성할 때 사용할 수 있는 요소에 대해 자세히 알아봅니다. 더 많은 정책 예제를 보면서 조건, 지원되는 데이터 유형, 다양한 서비스에서 사용되는 방법을 살펴봅니다.
- 정책 평가 로직 (p. 622) — 이 단원에서는 AWS 요청, 그 요청이 인증되는 방식 및 AWS가 정책을 사용하여 리소스에 대한 액세스를 결정하는 방식을 기술합니다.
- IAM JSON 정책 언어의 문법 (p. 637) — 이 단원에서는 IAM에서 정책 생성 시 사용되는 언어의 정규 문법에 대해 살펴보겠습니다.
- 직무 기능에 대한 AWS 관리형 정책 (p. 642) — 이 단원에서는 IT 업계의 일반적인 직무와 직접 매핑되는 모든 AWS 관리형 정책이 나열됩니다. 이러한 정책을 사용하여 특정 직무 담당자에게 기대되는 작업 수행에 필요한 권한을 부여할 수 있습니다. 이러한 정책은 다수의 서비스에 대한 권한을 단일 정책으로 통합합니다.
- AWS 전역 조건 컨텍스트 키 (p. 650) — 이 단원에는 IAM 정책에서 권한을 제한하는 데 사용할 수 있는 모든 AWS 전역 조건 키 목록이 포함되어 있습니다.
- IAM 및 AWS STS 조건 컨텍스트 키 (p. 664) — 이 단원에는 IAM 정책에서 권한을 제한하는 데 사용할 수 있는 모든 IAM 및 AWS STS 조건 키 목록이 포함되어 있습니다.
- AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) — 이 단원에는 IAM 정책에서 권한으로 사용할 수 있는 모든 AWS API 작업 목록이 나와 있습니다. 또한 요청을 추가로 미세 조정하는 데 사용할 수 있는 서비스별 조건 키도 포함되어 있습니다.

IAM JSON 정책 요소 참조

JSON 정책 문서는 여러 요소로 구성됩니다. 여기에 나열되는 요소들은 정책에서 사용되는 일반적인 순서를 따릅니다. 요소 순서는 중요하지 않습니다.—예를 들어 `Resource` 요소는 `Action` 요소 앞에 올 수 있습니다. 또한 정책에서 `Condition` 요소는 지정하지 않아도 됩니다. JSON 정책 문서의 일반적인 구조와 목적에 대해 자세히 알아보려면 JSON 정책 개요 (p. 354)를 참조하십시오.

일부 JSON 정책 요소는 함께 사용할 수 없습니다. 즉, 둘 다 사용하는 정책을 생성할 수 없습니다. 예를 들어 동일한 정책 문에서 `Action`과 `NotAction` 둘 다 사용할 수 없습니다. 함께 사용할 수 없는 다른 쌍에는 `Principal`/`NotPrincipal` 및 `Resource`/`NotResource`가 있습니다.

정책 세부 정보는 서비스에서 유효한 작업이나 추가되는 리소스 유형 등에 따라 각 서비스마다 차이가 있습니다. 따라서 특정 서비스에 맞는 정책을 작성할 때는 해당 서비스의 정책 예제를 살펴보는 것이 좋습니다. IAM을 지원하는 모든 서비스 목록을 비롯해 각 서비스의 IAM 및 정책 설명서 링크는 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

주제

IAM JSON 정책 요소: Version

동음이의어 참고

`Version` JSON 정책 요소는 정책 버전과 다릅니다. `Version` 정책 요소는 정책 내에서 사용되며 정책 언어의 버전을 정의합니다. 반면에 정책 버전은 IAM에서 고객 관리형 정책을 변경할 때 생성됩니다. 변경된 정책은 기존 정책을 덮어쓰지 않습니다. 대신 IAM에서 관리형 정책의 새 버전을 만듭니다. 관리형 정책에서 사용할 수 있는 여러 버전 지원에 대한 정보를 찾고 있다면 the section called “IAM 정책 버전 관리” (p. 458) 단원을 참조하십시오.

`Version` 정책 요소는 정책의 처리에 사용할 언어 구문 규칙을 지정합니다. 사용 가능한 모든 정책 기능을 사용하려면 모든 정책에서 `Statement` 요소 앞에 다음의 `Version` 요소를 포함시킵니다.

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

IAM은 다음과 같은 `Version` 요소 값을 지원합니다.

- `2012-10-17`. 이 값은 정책 언어의 현재 버전이며, 항상 `Version` 요소를 포함하여 `2012-10-17`로 설정해야 합니다. 그렇지 않으면 이 버전에 채택되지 않은 정책 변수 (p. 615) 등의 기능을 사용할 수 없습니다.
- `2008-10-17`. 이 값은 이전 정책 언어 버전입니다. 따라서 오래된 기존 정책에서는 이 버전이 표시될 수도 있습니다. 새로운 정책에서는 또는 기존 정책을 업데이트하는 경우에는 이 버전을 사용하지 마십시오.

`Version` 요소를 포함하지 않을 경우의 기본값은`2008-10-17`이지만 정책 기능 등 최신 기능을 정책에서 사용할 수 없습니다. 예를 들어 `${aws:username}` 같은 변수가 정책에서 변수로 인식되지 않고 리터럴 문자열로 취급됩니다.

IAM JSON 정책 요소: Id

`Id` 요소는 정책 식별자(옵션)를 지정합니다. 다른 서비스의 ID 사용 방법과는 다릅니다.

`ID` 요소를 설정할 수 있는 서비스의 경우에는 UUID(GUID)를 값으로 사용하거나, UUID를 ID 일부로 사용하여 고유성을 확보하는 것이 좋습니다.

```
"Id": "cd3ad3d9-2776-4ef1-a904-4c229d1642ee"
```

Note

AWS 서비스(예: Amazon SQS 또는 Amazon SNS 등) 중에는 이 요소가 필요하거나 고유성 요건을 따로 요구하는 경우도 있습니다. 정책 작성에 대한 서비스별 정보는 이용하려는 서비스의 설명서를 참조하십시오.

IAM JSON 정책 요소: Statement

`Statement` 요소는 정책의 주요 요소로서 필수입니다. `Statement` 요소는 단일 문 또는 개별 문의 배열을 포함할 수 있습니다. 각 개별 문 블록은 중괄호 `{}`로 묶어야 합니다. 여러 문의 경우 배열은 대괄호 `[]`로 묶어야 합니다.

```
"Statement": [{...},{...},{...}]
```

다음은 단일 `Statement` 요소에서 3개의 문이 하나의 배열을 이루는 정책을 나타낸 예제입니다 (이 정책에서는 Amazon S3 콘솔에서 자신의 'home 폴더'에 액세스할 수 있습니다). 정책에는 `aws:username` 변수가 추가되었습니다. 이 변수는 정책 평가 중 요청이 있으면 사용자 이름으로 바뀝니다. 자세한 내용은 소개 (p. 615)를 참조하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::BUCKET-NAME",
      "Condition": {"StringLike": {"s3:prefix": [
        "",
        "home/",
        "home/${aws:username}/"
      ]}}
    },
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::BUCKET-NAME/home/${aws:username}",
        "arn:aws:s3:::BUCKET-NAME/home/${aws:username}/*"
      ]
    }
  ]
}
```

IAM JSON 정책 요소: Sid

`Sid`(문 ID)는 정책 문에 입력되는 식별자(옵션)입니다. `Sid` 값은 문 배열에서 각 문에 할당할 수 있습니다. SQS나 SNS처럼 `ID` 요소를 지정할 수 있는 서비스에서는 `Sid` 값이 정책 문서 ID의 하위 ID나 마찬가지입니다. IAM에서 `Sid` 값은 JSON 정책 내 고유성이 보장되어야 합니다.

```
"Sid": "1"
```

`Sid` 요소는 대문자, 소문자 및 숫자를 지원합니다.

IAM에서 `Sid`는 IAM API에 노출되지 않습니다. 따라서 이 ID를 근거로 특정 문을 가져올 수는 없습니다.

> **Note**
>
> AWS 서비스(예: Amazon SQS 또는 Amazon SNS 등) 중에는 이 요소가 필요하거나 고유성 요건을 따로 요구하는 경우도 있습니다. 정책 작성에 대한 서비스별 정보는 이용하려는 서비스의 설명서를 참조하십시오.

IAM JSON 정책 요소: Effect

`Effect` 요소는 필수로서, 문의 허용(allow) 또는 명시적 거부(explicit deny) 중 하나를 지정합니다. `Effect` 유효값은 `Allow` 및 `Deny`입니다.

```
"Effect":"Allow"
```

기본적으로 리소스 액세스는 거부됩니다. 리소스 액세스를 허용하려면 `Effect` 요소를 `Allow`로 설정해야 합니다. 허용을 재정의하려면(예: 그 밖에 다른 방법으로 실행 중인 허용을 재정의하려면) `Effect` 요소를 `Deny`로 설정합니다. 자세한 내용은 정책 평가 로직 (p. 622) 단원을 참조하십시오.

AWS JSON 정책 요소: Principal

정책의 `Principal` 요소를 사용하여 리소스에 대한 액세스가 허용되거나 거부되는 보안 주체를 지정합니다. IAM 자격 증명 기반 정책에서는 `Principal` 요소를 사용할 수 없습니다. IAM 역할을 위한 신뢰 정책 및 리소스 기반 정책에서는 사용할 수 있습니다. 리소스 기반 정책은 IAM 리소스에 직접 삽입할 수 있는 정책입니다. 예를 들어, Amazon S3 버킷 또는 AWS KMS 고객 마스터 키(CMK)에 정책을 삽입할 수 있습니다.

정책에서 다음 보안 주체를 지정할 수 있습니다.

- AWS 계정 및 루트 사용자
- IAM 사용자
- 연동 사용자(웹 자격 증명 또는 SAML 연동 사용)
- IAM 역할
- 위임된 역할 세션
- AWS 서비스
- 익명 사용자(권장하지 않음)

`Principal` 요소의 사용 방법은 아래와 같습니다.

- IAM 역할의 신뢰 정책에서 `Principal` 요소를 사용하여 역할을 위임할 사용자를 지정합니다. 교차 계정 액세스인 경우에는 신뢰할 수 있는 계정의 12자리 식별자를 지정합니다. 해당 신뢰 영역(신뢰할 수 있는 조직 또는 계정) 외의 계정 내 보안 주체가 역할을 수임하는 권한이 있는지 자세히 알고 싶다면, IAM Access Analyzer란 무엇일까요? 단원을 참조하십시오.

  > **Note**
  >
  > 역할을 생성한 이후 계정을 "*"로 변경하여 모두가 이 역할을 수임하도록 할 수 있습니다. 이렇게 하는 경우 다른 방법(예: 특정 IP 주소로만 액세스를 제한하는 `Condition` 요소)을 통해 역할에 액세스할 수 있는 사용자를 제한하는 것이 좋습니다. 역할을 모두 액세스할 수 있는 상태로 두지 마십시오.
- 리소스 기반 정책에서는 `Principal` 요소를 사용해 리소스 액세스가 허용된 계정 또는 사용자를 지정합니다.

IAM 사용자 및 그룹에 연결한 정책에서는 `Principal` 요소를 사용하지 마십시오. 마찬가지로 IAM 역할의 권한 정책에서도 보안 주체를 지정해서는 안 됩니다. 이 경우 보안 주체는 묵시적으로 정책이 연결되어 있는 사용자(IAM 사용자) 또는 역할을 위임하는 사용자(역할 액세스 정책)가 됩니다. 그리고, 정책이 IAM 그룹에 연결되면 해당 그룹 내에서 요청하는 IAM 사용자가 보안 주체가 됩니다.

보안 주체 지정

보안 주체자의 Amazon 리소스 이름(ARN) (p. 564) 또는 다른 식별자를 사용하여 보안 주체를 지정합니다. IAM 그룹 및 인스턴스 프로파일을 보안 주체로 지정할 수 없습니다.

다음 예에서는 보안 주체를 지정하는 여러 가지 방법을 보여 줍니다.

특정 AWS 계정

정책에서 AWS 계정 식별자를 보안 주체로 사용할 경우 권한을 해당 계정에게 위임하는 것과 다름없습니다. 이 계정 내에서는 정책 문의 권한을 모든 자격 증명에게 부여할 수 있습니다. 여기에는 해당 계정의 IAM 사용

자 및 역할이 포함됩니다. AWS 계정을 지정하는 경우 계정 ARN(arn:aws:iam::*AWS-account-ID*:root)을 사용하거나 접두사 `AWS:`와 그 뒤에 계정 ID가 따라오는 약식 형태를 사용할 수 있습니다.

예를 들어, 계정 ID `123456789012`의 경우 다음 방법 중 하나를 사용하여 `Principal` 요소에서 해당 계정을 지정할 수 있습니다.

```
"Principal": { "AWS": "arn:aws:iam::123456789012:root" }
```

```
"Principal": { "AWS": "123456789012" }
```

또한 앞서 언급한 방법을 자유롭게 조합하여 배열을 사용해 두 개 이상의 AWS 계정을 보안 주체로 지정할 수 있습니다.

```
"Principal": {
  "AWS": [
    "arn:aws:iam::123456789012:root",
    "999999999999"
  ]
}
```

일부 AWS 서비스는 계정 보안 주체를 지정하기 위한 몇 가지 옵션을 추가로 지원합니다. 예를 들어 Amazon S3에서는 다음 형식을 사용하여 정식 사용자 ID를 지정할 수 있습니다.

```
"Principal": { "CanonicalUser":
 "79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be" }
```

개별 IAM 사용자

다음 예제와 같이 개별 IAM 사용자를 보안 주체로 지정할 수 있습니다. 요소에 둘 이상의 보안 주체를 지정할 때 각 보안 주체에 권한을 부여하십시오. 한 번에 하나의 보안 주체로 인증되기 때문에 이것은 논리적 `AND`이며 논리적 `OR`이 아닙니다.

> **Note**
>
> `Principal` 요소에서 사용자 이름은 대/소문자를 구분합니다.

```
"Principal": { "AWS": "arn:aws:iam::AWS-account-ID:user/user-name" }
```

```
"Principal": {
  "AWS": [
    "arn:aws:iam::AWS-account-ID:user/user-name-1",
    "arn:aws:iam::AWS-account-ID:user/UserName2"
  ]
}
```

`Principal` 요소로 사용자를 지정할 때는 "모든 사용자"의 의미로 와일드카드(`*`)를 사용할 수 없습니다. 보안 주체는 항상 특정 사용자가 되어야 하기 때문입니다.

> **Important**
>
> 역할 신뢰 정책의 `Principal` 요소에 특정 IAM 사용자를 가리키는 ARN이 포함되어 있으면, 정책을 저장할 때 해당 ARN이 해당 사용자의 고유 보안 주체 ID로 변환됩니다. 그러면 누군가가 해당 사용자를 제거하고 다시 만들어 본인의 권한을 에스컬레이션할 위험을 완화할 수 있습니다. 일반적으로 콘솔에서는 이 ID가 보이지 않습니다. 신뢰 정책이 표시될 때 해당 사용자의 ARN으로 다시 역변환되기 때문입니다. 그러나 해당 사용자를 삭제하면 관계가 깨집니다. 사용자를 다시 생성해도 정책은 더 이상 적용되지 않습니다. 새 사용자의 새 보안 주체 ID가 신뢰 정책에 저장된 ID와 일치하지 않기 때문입니다. 이 경우 보안 주체 ID가 콘솔에 표시됩니다. AWS에서 더 이상 이를 유효한 ARN

에 다시 매핑할 수 없기 때문입니다. 결과적으로 신뢰 정책의 `Principal` 요소에서 참조된 사용자를 삭제하고 다시 만드는 경우, 역할을 편집하여 현재의 잘못된 보안 주체 ID를 올바른 ARN으로 바꿔야 합니다. 정책을 저장하면 ARN이 다시 해당 사용자의 새로운 보안 주체 ID로 변환됩니다.

연동 웹 자격 증명 사용자

```
"Principal": { "Federated": "cognito-identity.amazonaws.com" }
```

```
"Principal": { "Federated": "www.amazon.com" }
```

```
"Principal": { "Federated": "graph.facebook.com" }
```

```
"Principal": { "Federated": "accounts.google.com" }
```

연동 SAML 사용자

```
"Principal": { "Federated": "arn:aws:iam::AWS-account-ID:saml-provider/provider-name" }
```

IAM역할

```
"Principal": { "AWS": "arn:aws:iam::AWS-account-ID:role/role-name" }
```

Important

역할 신뢰 정책의 `Principal` 요소에 특정 IAM 역할을 가리키는 ARN이 포함되어 있으면, 정책을 저장할 때 해당 ARN이 해당 역할의 고유 보안 주체 ID로 변환됩니다. 그러면 누군가가 해당 역할을 제거하고 다시 만들어 본인의 권한을 에스컬레이션할 위험을 완화할 수 있습니다. 일반적으로 콘솔에서는 이 ID가 보이지 않습니다. 신뢰 정책이 표시될 때 해당 역할의 ARN으로 다시 역변환되기 때문입니다. 그러나 해당 역할을 삭제하면 관계가 깨집니다. 역할을 다시 만들더라도 해당 정책이 더 이상 적용되지 않습니다. 새 역할의 새 보안 주체 ID가 신뢰 정책에 저장된 ID와 일치하지 않기 때문입니다. 이 경우 보안 주체 ID가 콘솔에 표시됩니다. AWS에서 더 이상 이를 유효한 ARN에 다시 매핑할 수 없기 때문입니다. 결과적으로 신뢰 정책의 `Principal` 요소에서 참조된 역할을 삭제하고 다시 만드는 경우, 현재 잘못된 보안 주체 ID를 올바른 ARN으로 바꾸도록 역할을 편집해야 합니다. 정책을 저장하면 ARN이 다시 해당 역할의 새로운 보안 주체 ID로 변환됩니다.

특정 위임된 역할 세션

```
"Principal": { "AWS": "arn:aws:sts::AWS-account-ID:assumed-role/role-name/role-session-name" }
```

`Principal` 요소에 위임된 역할 세션을 지정할 때 와일드카드(*)를 사용하여 "모든 세션"을 의미할 수 없습니다. 보안 주체는 항상 특정 세션의 이름을 지정해야 합니다.

AWS 서비스

AWS 서비스에서 위임할 수 있는 IAM 역할을 서비스 역할 (p. 175)이라고 합니다. 서비스 역할에는 신뢰 정책이 포함되어 있어야 합니다. 신뢰 정책은 역할을 위임할 수 있는 보안 주체를 정의하는 역할에 연결된 리소스 기반 정책입니다. 일부 서비스 역할에는 신뢰 정책이 미리 정의되어 있습니다. 그러나 신뢰 정책에 서비스 보안 주체를 지정해야 하는 경우도 있습니다. 서비스 보안 주체는 서비스에 권한을 부여하는 데 사용되는 식별자입니다. 식별자에는 긴 버전의 서비스 이름이 포함되어 있고 보통은 다음과 같은 형식을 갖습니다.

long_service-name`.amazonaws.com`

서비스 보안 주체는 서비스가 정의합니다. 서비스의 보안 주체를 확인하려면 해당 서비스의 설명서를 참조하십시오. 일부 서비스에 대해서는 IAM로 작업하는 AWS 서비스 (p. 573)을 참조하여 서비스 연결 역할 열에

예라고 표시된 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [Yes] 링크를 선택합니다. 서비스의 보안 주체를 보려면 Service-Linked Role Permissions(서비스 연결 역할 권한) 단원을 참조하십시오.

다음 예제는 서비스 역할에 연결할 수 있는 정책을 보여줍니다. 이 정책은 Amazon EMR 서비스와 AWS Data Pipeline 서비스가 역할을 수행할 수 있도록 합니다. 그러면 서비스가 해당 역할에 할당된 권한 정책에서 부여한 모든 작업을 수행할 수 있습니다(표시되지 않음). 여러 서비스 보안 주체를 지정할 때 `Service` 요소를 두 개 지정하면 안 됩니다. 하나만 지정할 수 있습니다. 대신 여러 서비스 보안 주체의 배열을 하나의 `Service` 요소의 값으로 사용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "elasticmapreduce.amazonaws.com",
          "datapipeline.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

익명 사용자(퍼블릭)

Amazon S3 버킷 정책과 같은 리소스 기반 정책의 경우 보안 주체 요소의 와일드카드(*)는 모든 사용자와 퍼블릭 액세스를 지정합니다. 다음 요소는 동일합니다.

```
"Principal": "*"
```

```
"Principal" : { "AWS" : "*" }
```

이름이나 ARN의 일부를 나타내기 위해 와일드카드를 사용할 수 없습니다.

정책에서 `Principal` 요소를 통해 액세스를 달리 제한하지 않을 경우 역할의 신뢰 정책에서 `Condition` 요소에 와일드카드를 사용하지 않는 것이 좋습니다. 그렇지 않으면 파티션 (p. 564) 내 계정의 모든 IAM 사용자가 역할에 액세스할 수 있습니다.

추가 정보

자세한 내용은 다음을 참조하십시오.

- Amazon Simple Storage Service 개발자 가이드의 버킷 정책 예제
- Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 정책의 예
- Amazon Simple Queue Service 개발자 안내서의 Amazon SQS 정책 예제
- AWS Key Management Service Developer Guide의 키 정책
- AWS General Reference의 계정 식별자
- 웹 자격 증명 연동에 대하여 (p. 183)

AWS JSON 정책 요소: NotPrincipal

`NotPrincipal` 요소를 사용하여 IAM 사용자, 연합된 사용자, IAM 역할, AWS 계정, AWS 서비스 또는 그 밖에 리소스에 대한 액세스가 허용되거나 거부되지 않은 다른 보안 주체를 지정할 수 있습니다.

NotPrincipal 요소를 사용하면 보안 주체 목록에 예외를 지정할 수 있습니다. 이 요소를 사용하여 NotPrincipal 요소로 지정된 보안 주체를 제외하고모든 보안 주체에 대한 액세스를 거부할 수 있습니다. NotPrincipal 지정 구문은 AWS JSON 정책 요소: Principal (p. 589) 지정할 때와 동일합니다.

IAM 자격 증명 기반 정책에서는 NotPrincipal 요소를 사용할 수 없습니다. IAM 역할을 위한 신뢰 정책 및 리소스 기반 정책에서는 사용할 수 있습니다. 리소스 기반 정책은 IAM 리소스에 직접 삽입할 수 있는 정책입니다.

> **Important**
>
> NotPrincipal을 사용해야 하는 시나리오는 극히 드뭅니다. 따라서 NotPrincipal 사용을 결정하기 전에 다른 권한 부여 옵션을 살펴보는 것이 바람직합니다.

NotPrincipal다음으로 바꿉니다.Allow

따라서 "Effect": "Allow"와 동일한 정책 문에는 NotPrincipal을 사용하지 않는 것이 좋습니다. 사용하면 NotPrincipal 요소에 지정된 보안 주체를 제외하고 모든 보안 주체가 허용됩니다. 그러면 지정된 보안 주체를 제외한 모든 보안 주체에 정책 문에 지정된 권한이 부여되기 때문에 이렇게 하지 않는 것이 좋습니다. 익명(비인증) 사용자에게 액세스를 부여하게 될 수도 있기 때문입니다.

NotPrincipal다음으로 바꿉니다.Deny

"Effect": "Deny"와 동일한 정책 문에 NotPrincipal을 사용할 경우, 정책 문에 지정된 작업은 지정된 보안 주체를 제외한 모든 보안 주체에 대해 명시적으로 거부됩니다. 이 방법을 사용하여 화이트리스트를 구현할 수 있습니다. NotPrincipal과 Deny를 함께 사용할 경우, 거부되지 않은 보안 주체의 계정 ARN도 지정해야 합니다. 지정하지 않으면 정책에서 해당 보안 주체를 포함하는 전체 계정에 대한 액세스가 거부될 수 있습니다. 정책에 포함하는 서비스에 따라 AWS에서 먼저 계정을 검증한 후 사용자를 검증할 수 있습니다. 위임된 역할 사용자(역할을 사용하는 사람)를 평가할 때 AWS는 먼저 계정을 검증한 후 위임된 역할 사용자를 평가합니다. 위임된 역할 사용자는 그 역할을 위임 받을 때 지정된 역할 세션 이름으로 식별할 수 있습니다. 따라서 사용자 계정의 ARN을 명시적으로 포함시키거나, 역할의 ARN과 해당 역할을 포함하는 계정의 ARN을 모두 포함시킬 것을 권장합니다.

> **Note**
>
> 최선의 결과를 위해 정책에 계정의 ARN을 포함시켜야 합니다. 모든 경우에 해당하는 것은 아니지만 일부 서비스에서는 계정 ARN이 필요합니다. 기존 정책은 필요한 ARN 없이 계속 적용되지만 이러한 서비스를 포함하는 새 정책은 계정 ARN을 포함시켜야 합니다. IAM은 이러한 서비스를 추적하지 않으므로 계정 ARN을 항상 포함시키는 것이 좋습니다.

다음 예제들은 같은 정책 설명에 있는 NotPrincipal과 "Effect": "Deny"를 효과적으로 사용하는 방법을 보여줍니다.

Example 1: 같은 또는 다른 계정의 IAM 사용자

다음 예제에서는 AWS 계정 444455556666에서 Bob이라는 이름의 사용자만 제외하고 모든 보안 주체의 리소스 액세스가 명시적으로 거부되었습니다. 모범 사례로서 NotPrincipal 요소는 사용자 Bob과 Bob이 속한 AWS 계정(arn:aws:iam::444455556666:root)의 ARN을 모두 포함한다는 점을 유념하십시오. NotPrincipal 요소에 Bob의 ARN만 추가될 경우, 정책의 효과에 따라 사용자 Bob을 포함하는 AWS계정에 대한 액세스가 명시적으로 거부될 수 있습니다. 경우에 따라, 사용자는 자신의 상위 계정보다 많은 권한을 가질 수 없습니다. 따라서 Bob의 계정에 대한 액세스가 명시적으로 거부되면 Bob은 리소스에도 액세스하지 못할 수도 있습니다.

이 예제는 444455556666가 아닌 같은 또는 다른 AWS 계정의 리소스에 연결된 리소스 기반 정책의 정책 설명에 포함될 때 의도한 대로 작동합니다. 이 예제 자체로는 Bob에게 액세스 권한을 부여하지 않지만 명시적으로 거부된 보안 주체 목록에서 Bob만 제외됩니다. Bob에게 리소스 액세스 권한을 허용하려면 다른 정책 문으로 "Effect": "Allow"를 작성함으로써 액세스를 명시적으로 허용해야 합니다.

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

```
    "Statement": [{
        "Effect": "Deny",
        "NotPrincipal": {"AWS": [
            "arn:aws:iam::444455556666:user/Bob",
            "arn:aws:iam::444455556666:root"
        ]},
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3:::BUCKETNAME",
            "arn:aws:s3:::BUCKETNAME/*"
        ]
    }]
}
```

Example 2: 같은 또는 다른 계정의 IAM 역할

다음 예제에서는 AWS 계정 444455556666에서 cross-account-audit-app이라는 이름의 위임된 역할 사용자만 제외하고 모든 보안 주체의 리소스 액세스가 명시적으로 거부되었습니다. 모범 사례로서, `NotPrincipal` 요소는 수임된 역할 사용자(cross-account-audit-app), 역할(cross-account-read-only-role), 및 역할이 속한 AWS 계정(444455556666)의 ARN을 포함합니다. `NotPrincipal` 요소에 역할의 ARN이 누락될 경우 정책 효과에 따라 역할에 대한 액세스가 명시적으로 거부될 수 있습니다. 마찬가지로, `NotPrincipal` 요소에 역할이 속한 AWS 계정의 ARN이 누락될 경우에는 정책의 효과에 따라 AWS 계정과 그 계정의 모든 엔터티에 대한 액세스가 명시적으로 거부될 수 있습니다. 경우에 따라, 위임된 역할 사용자는 자신의 상위 역할보다 많은 권한을 가질 수 없고, 역할은 자신의 상위 AWS 계정보다 많은 권한을 가질 수 없습니다. 따라서 역할 또는 계정에 대한 액세스가 명시적으로 거부되면 위임된 역할 사용자는 리소스에 액세스하지 못할 수 있습니다.

이 예제는 444455556666이 아닌 다른 AWS 계정의 리소스에 연결된 정책 문이 리소스 기반 정책의 정책 문에 포함되기 때문에 의도한 대로 효과가 나타납니다. 이 예제 자체에서는 위임된 역할 사용자인 cross-account-audit-app에게 액세스를 허용하지 않지만 명시적으로 거부된 보안 주체 목록에서 cross-account-audit-app만 제외됩니다. cross-account-audit-app에게 리소스 액세스 권한을 부여하려면 다른 정책 문으로 `"Effect": "Allow"`를 작성함으로써 액세스를 명시적으로 허용해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Deny",
        "NotPrincipal": {"AWS": [
            "arn:aws:sts::444455556666:assumed-role/cross-account-read-only-role/cross-
account-audit-app",
            "arn:aws:iam::444455556666:role/cross-account-read-only-role",
            "arn:aws:iam::444455556666:root"
        ]},
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3:::Bucket_AccountAudit",
            "arn:aws:s3:::Bucket_AccountAudit/*"
        ]
    }]
}
```

`NotPrincipal` 요소에 위임된 역할 세션을 지정할 때 와일드카드(*)를 사용하여 “모든 세션”을 의미할 수 없습니다. 보안 주체는 항상 특정 세션의 이름을 지정해야 합니다.

IAM JSON 정책 요소: Action

`Action` 요소는 특정 작업의 허용 또는 거부 여부를 지정합니다. 문에는 `Action` 또는 `NotAction` 요소가 반드시 추가되어야 합니다. AWS 서비스마다 실행할 수 있는 작업을 설명한 목록이 있습니다. 예를 들어 Amazon S3 작업 목록은 Amazon Simple Storage Service 개발자 가이드의 정책에서 권한 지정에서, Amazon EC2 작업 목록은 Amazon EC2 API Reference에서, 그리고 AWS Identity and Access Management

작업 목록은 IAM API Reference에서 확인할 수 있습니다. 그 밖에 다른 서비스의 작업 목록은 해당 서비스의 API 참조 설명서를 참조하십시오.

서비스 네임스페이스를 작업 접두사(iam, ec2 sqs, sns, s3 등)로 사용하고 허용 또는 거부할 작업 이름을 사용하여 값을 지정합니다. 이름은 서비스에서 지원되는 작업과 일치해야 합니다. 접두사와 작업 이름은 대/소문자를 구분하지 않습니다. 예를 들어 `iam:ListAccessKeys`는 `IAM:listaccesskeys`와 동일합니다. 다음은 각 서비스의 `Action` 요소를 나타낸 예제입니다.

Amazon SQS 작업

```
"Action": "sqs:SendMessage"
```

Amazon EC2 작업

```
"Action": "ec2:StartInstances"
```

IAM 작업

```
"Action": "iam:ChangePassword"
```

Amazon S3 작업

```
"Action": "s3:GetObject"
```

`Action` 요소는 다수의 값을 지정할 수도 있습니다.

```
"Action": [ "sqs:SendMessage", "sqs:ReceiveMessage", "ec2:StartInstances",
 "iam:ChangePassword", "s3:GetObject" ]
```

특정 AWS 제품이 제공하는 모든 작업에 대해 액세스 권한을 부여하려면 와일드카드(*)를 사용하면 됩니다. 예를 들어, 다음 `Action` 요소는 모든 S3 작업에 적용됩니다.

```
"Action": "s3:*"
```

와일드카드(*)는 작업 이름에도 사용할 수 있습니다. 예를 들어 다음 `Action` 요소는 `CreateAccessKey`, `DeleteAccessKey`, `ListAccessKeys`, `UpdateAccessKey` 등 문자열 `AccessKey`를 포함하는 IAM 작업 모두에게 적용됩니다.

```
"Action": "iam:*AccessKey*"
```

일부 서비스에서는 사용 가능한 작업을 제한할 수도 있습니다. 예를 들어 Amazon SQS에서는 가능한 모든 Amazon SQS 작업의 하위 집합만 사용할 수 있습니다. 이 경우 와일드카드(*)는 대기열 전체를 제어하지 못하고, 공유한 작업의 하위 집합만 제어가 가능합니다. 자세한 내용은 Amazon Simple Queue Service 개발자 안내서의 Understanding Permissions 단원을 참조하십시오.

IAM JSON 정책 요소: NotAction

`NotAction`은 지정된 작업의 목록을 제외한 모든 작업과 명시적으로 일치하는 고급 정책 요소입니다. `NotAction`을 사용하면 일치하는 작업의 긴 목록을 포함하는 대신 일치하지 않는 몇몇 작업만 나열함으로써 정책을 줄일 수 있습니다. `NotAction`을 사용할 때는 이 요소에 지정된 작업들이 제한되는 유일한 작업이라는 점을 유의해야 합니다. 따라서 나열되지 않은 모든 해당 작업 또는 서비스가 `Allow` 효과를 사용할 경우 허용되고, `Deny`를 사용하려는 경우에는 나열되지 않은 작업 또는 서비스가 거부됩니다. `NotAction`을 `Resource` 요소와 함께 사용할 경우 정책 범위를 제공해야 합니다. 이에 따라 AWS는 어떤 작업이나 서비스를 적용할 수 있는지 결정합니다. 자세한 내용은 다음 예제 정책을 참조하십시오.

NotAction 및 Allow

설명문에서 `NotAction` 요소를 `"Effect": "Allow"`와 함께 사용하여 AWS 서비스에서 `NotAction`에 지정된 작업을 제외한 모든 작업에 대한 액세스 권한을 제공할 수 있습니다. 이 요소와 `Resource` 요소를 함께 사용하여 정책에 대한 범위를 제공하고 지정한 리소스에서 수행할 수 있는 작업으로만 작업을 제한할 수 있습니다.

다음 예제는 사용자에게 버킷 삭제를 제외하고 S3 리소스에서 수행할 수 있는 모든 Amazon S3 작업에 대한 액세스를 제공합니다. `ListAllMyBuckets` S3 API 작업은 "*" 리소스가 필요하기 때문에 이 작업은 사용자가 사용할 수 없습니다. 이 정책은 또한 다른 서비스에서의 작업을 허용하지 않습니다. 다른 서비스 작업은 S3 리소스에 적용되지 않기 때문입니다.

```
"Effect": "Allow",
"NotAction": "s3:DeleteBucket",
"Resource": "arn:aws:s3:::*",
```

때로는 다수의 작업에 액세스하도록 허용해야 할 수 있습니다. `NotAction` 요소를 사용하여 효과적으로 설명문을 반전시켜 작업 목록을 단축시킬 수 있습니다. 예를 들어 AWS 서비스는 종류가 다양하므로 사용자에게 IAM 작업에 대한 액세스를 제외한 모든 것을 허용하는 정책을 만들기를 원할 수 있습니다.

다음 예제는 사용자가 IAM을 제외한 모든 AWS 서비스에서 모든 작업에 액세스하도록 허용합니다.

```
"Effect": "Allow",
"NotAction": "iam:*",
"Resource": "*"
```

동일한 설명문에서 또는 동일한 정책의 다른 설명문에서 `NotAction` 요소와 `"Effect": "Allow"`를 사용할 경우 주의하십시오. `NotAction`은 명시적으로 나열되지 않거나 특정 리소스에 적용되지 않는 모든 서비스 및 작업과 일치하므로 사용자에게 의도한 것보다 많은 권한을 부여하는 결과를 가져올 수 있습니다.

NotAction 및 Deny

설명문에서 `NotAction` 요소를 `"Effect": "Deny"`와 함께 사용하여 `NotAction` 요소에 지정된 작업을 제외하고 모든 나열된 리소스에 대한 액세스를 거부할 수 있습니다. 이 조합은 나열된 항목을 허용하는 것이 아니라 나열되지 않은 작업을 명시적으로 거부합니다. 그러므로 허용하려는 작업은 별도로 허용해야 합니다.

다음의 조건부 예제는 사용자가 MFA를 사용하여 로그인하지 않은 경우 비 IAM 작업에 대한 액세스를 거부합니다. 사용자가 MFA를 사용하여 로그인한 경우에는 `"Condition"` 테스트에 실패하며 최종 `"Deny"` 문은 효과가 없습니다. 단, 이 정책은 사용자에게 작업에 대한 액세스 권한을 부여하는 것이 아니라 IAM 작업을 제외한 다른 모든 작업을 명시적으로 거부할 뿐입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DenyAllUsersNotUsingMFA",
        "Effect": "Deny",
        "NotAction": "iam:*",
        "Resource": "*",
        "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": "false"}}
    }]
}
```

다음 예제 정책은 나열된 서비스의 작업을 제외하고 `eu-central-1` 및 `eu-west-1` 리전 외부의 작업에 대한 액세스를 거부합니다. `NotActions` 요소에 나열된 서비스는 `us-east-1` 리전에 실제로 단일 엔드포인트가 있는 AWS 글로벌 서비스의 일부입니다. 그렇지 않다면 이러한 서비스의 작업은 실패할 것입니다. 이 정책은 액세스를 거부하고 다른 정책이 액세스 권한을 부여하도록 요구합니다. 예시 정책을 보려면 AWS: 요청된 리전에 따라 AWS에 대한 액세스를 거부 (p. 400) 단원을 참조하십시오.

IAM JSON 정책 요소: Resource

`Resource` 요소는 문에서 다루는 객체를 지정합니다. 문에는 `Resource` 또는 `NotResource` 요소가 반드시 추가되어야 합니다. 리소스는 ARN을 사용하여 지정할 수 있습니다. ARL의 형식에 대한 자세한 내용은 IAM ARN (p. 564) 단원을 참조하십시오.

각 서비스마다 고유의 리소스가 있습니다. 리소스를 지정하려면 항상 ARN을 사용해야 하지만 리소스의 ARN 세부 정보는 서비스와 리소스에 따라 달라집니다. 리소스 지정 방법에 대한 자세한 내용은 문을 작성하려는 리소스의 서비스 설명서를 참조하십시오.

> **Note**
>
> 서비스 중에는 개별적인 리소스로 작업을 지정하지 못하는 서비스도 있습니다. 대신 `Action` 또는 `NotAction` 요소로 나열하는 작업이 모두 해당 서비스의 모든 리소스에 적용됩니다. 이 경우에는 `*` 요소에 와일드카드(`Resource`)를 사용합니다.

다음은 특정 Amazon SQS 대기열을 나타낸 예제입니다.

```
"Resource": "arn:aws:sqs:us-east-2:account-ID-without-hyphens:queue1"
```

다음은 AWS 계정에서 Bob이라는 이름의 IAM 사용자를 나타내는 예제입니다.

```
"Resource": "arn:aws:iam::account-ID-without-hyphens:user/Bob"
```

와일드카드는 리소스 ARN에도 사용할 수 있습니다. ARN 세그먼트(콜론으로 구분된 부분) 내에서 와일드카드 문자(* 및 ?)를 사용할 수 있습니다. 별표(*)는 0개 이상의 문자 조합을 나타내고 물음표(?)는 단일 문자를 나타냅니다. * 또는 ? 문자를 각 세그먼트에서 여러 번 사용할 수 있지만, 와일드카드 한 개를 여러 세그먼트에 걸쳐서 적용할 수는 없습니다. 다음은 경로가 `/accounting`인 IAM 사용자를 모두 나타낸 예제입니다.

```
"Resource": "arn:aws:iam::account-ID-without-hyphens:user/accounting/*"
```

다음은 특정 Amazon S3 버킷 내에 포함된 모든 항목을 나타낸 예제입니다.

```
"Resource": "arn:aws:s3:::my_corporate_bucket/*"
```

다수의 리소스를 지정할 수도 있습니다. 다음은 DynamoDB 테이블을 2개 나타낸 예제입니다.

```
"Resource": [
    "arn:aws:dynamodb:us-east-2:account-ID-without-hyphens:table/books_table",
    "arn:aws:dynamodb:us-east-2:account-ID-without-hyphens:table/magazines_table"
]
```

`Resource` 요소에서 ARN의 부분에 JSON 정책 변수 (p. 615)를 사용하여 특정 리소스를 식별할 수 있습니다(ARN의 끝 부분에 사용). 예를 들어 `{aws:username}` 키를 리소스 ARN에 사용하여 현재 사용자의 이름을 리소스 이름에 추가해야 한다는 것을 나타낼 수 있습니다. 다음은 `{aws:username}` 요소에서 `Resource` 키를 사용하는 방법을 나타낸 예제입니다. 이 정책에서는 현재 사용자 이름과 일치하는 Amazon DynamoDB 테이블에 대한 액세스가 허용됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-2:ACCOUNT-ID-WITHOUT-HYPHENS:table/
${aws:username}"
  }
}
```

JSON 정책 변수에 대한 자세한 내용은 IAM 정책 요소: 변수 및 태그 (p. 615) 단원을 참조하십시오.

IAM JSON 정책 요소: NotResource

NotResource는 지정된 리소스를 제외한 모든 리소스와 명시적으로 일치하는 고급 정책 요소입니다. NotResource를 사용하면 일치하는 리소스의 긴 목록을 포함하는 대신 일치하지 않는 몇몇 리소스만 나열함으로써 정책을 줄일 수 있습니다. 이는 단일 AWS 서비스 내에서 적용되는 정책에 특히 유용합니다.

예를 들어 HRPayroll라는 이름의 그룹이 있다고 가정하겠습니다. 그리고 HRPayroll 멤버는 HRBucket 버킷의 Payroll 폴더를 제외하고 모든 Amazon S3 리소스에 액세스할 수 없습니다. 다음 정책은 나열된 리소스 이외의 모든 Amazon S3 리소스에 대한 액세스를 거부합니다. 단, 이 정책은 사용자에게 리소스에 대한 액세스 권한을 부여하는 것이 아닙니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "NotResource": [
      "arn:aws:s3:::HRBucket/Payroll",
      "arn:aws:s3:::HRBucket/Payroll/*"
    ]
  }
}
```

일반적으로 리소스에 대한 액세스를 명시적으로 거부하려면 "Effect":"Deny"를 사용하고 각 폴더를 개별적으로 나열하는 Resource 요소를 포함하는 정책을 작성합니다. 하지만 이때 사용자가 HRBucket에 폴더를 추가하거나 액세스하면 안 되는 Amazon S3에 리소스를 추가할 때마다 그 이름 역시 Resource 목록에 추가해야 합니다. 그렇지 않고 NotResource 요소를 사용할 때는 폴더 이름을 NotResource 요소에 추가하지 않더라도 사용자가 새 폴더에 대한 액세스 권한이 자동으로 거부됩니다.

NotResource를 사용할 때는 이 요소에 지정된 리소스가 제한되지 않는 유일한 리소스라는 점을 명심해야 합니다. 이렇게 하면 작업에 적용되는 모든 리소스가 제한됩니다. 위의 예에서 정책은 Amazon S3 작업에만 적용되므로 Amazon S3 리소스에만 영향을 미칩니다. 작업에도 Amazon EC2 작업이 포함되어 있으면 정책에서 EC2 리소스에 대한 액세스를 거부하지 않습니다. 또한 이 정책은 s3:ListAllMyBuckets와 같은 특정 리소스에서 수행할 수 없는 S3 작업에 대한 액세스를 거부하지 않습니다. 서비스에서 리소스의 ARN을 지정할 수 있는 작업에 대한 자세한 내용은 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

다른 요소가 있는 NotResource

"Effect": "Allow", "Action": "*" 및 "NotResource": "arn:aws:s3:::HRBucket" 요소를 함께 사용하면 안 됩니다. 이 문은 HRBucket S3 버킷을 제외한 모든 리소스에 대해 AWS의 모든 작업을 허용하므로 매우 위험합니다. 이렇게 하면 HRBucket에 액세스할 수 있는 정책을 사용자가 직접 추가할 수 있으므로 주의해야 합니다.

동일한 설명문에서 또는 동일한 정책의 다른 설명문에서 NotResource 요소와 "Effect": "Allow"를 사용할 경우 주의하십시오. NotResource은 명시적으로 나열되지 않은 모든 서비스 및 작업을 허용하므로 사용자에게 의도한 것보다 많은 권한을 부여하는 결과를 가져올 수 있습니다. 동일한 설명문에서 NotResource 요소와 "Effect": "Deny"를 사용하면 명시적으로 나열되지 않은 서비스 및 리소스를 거부합니다.

IAM JSON 정책 요소: Condition

Condition 요소(또는 Condition 블록)를 사용하여 정책의 효력이 발생하는 시점에 대한 조건을 지정할 수 있습니다. Condition 요소는 선택 사항입니다. Condition 요소에서 조건 연산자 (p. 601)(같음, 보다 작음 등)를 사용하여 정책의 조건 키 및 값을 요청 컨텍스트의 키 및 값과 일치시키는 표현식을 작성합니다. 요청 컨텍스트에 대한 자세한 내용은 요청 (p. 5) 단원을 참조하십시오.

```
"Condition" : { "{condition-operator}" : { "{condition-key}" : "{condition-value}" }}
```

지정하는 조건 키는 전역 조건 키 (p. 650) 또는 서비스별 조건 키일 수 있습니다. 전역 조건 키에는 aws: 접두사가 있습니다. 서비스별 조건 키에는 서비스 접두사가 있습니다. 예를 들어, Amazon EC2를 사용하면 ec2:InstanceType 키를 사용하여 해당 서비스에 고유한 조건을 작성할 수 있습니다. iam: 접두사가 있는 서비스별 IAM 조건 키를 보려면 IAM 및 AWS STS 조건 컨텍스트 키 (p. 664) 단원을 참조하십시오.

조건 키 이름은 대/소문자를 구분하지 않습니다. 예를 들어 aws:SourceIP 조건 키를 포함시키는 것은 AWS:SourceIp에 대한 테스트와 동일합니다. 조건 키 값의 대/소문자 구분은 사용하는 조건 연산자 (p. 601)에 따라 다릅니다. 예를 들어 다음 조건에는 StringEquals 연산자가 포함되어 johndoe에서 생성하는 요청만 일치하도록 합니다. 이름이 JohnDoe인 사용자는 액세스가 거부됩니다.

```
"Condition" : { "StringEquals" : { "aws:username" : "johndoe" }}
```

다음 조건은 StringEqualsIgnoreCase (p. 602) 연산자를 사용하여 이름이 johndoe 또는 JohnDoe인 사용자와 일치합니다.

```
"Condition" : { "StringEqualsIgnoreCase" : { "aws:username" : "johndoe" }}
```

일부 조건 키는 키 이름의 특정 부분을 지정하도록 허용하는 키-값 페어를 지원합니다. aws:RequestTag/*tag-key* (p. 650) 전역 조건 키, AWS KMS kms:EncryptionContext:*encryption_context_key* 및 여러 서비스에서 지원하는 ResourceTag/*tag-key* 조건 키가 그 예입니다. Amazon EC2와 같은 서비스에 대해 ResourceTag/*tag-key* 조건 키를 사용하는 경우 tag-key에 대한 키 이름을 지정해야 합니다. 키 이름은 대/소문자를 구분하지 않습니다. 따라서 정책의 조건 요소에서 "ec2:ResourceTag:TagKey1": "Value1" 지정을 수행한 경우 조건은 이름이 TagKey1 또는 tagkey1인 리소스 태그 키와 일치하지만, 두 가지 모두와 일치하지는 않습니다. 이러한 속성을 지원하는 AWS 서비스를 통해 대소문자만 다른 여러 키 이름을 생성할 수 있습니다. 예를 들어 foo=bar1과 Foo=bar2 를 사용해 Amazon EC2 인스턴스에 태그를 지정하는 경우가 여기에 해당합니다. "ec2:ResourceTag:Foo": "bar1" 같은 조건을 사용하여 리소스에 대한 액세스를 허용하는 경우 키 이름은 두 태그 모두와 일치하지만, 하나의 값만 일치합니다. 이로 인해 예기치 않은 조건 실패가 발생할 수 있습니다.

> **Important**
>
> 모범 사례로서 키-값 페어 속성 이름을 지정할 때 계정의 멤버가 일관적인 명명 규칙을 따르도록 해야 합니다. 예를 들어 태그 또는 AWS KMS 암호화 컨텍스트가 여기에 해당합니다. 태그 지정에 대해 aws:TagKeys (p. 662) 조건 키를 사용하거나 AWS KMS 암호화 컨텍스트에 대해 kms:EncryptionContextKeys 사용을 통해 이를 적용할 수 있습니다.

- 모든 조건 연산자의 목록과 각 연산자의 작동 방식에 대한 설명을 보려면 조건 연산자 (p. 601)를 참조하십시오.
- 달리 지정하지 않는 경우 모든 키는 다수의 값을 가질 수 있습니다. 복수 값을 가진 조건 키를 취급하는 방법에 대한 설명은 다수의 키 또는 값을 사용하는 조건 생성 (p. 608) 부분을 참조하십시오.
- 전역에서 사용 가능한 모든 조건 키의 목록은 AWS 전역 조건 컨텍스트 키 (p. 650) 단원을 참조하십시오.
- 각 서비스에서 정의된 조건 키는 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오.

요청 컨텍스트

보안 주체 (p. 5)가 AWS에 요청 (p. 5)하면 AWS는 요청 정보를 요청 컨텍스트로 수집합니다. 이 정보는 요청을 평가하고 승인하는 데 사용됩니다. JSON 정책의 Condition 요소를 사용하여 요청 컨텍스트에 대해 특정 조건을 테스트할 수 있습니다. 예를 들어, 사용자가 업무 시간 중에만 특정 작업을 수행할 수 있도록 (p. 390) aws:CurrentTime (p. 653) 조건 키를 사용하는 정책을 생성할 수 있습니다.

요청이 제출되면 AWS는 정책의 각 조건 키를 평가하여 true, false, not present, 때로는 null(빈 데이터 문자열) 값을 반환합니다. 요청에 없는 키는 불일치로 간주되지 않습니다. 예를 들어, 다음 정책에서는 지난 1시간(3,600초) 동안 MFA를 사용하여 로그인한 경우에만 자체 MFA(Multi-Factor Authentication) 디바이스를 제거할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "AllowRemoveMfaOnlyIfRecentMfa",
        "Effect": "Allow",
        "Action": [
            "iam:DeactivateMFADevice",
            "iam:DeleteVirtualMFADevice"
        ],
        "Resource": "arn:aws:iam::*:user/${aws:username}",
        "Condition": {
            "NumericLessThanEquals": {"aws:MultiFactorAuthAge": "3600"}
        }
    }
}
```

요청 컨텍스트는 다음 값을 반환할 수 있습니다.

- True – 요청자가 지난 1시간 이내에 MFA를 사용하여 로그인한 경우 조건은 true를 반환합니다.
- False – 요청자가 1시간 이전에 MFA를 사용하여 로그인한 경우 조건은 false를 반환합니다.
- Not present – 요청자가 AWS CLI 또는 AWS API에서 IAM 사용자 액세스 키를 사용하여 요청한 경우 키가 존재하지 않습니다. 이 경우 키가 존재하지 않으므로 일치하지 않습니다.
- Null – 요청에 태그를 전달하는 등 사용자가 정의한 조건 키의 경우 빈 문자열을 포함할 수 있습니다. 이 경우 요청 컨텍스트의 값은 null입니다. 경우에 따라 null 값이 true를 반환할 수 있습니다. 예를 들어, `aws:TagKeys (p. 662)` 조건 키와 함께 다중 값 `ForAllValues (p. 610)` 조건 연산자를 사용하는 경우 요청 컨텍스트가 null을 반환하면 예기치 않은 결과가 발생할 수 있습니다. 자세한 내용은 aws:TagKeys (p. 662) 및 다수의 키와 값 사용 (p. 610) 단원을 참조하십시오.

조건 블록

다음은 `Condition` 요소의 기본 형식을 나타낸 예제입니다.

```
"Condition": {
  "DateGreaterThan" : {
     "aws:CurrentTime" : "2013-12-15T12:00:00Z"
   }
}
```

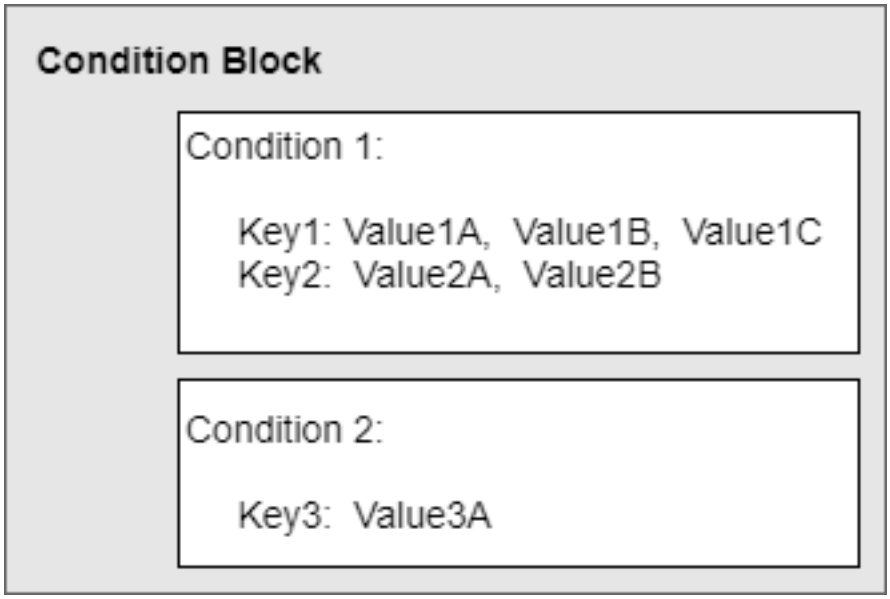
요청 값은 키로 나타내며, 여기에서는 `aws:CurrentTime`이 요청 값에 해당합니다. 키 값은 나중에 설명하겠지만 리터럴 값(`2013-08-16T12:00:00Z`) 또는 정책 변수로 지정하는 값과 비교됩니다. 비교 유형은 조건 연산자 (p. 601)에서 지정합니다(여기서는 `DateGreaterThan`). equals, greater than 및 less than과 같은 일반적인 부울 비교를 사용하여 문자열, 날짜, 숫자 등을 비교하는 조건을 만들 수 있습니다.

키에 다수의 값을 추가할 수 있는 경우도 있습니다. 예를 들어 Amazon DynamoDB에 대한 요청에서는 다수의 테이블 속성 반환이나 업데이트를 요청할 수 있습니다. DynamoDB 테이블에 대한 액세스 정책에 따르면 `dynamodb:Attributes` 키를 추가하여 요청 시 나열되는 모든 속성 저장이 가능합니다. `Condition` 요소의 설정 연산자를 사용하여 정책에 허용된 속성 목록과 요청에 포함된 속성 여러 가지를 비교함으로써 테스트할 수 있습니다. 자세한 내용은 다수의 키 또는 값을 사용하는 조건 생성 (p. 608) 단원을 참조하십시오.

요청 단계에서 정책을 평가할 때는 AWS가 키를 해당하는 요청 값으로 변환합니다. (이 예제에서는 AWS가 요청 날짜와 시간을 사용합니다). 조건 평가에 따라 true 또는 false가 반환되고, 이후 이 조건 평가 결과를 고려하여 정책 전반적인 요청 허용 또는 거부 여부를 결정합니다.

다수의 조건 값

`Condition` 요소에는 여러 조건을 추가할 수 있으며, 다시 한 번 각 조건마다 다수의 키-값 페어가 포함됩니다. 다음은 이것을 설명한 그림입니다.



자세한 내용은 다수의 키 또는 값을 사용하는 조건 생성 (p. 608) 단원을 참조하십시오.

IAM JSON; 정책 요소: 조건 연산자

`Condition` 요소의 조건 연산자를 사용하여 정책의 조건 키 및 값을 요청 컨텍스트의 값과 일치시킵니다. `Condition` 요소에 대한 자세한 내용은 IAM JSON 정책 요소: Condition (p. 598)을 참조하십시오.

정책에서 사용할 수 있는 조건 연산자는 선택한 조건 키에 따라 다릅니다. 전역 조건 키 또는 서비스별 조건 키를 선택할 수 있습니다. 전역 조건 키에 사용할 수 있는 조건 연산자를 알아보려면 AWS 전역 조건 컨텍스트 키 (p. 650) 단원을 참조하십시오. 서비스별 조건 키에 사용할 수 있는 조건 연산자를 알아보려면 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하고 보려는 서비스를 선택하십시오.

> **Important**
>
> 정책 조건에서 지정한 키가 요청 컨텍스트에 없으면 값이 일치하지 않습니다. 이는 ...IfExists (p. 607) 및 Null check (p. 608)를 제외한 모든 조건 연산자에 적용됩니다. 이 연산자는 키가 요청 컨텍스트에 존재하는지 여부를 테스트합니다.

조건 연산자는 다음 범주로 그룹화할 수 있습니다.

- 문자열 (p. 602)
- 숫자 (p. 603)
- 날짜 및 시간 (p. 604)
- 부울 (p. 604)
- Binary (p. 605)
- IP 주소 (p. 605)
- Amazon 리소스 이름(ARN) (p. 606)(일부 서비스에서만 사용 가능.)
- ...IfExists (p. 607)(키 값이 다른 확인을 위해 존재하는지 여부를 확인)
- Null 확인 (p. 608)(키 값이 단독 확인을 위해 존재하는지 여부를 확인)

문자열 조건 연산자

문자열 조건 연산자를 사용하여 키와 문자열 값을 비교한 결과에 따라 액세스를 제한하는 `Condition` 요소를 생성할 수 있습니다.

조건 연산자	설명
`StringEquals`	정확한 일치, 대소문자 구분
`StringNotEquals`	불일치
`StringEqualsIgnoreCase`	정확한 일치, 대소문자 무시
`StringNotEqualsIgnoreCase`	불일치, 대소문자 무시
`StringLike`	대소문자 구분 일치. 문자열 어디에서나 다중 문자 매칭 와일드카드(*) 또는 단일 문자 매칭 와일드카드(?)를 값에 포함할 수 있습니다. **Note** 키에 다수의 값이 저장되는 경우에는 설정 연산자 - `ForAllValues:StringLike` 및 `ForAnyValue:StringLike`를 사용해 `StringLike`를 한정할 수 있습니다. 자세한 정보는 다수의 키 또는 값을 사용하는 조건 생성 (p. 608) 단원을 참조하십시오.
`StringNotLike`	대소문자 구분 불일치. 문자열 어디에서나 다중 문자 매칭 와일드카드(*) 또는 단일 문자 매칭 와일드카드(?)를 값에 포함할 수 있습니다.

예를 들어, 다음 문에는 `StringEquals` 조건 연산자를 `aws:PrincipalTag` 키와 함께 사용하여 요청을 수행하는 보안 주체에게 `iamuser-admin` 작업 범주에서 태그를 지정하도록 지정하는 `Condition` 요소가 포함되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:*AccessKey*",
    "Resource": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:user/*",
    "Condition": {"StringEquals": {"aws:PrincipalTag/job-category": "iamuser-admin"}}
  }
}
```

정책 조건에서 지정한 키가 요청 컨텍스트에 없으면 값이 일치하지 않습니다. 이 예제에서는 보안 주체가 태그가 연결된 IAM 사용자를 사용하는 경우 `aws:PrincipalTag/job-category` 키가 요청 컨텍스트에 존재합니다. 이는 태그 또는 세션 태그가 연결된 IAM 역할을 사용하는 보안 주체를 위해 포함된 것이기도 합니다. 태그가 없는 사용자가 액세스 키를 보거나 편집하려고 하면 조건이 `false`을 반환하고 요청이 이 문에 의해 묵시적으로 거부됩니다.

다음은 정책 변수 (p. 615)와의 문자열 일치를 수행하는 `StringLike` 조건 연산자를 사용하여 정책을 만드는 예제입니다. 이 정책에서는 IAM 사용자가 Amazon S3 콘솔을 사용하여 Amazon S3 버킷에 있는 자신의 '홈 디렉터리'를 관리할 수 있습니다. 이 정책은 `s3:prefix`가 지정된 패턴 중 하나와 일치하는 경우 S3 버킷에서 지정된 작업을 허용합니다.

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

```
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::BUCKET-NAME",
      "Condition": {"StringLike": {"s3:prefix": [
        "",
        "home/",
        "home/${aws:username}/"
      ]}}
    },
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::BUCKET-NAME/home/${aws:username}",
        "arn:aws:s3:::BUCKET-NAME/home/${aws:username}/*"
      ]
    }
  ]
}
```

웹 자격 증명 연동 시 `Condition` 요소를 사용하여 애플리케이션 ID와 사용자 ID에 따라 리소스 액세스를 제한하는 방법을 나타낸 정책 예는 Amazon S3: Amazon Cognito 사용자가 자신의 버킷에 있는 객체에 액세스할 수 있도록 허용 (p. 429) 단원을 참조하십시오.

숫자 조건 연산자

숫자 조건 연산자를 사용하여 키와 정수 또는 십진수 값을 비교한 결과에 따라 액세스를 제한하는 `Condition` 요소를 생성할 수 있습니다.

조건 연산자	설명
`NumericEquals`	일치
`NumericNotEquals`	불일치
`NumericLessThan`	"미만" 일치
`NumericLessThanEquals`	"이하" 일치
`NumericGreaterThan`	"초과" 일치
`NumericGreaterThanEquals`	"이상" 일치

예를 들어, 다음 문에는 `NumericLessThanEquals` 조건 연산자에 `s3:max-keys` 키를 사용하여 요청자가 `example_bucket`에서 한 번에 최대 10개까지 객체를 나열할 수 있다고 지정하는 `Condition` 요소가 포함되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
```

```
    "Resource": "arn:aws:s3:::example_bucket",
    "Condition": {"NumericLessThanEquals": {"s3:max-keys": "10"}}
  }
}
```

정책 조건에서 지정한 키가 요청 컨텍스트에 없으면 값이 일치하지 않습니다. 이 예제에서는`ListBucket` 작업을 수행할 때 요청에 `s3:max-keys` 키가 항상 존재합니다. 이 정책에서 모든 Amazon S3 작업을 허용한 경우에는 값이 10 이하인 `max-keys` 컨텍스트 키를 포함하는 작업만 허용됩니다.

날짜 조건 연산자

날짜 조건 연산자를 사용하여 키와 날짜/시간 값을 비교한 결과에 따라 액세스를 제한하는 `Condition` 요소를 생성할 수 있습니다. 이러한 조건 연산자는 `aws:CurrentTime` 키 또는 `aws:EpochTime` 키와 함께 사용합니다. 날짜/시간 값은 ISO 8601 날짜 형식의 W3C 구현 값 하나로 혹은 epoch(UNIX) 시간 로 지정해야 합니다.

> **Note**
>
> 날짜 조건 연산자에는 와일드카드를 사용할 수 없습니다.

조건 연산자	설명
`DateEquals`	특정 날짜 일치
`DateNotEquals`	불일치
`DateLessThan`	특정 날짜/시간 이전에 일치
`DateLessThanEquals`	특정 날짜/시간 또는 이전에 일치
`DateGreaterThan`	특정 날짜/시간 이후에 일치
`DateGreaterThanEquals`	특정 날짜/시간 또는 이후에 일치

예를 들어, 다음 문에는 `aws:TokenIssueTime` 키와 함께 `DateLessThan` 조건 연산자를 사용하는 `Condition` 요소가 포함되어 있습니다. 이 조건은 요청을 생성하는 데 사용된 임시 보안 자격 증명이 2020년에 발급되었음을 지정합니다. 계정 멤버가 새로운 자격 증명을 사용하도록 매일 프로그래밍 방식으로 이 정책을 업데이트할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:*AccessKey*",
    "Resource": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:user/*",
    "Condition": {"DateGreaterThan": {"aws:TokenIssueTime": "2020-01-01T00:00:01Z"}}
  }
}
```

정책 조건에서 지정한 키가 요청 컨텍스트에 없으면 값이 일치하지 않습니다. `aws:TokenIssueTime` 키는 사용자가 임시 자격 증명을 사용하여 요청을 생성하는 경우에만 요청 컨텍스트에 존재합니다. 액세스 키를 사용하는 AWS CLI, AWS API 또는 AWS SDK 요청에는 이 키가 존재하지 않습니다. 이 예제에서 IAM 사용자가 액세스 키를 보거나 편집하려고 하면 요청이 거부됩니다.

부울 조건 연산자

부울 조건을 사용하여 키를 "true" 또는 "false"와 비교하고 그에 따라 액세스를 제한하는 `Condition` 요소를 생성할 수 있습니다.

조건 연산자	설명
Bool	부울 일치

예를 들어, 다음 문은 Bool 조건 연산자에 aws:SecureTransport 키를 사용하여 요청에 SSL을 사용해야 한다고 지정하고 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:*AccessKey*",
    "Resource": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:user/*",
    "Condition": {"Bool": {"aws:SecureTransport": "true"}}
  }
}
```

정책 조건에서 지정한 키가 요청 컨텍스트에 없으면 값이 일치하지 않습니다. aws:SecureTransport 키는 항상 요청 컨텍스트에 존재합니다.

이진 조건 연산자

BinaryEquals 조건 연산자를 사용하면 이진 형식의 키 값을 테스트하는 Condition 요소를 생성할 수 있습니다. 지정한 키 값을 정책 내 이진 값의 base-64 인코딩 표시와 바이트 단위(byte for byte)로 비교합니다.

```
"Condition" : {
  "BinaryEquals": {
    "key" : "QmluYXJ5VmFsdWVJbkJhc2U2NA=="
  }
}
```

정책 조건에서 지정한 키가 요청 컨텍스트에 없으면 값이 일치하지 않습니다.

IP 주소 조건 연산자

IP 주소 조건 연산자를 사용하여 IPv4/IPv6 주소 또는 IP 주소 범위와 키를 비교한 결과에 따라 액세스를 제한하는 Condition 요소를 생성할 수 있습니다. 이 조건에는 aws:SourceIp 키가 사용됩니다. 값은 표준 CIDR 형식(예: 203.0.113.0/24 또는 2001:DB8:1234:5678::/64)을 따라야 합니다. 연결된 라우팅 접두사 없이 IP 주소를 지정하면 IAM은 기본 접두사 값 /32를 사용합니다.

일부 AWS 서비스는 0의 범위를 나타내기 위해 ::을 사용해 IPv6를 지원합니다. 서비스가 IPv6를 지원하는지 여부를 확인하려면 서비스 설명서를 참조하십시오.

조건 연산자	설명
IpAddress	지정된 IP 주소 또는 범위
NotIpAddress	지정된 IP 주소 또는 범위를 제외한 모든 IP 주소

예를 들어, 다음 문은 IpAddress 조건 연산자에 aws:SourceIp 키를 사용하여 IP 범위 203.0.113.0 - 203.0.113.255에서 요청이 전송되어야 한다고 지정하고 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
```

```
    "Action": "iam:*AccessKey*",
    "Resource": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:user/*",
    "Condition": {"IpAddress": {"aws:SourceIp": "203.0.113.0/24"}}
  }
}
```

`aws:SourceIp` 조건 키는 요청이 전송되는 IP 주소를 확인합니다. 요청이 Amazon EC2 인스턴스에서 전송된 경우에는 `aws:SourceIp`가 인스턴스의 퍼블릭 IP 주소로 계산되어야 합니다.

정책 조건에서 지정한 키가 요청 컨텍스트에 없으면 값이 일치하지 않습니다. `aws:SourceIp` 키는 요청자가 VPC 엔드포인트를 사용하여 요청을 생성한 경우를 제외하고 요청 컨텍스트에 항상 존재합니다. 이 경우 조건이 `false`를 반환하고 요청이 이 문에 의해 묵시적으로 거부됩니다.

다음 예제에서는 IPv4와 IPv6 주소를 혼합하여 조직의 유효 IP 주소를 모두 표현하는 방법을 보여줍니다. IPv6으로 전환하는 동안 조직의 정책이 계속 적용되도록 하려면 기존의 IPv4 주소 범위에 IPv6 범위를 더하여 정책을 보완하는 것이 좋습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "someservice:*",
    "Resource": "*",
    "Condition": {
      "IpAddress": {
        "aws:SourceIp": [
          "203.0.113.0/24",
          "2001:DB8:1234:5678::/64"
        ]
      }
    }
  }
}
```

사용자 자격으로 직접 테스트한 API를 호출하는 경우 `aws:SourceIp` 조건 키는 JSON 정책에서만 작동합니다. 서비스를 사용하여 사용자를 대신해 대상 서비스를 호출하는 경우, 대상 서비스는 원래 사용자의 IP 주소 대신 호출 서비스의 IP 주소를 봅니다. 이러한 상황은 예를 들어 AWS CloudFormation을 사용하여 인스턴스를 생성하는 Amazon EC2를 호출하는 경우에 발생할 수 있습니다. 현재로서는 JSON 정책에 따라 평가하기 위해 원본 IP 주소를 호출 서비스를 통해 대상 서비스로 보낼 방법이 없습니다. 이러한 서비스 API 호출 유형의 경우 `aws:SourceIp` 조건 키를 사용하지 마십시오.

Amazon 리소스 이름(ARN) 조건 연산자

Amazon 리소스 이름(ARN) 조건 연산자를 사용하면 키와 ARN을 비교한 결과에 따라 액세스를 제한하는 `Condition` 요소를 생성할 수 있습니다. ARN은 문자열로 알려져 있습니다. 모든 서비스가 이 연산자를 사용하여 ARN 비교를 지원하는 것은 아닙니다. ARN 조건 연산자가 작동하지 않으면 문자열 조건 연산자 (p. 602)를 사용해 보십시오.

조건 연산자	설명
`ArnEquals`, `ArnLike`	ARN 대소문자 구분 일치. ARN에서 콜론으로 구분된 구성요소 6개는 각각 별도로 확인하며, 다중 문자 매칭 와일드카드(*) 또는 단일 문자 매칭 와일드카드(?)가 추가될 수 있습니다. 이들은 동일하게 동작합니다.
`ArnNotEquals`, `ArnNotLike`	ARN 불일치. 이들은 동일하게 동작합니다.

다음의 리소스 기반 정책 예제는 SNS 메시지를 전송하고 싶은 Amazon SQS 대기열에 연결된 정책을 보여줍니다. 이 예제에서는 선택한 대기열로 메시지를 전송할 수 있는 권한을 Amazon SNS에 부여하고 있습니

다. 단, 서비스에서 특정 Amazon SNS 주제와 관련하여 메시지를 전송하는 경우로 제한됩니다. 대기열을 `Resource` 필드에, 그리고 Amazon SNS 주제는 `SourceArn` 키 값으로 지정합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"AWS": "123456789012"},
    "Action": "SQS:SendMessage",
    "Resource": "arn:aws:sqs:REGION:123456789012:QUEUE-ID",
    "Condition": {"ArnEquals": {"aws:SourceArn": "arn:aws:sns:REGION:123456789012:TOPIC-
ID"}}
  }
}
```

정책 조건에서 지정한 키가 요청 컨텍스트에 없으면 값이 일치하지 않습니다. `aws:SourceArn` 키는 리소스가 리소스 소유자를 대신하여 다른 서비스를 호출하도록 서비스를 트리거하는 경우에만 요청 컨텍스트에 존재합니다. IAM 사용자가 이 작업을 직접 수행하려고 하면 조건이 `false`을 반환하고 요청이 이 문에 의해 묵시적으로 거부됩니다.

IfExists 조건 연산자

`Null` 조건 - 예를 들어 `StringLikeIfExists`를 제외한 모든 조건 연산자 이름 끝에 `IfExists`를 추가할 수 있습니다. 이렇게 하면 "요청 콘텍스트에 정책 키가 있으면 정책에 지정된 대로 키를 처리하고, 키가 없으면 조건 요소를 true로 평가합니다." 문의 다른 조건 요소는 여전히 불일치한 결과를 발생시킬 수 있지만 `...IfExists`로 확인하면 누락되는 키는 없습니다.

`IfExists` 사용 예제

대부분 조건 키는 특정 형식의 리소스 정보를 의미하기 때문에 해당 형식의 리소스에 액세스할 때만 존재합니다. 이러한 조건 키는 다른 형식의 리소스에는 표시되지 않습니다. 그렇다고 정책 문이 한 가지 형식의 리소스에만 적용된다고 해서 문제가 되지는 않습니다. 하지만 정책 문이 여러 서비스의 작업을 참조하는 경우나, 혹은 한 가지 서비스 내에서 임의의 작업이 동일한 서비스에서 여러 가지 다른 리소스 형식에 액세스하는 경우처럼 단일 문이 여러 유형의 리소스에 적용될 수 있는 경우도 있습니다. 이런 경우 오직 한 가지 리소스에만 적용되는 조건 키를 정책 문에 추가하면 정책 문의 `Condition` 요소를 충족하지 못하고 결국 `"Effect"`가 적용되지 않습니다.

예를 들어 다음과 같은 정책 예제를 살펴보십시오.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "THISPOLICYDOESNOTWORK",
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": "*",
    "Condition": {"StringLike": {"ec2:InstanceType": [
      "t1.*",
      "t2.*",
      "m3.*"
    ]}}
  }
}
```

위 정책은 사용자가 t1, t2 또는 m3 형식의 인스턴스를 모두 실행할 수 있도록 하는 것이 목적입니다. 하지만 실제로 인스턴스를 실행하려면 인스턴스 외에도 이미지, 키 페어, 보안 그룹 등 다양한 리소스에 액세스해야 합니다. 전체 문은 인스턴스를 실행하는 데 필요한 모든 리소스와 비교하여 평가됩니다. 하지만 이러한 추가 리소스에는 `ec2:InstanceType` 조건 키가 없기 때문에 `StringLike` 검사는 fail로 끝나고 사용자에게 권한이 부여되지 않아 어떤 인스턴스 유형도 실행하지 못합니다. 이 문제를 해결하려면 그 대신 `StringLikeIfExists` 조건 연산자를 사용해야 합니다. 이렇게 하면 조건 키가 존재하는 경우에만 테스트가 실행됩니다. 그 결과 다음 예제는 이렇게 해석할 수 있습니다. '검사 대상 리소스에 `'ec2:InstanceType'`

조건 키가 있으면 키 값이 "t1.*", "t2.*" 또는 "m3.*"로 시작할 때에만 작업을 허용한다.' 검사 대상 리소스에 조건 키가 없으면 그냥 둡니다." `DescribeActions` 문에는 콘솔에서 해당 인스턴스를 보는 데 필요한 작업이 포함되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RunInstance",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "ec2:InstanceType": [
                        "t1.*",
                        "t2.*",
                        "m3.*"
                 ]}}
        },
        {
            "Sid": "DescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        }]
}
```

조건 키의 존재를 확인하는 조건 연산자

`Null` 조건 연산자를 사용하여 권한을 부여하는 시점에 조건 키의 유무를 검사할 수 있습니다. 정책 문에서는 `true`(키가 부재하며 — 값이 null임) 또는 `false`(키가 존재하며 값이 null이 아님)를 사용합니다.

예를 들어, 이 조건 연산자를 사용하여 작업 시 사용자가 자신의 자격 증명을 사용하는지, 혹은 임시 자격 증명을 사용하는지 알 수 있습니다. 사용자가 임시 자격 증명을 사용하는 경우에는 `aws:TokenIssueTime` 키가 존재하며, 값을 갖고 있습니다. 다음은 Amazon EC2 API 사용자의 경우 임시 자격 증명의 사용이 제한된다는 것(키가 존재해서는 안 됨)을 명시하는 조건을 나타낸 예제입니다.

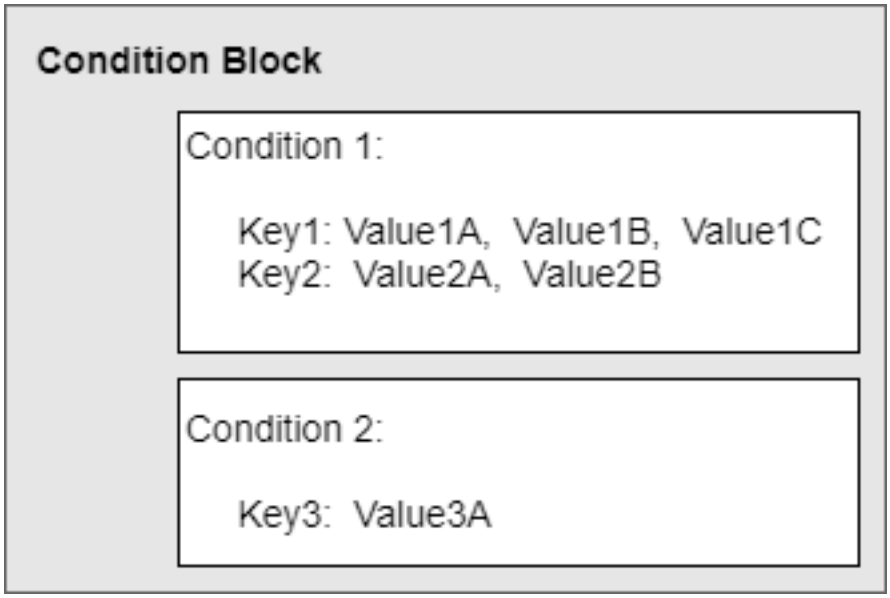
```
{
  "Version": "2012-10-17",
  "Statement":{
      "Action":"ec2:*",
      "Effect":"Allow",
      "Resource":"*",
      "Condition":{"Null":{"aws:TokenIssueTime":"true"}}
  }
}
```

다수의 키 또는 값을 사용하는 조건 생성

정책의 `Condition` 요소를 사용하여 요청에서 다수의 키, 혹은 단일 키에 대한 다수의 값을 테스트할 수 있습니다. 프로그래밍 방식이든, AWS Management 콘솔을 사용하든 상관없이 AWS에게 요청할 경우 요청에 보안 주체, 작업, 태그 등에 대한 정보가 포함됩니다. 요청에 포함되는 정보 및 데이터에 대한 자세한 내용은 요청 (p. 5) 단원을 참조하십시오. 조건 키를 사용하여 요청의 일치하는 키의 값을 테스트할 수 있습니다. 예

를 들어, 조건 키를 사용하여 DynamoDB 테이블의 특정 속성 또는 태그에 근거한 Amazon EC2 인스턴스에 대한 액세스를 제어할 수 있습니다.

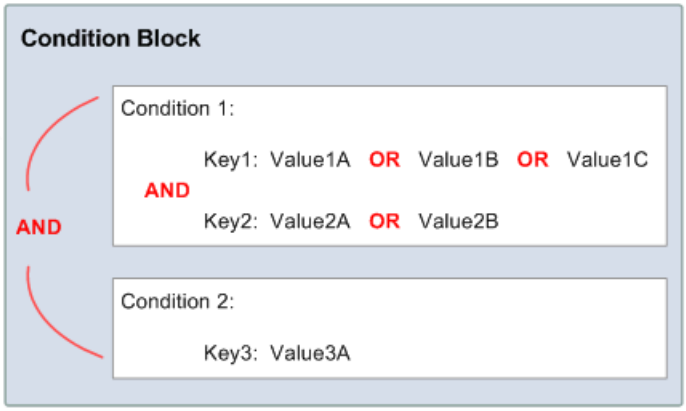
`Condition` 요소에는 여러 조건을 추가할 수 있으며, 다시 한 번 각 조건마다 다수의 키-값 페어가 포함됩니다. 대부분 조건 키는 다수의 값을 사용할 수 있도록 지원합니다. 다음은 이것을 설명한 그림입니다. 달리 지정하지 않는 경우 모든 키는 다수의 값을 가질 수 있습니다.



주제

다수의 키 또는 값이 포함된 조건의 평가 로직

정책에 다수의 조건 연산자가 있거나, 다수의 키가 단일 조건 연산자에 추가되어 있으면 논리 연산자인 `AND`를 사용하여 조건을 평가합니다. 단일 조건 연산자에 키 하나마다 여러 값이 포함된 경우에는 논리 연산자 `OR`를 사용하여 해당 조건 연산자를 평가합니다. 원하는 `Allow` 또는 `Deny` 효과를 트리거하려면 모든 조건이 true여야 합니다.

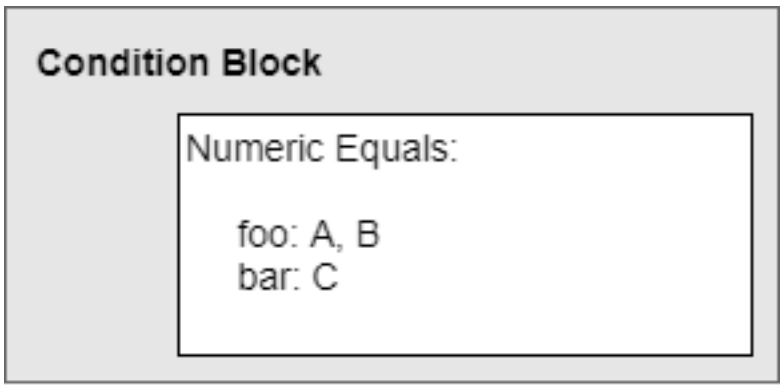


다수의 키와 값 사용

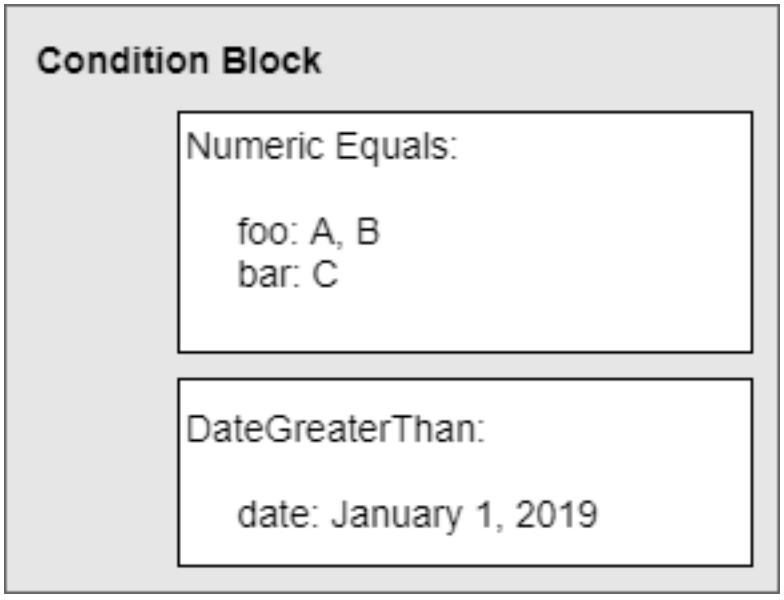
단일 키에 다수의 값이 포함된 요청일 경우에는 예를 들어 ("Key2":["Value2A", "Value2B"]) 같이 조건을 대괄호로 묶어야 합니다. 또한 `ForAllValues` 또는 `ForAnyValue` 집합 연산자는 `StringLike` 조건 연산자 (p. 602)와 함께 사용해야 합니다. 이러한 한정자는 조건 연산자에 설정 작업 기능을 추가하므로 여러 요청 값을 여러 조건 값에 대해 테스트할 수 있습니다.

- `ForAllValues` – 요청 세트의 모든 멤버 값이 조건 키 세트의 하위 세트인지 여부를 테스트합니다. 요청의 모든 키 값이 정책에 있는 하나 이상의 값과 일치하면 조건이 true를 반환합니다. 요청에 키가 없거나 키 값이 빈 문자열과 같은 null 데이터 세트로 확인되는 경우에도 true를 반환합니다.
- `ForAnyValue` – 요청 값 세트에서 하나 이상의 멤버가 조건 키 값 세트에서 멤버 1개 이상과 일치하는지 테스트합니다. 요청의 키 값 중 하나가 정책의 조건 값 중 하나와 일치하면 조건이 true를 반환합니다. 일치하는 키가 없거나 null 데이터 세트의 경우 조건에서 false를 반환합니다.

숫자 값 foo가 A 또는 B와 일치하고, 다른 숫자 값 bar가 C와 일치하는 경우에 한해 John에게 리소스 사용을 허용한다고 가정하겠습니다. 이 경우 다음 그림과 같이 조건 블록을 생성하게 됩니다.



이번에는 2019년 1월 1일 이후에 대한 John의 액세스 권한을 제한한다고 가정하겠습니다. 그렇다면 다른 조건으로 2019년 1월 1일에 해당하는 날짜와 함께 `DateGreaterThan`을 추가해야 합니다. 조건 블록의 모습은 다음 그림과 같습니다.



AWS에는 사전 정의된 조건 연산자 및 키가 있습니다(`aws:CurrentTime` 등). 마찬가지로 AWS 서비스 역시 각각 정의되어 있는 키가 따로 있습니다.

예를 들어 다음과 같은 조건에서 사용자 John에게 Amazon SQS 대기열에 대한 액세스를 허용한다고 가정하겠습니다.

- 시간은 2019년 7월 16일 오후 12:00 이후입니다.
- 시간은 2019년 7월 16일 오후 3:00 이전입니다.
- 요청이 전송되는 IP 주소의 범위는 192.0.2.0~192.0.2.255 또는 203.0.113.0~203.0.113.255입니다.

조건 블록에는 서로 다른 세 개의 조건 연산자가 있으며, John이 대기열, 주제 또는 리소스에 액세스하려면 이 세 가지 조건 연산자가 모두 충족되어야 합니다.

다음은 정책의 조건 블록을 나타낸 예제입니다. `aws:SourceIp`의 값 2개는 `OR`을 사용하여 평가합니다. 서로 다른 세 개의 조건 연산자는 `AND`를 사용하여 평가합니다.

```
"Condition" :  {
      "DateGreaterThan" : {
         "aws:CurrentTime" : "2019-07-16T12:00:00Z"
       },
      "DateLessThan": {
         "aws:CurrentTime" : "2019-07-16T15:00:00Z"
       },
       "IpAddress" : {
          "aws:SourceIp" : ["192.0.2.0/24", "203.0.113.0/24"]
      }
}
```

다수의 값을 조건 집합 연산자와 함께 사용하는 예제

정책을 만들어 그 정책에 지정된 하나 이상의 값에 대해 요청의 여러 값을 테스트할 수 있습니다. 기술 지원 포럼의 스레드에 대한 정보를 저장하는 데 사용되는 `Thread`라는 Amazon DynamoDB 테이블이 있다고 가정해 보십시오. 이 테이블에는 `ID`, `UserName`, `PostDateTime`, `Message`, `Tags`라는 이름의 속성이 있습니다.

```
{
  ID=101
  UserName=Bob
  PostDateTime=20130930T231548Z
  Message="A good resource for this question is docs.aws.amazon.com"
  Tags=["AWS", "Database", "Security"]
}
```

DynamoDB에서 설정된 연산자를 사용하여 개별 데이터 항목 및 속성에 대한 세부적인 액세스를 구현하는 방법은 Amazon DynamoDB 개발자 안내서에서 DynamoDB에 대한 세분화된 액세스 제어 단원을 참조하십시오.

`PostDateTime`, `Message`, `Tags` 속성만 볼 수 있도록 허용하는 정책을 만들 수 있습니다. 사용자 요청에 이러한 속성이 하나라도 포함되어 있으면 요청이 허용됩니다. 하지만 요청에 다른 속성(`ID` 등)이 포함되어 있으면 요청이 거부됩니다. 논리적으로 보았을 때 사용자는 허용되는 속성(`PostDateTime`, `Message`, `Tags`) 목록을 생성하려고 합니다. 또한 사용자가 요청한 모든 속성이 허용되는 속성 목록에 포함되어야 한다고 정책에 명시하려고 합니다.

다음 정책 예제는 `ForAllValues` 한정자를 `StringEquals` 조건 연산자와 함께 사용하는 방법을 보여줍니다. 이 조건에서는 사용자가 `Thread`라는 DynamoDB 테이블에서 `ID`, `Message` 또는 `Tags` 속성만 요청하도록 허용합니다.

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

```
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:*:*:table/Thread",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "dynamodb:Attributes": [
                        "ID",
                        "Message",
                        "Tags"
                    ]
                }
            }
        }
    ]
}
```

사용자가 DynamoDB에게 `Message` 및 `Tags` 속성을 `Thread` 테이블에서 가져오도록 요청한다고 가정하겠습니다. 이러한 경우에는 사용자가 요청하는 속성이 모두 정책에서 지정한 값과 일치하기 때문에 요청이 허용됩니다. `GetItem` 작업을 하려면 사용자는 `ID` 속성을 정책에서도 허용되는 데이터베이스 테이블 키로 전달해야 합니다. 하지만 사용자 요청에 `UserName` 속성이 포함되면 요청이 거부됩니다. `UserName`은 허용되는 속성 목록에 들어 있지 않고, `ForAllValues` 한정자는 요청된 모든 값이 정책에 나열되어 있을 것을 요구하기 때문입니다.

> **Important**
>
> `dynamodb:Attributes`를 사용하는 경우 테이블에 대한 모든 기본 키 및 인덱스 키 속성의 이름을 지정해야 합니다. 또한 정책에 나열되는 보조 인덱스도 지정해야 합니다. 그렇지 않으면, DynamoDB에서 이러한 키 속성을 사용하여 요청한 작업을 수행할 수 없습니다.

또는 사용자가 `ID` 및 `UserName` 등 일부 속성을 요청에 포함시키는 것을 명시적으로 금지할 수 있습니다. 예를 들어, 업데이트(`PUT` 작업)로 인해 특정 속성이 변경되지 않도록 사용자가 DynamoDB 테이블을 업데이트할 때 일부 속성을 제외할 수 있습니다. 이러한 경우에는 금지된 속성(`ID`, `UserName`) 목록을 생성합니다. 사용자가 요청한 속성 중 금지된 속성이 있는 경우, 요청이 거부됩니다.

다음 예제에서는 사용자가 `ForAnyValue` 작업을 수행하려는 경우, `ID` 한정자를 사용해 `PostDateTime` 및 `PutItem` 속성에 대한 액세스를 거부하는 방법을 보여줍니다. 즉 사용자가 `Thread` 테이블에 있는 이 두 가지 속성 중 어느 하나를 업데이트하려 하는 경우를 말합니다. `Effect` 요소는 `Deny`로 설정됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "dynamodb:PutItem",
        "Resource": "arn:aws:dynamodb:*:*:table/Thread",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "dynamodb:Attributes": [
                    "ID",
                    "PostDateTime"
                ]
            }
        }
    }
}
```

사용자가 `PostDateTime` 테이블의 `Message` 및 `Thread` 속성의 업데이트를 요청한다고 가정할 경우, `ForAnyValue` 한정자는 요청된 속성 중 정책 목록에 표시되는 것이 있는지 여부를 결정합니다. 이 경우 하나가 일치하므로(`PostDateTime`) 조건은 true입니다. 요청의 다른 값(예: 리소스)도 일치한다고 가정하면, 전체 정책 평가는 true를 반환합니다. 정책의 효력이 `Deny`이므로 요청은 거부됩니다.

한편 사용자가 `PutItem` 속성만으로 `UserName` 수행을 요청한다고 가정해 보겠습니다. 요청의 속성(`UserName`이 유일) 중 어떤 것도 정책에 나열된 속성(`ID`, `PostDateTime`)과 일치하지 않습니다. 조건이 false를 반환하므로 정책의 효력(`Deny`) 또한 false이고, 따라서 이 정책은 요청을 거부하지 않습니다. (요청이

성공하려면 다른 정책에서 이를 명시적으로 허용해야 합니다. 이 요청은 이 정책에 의해 명시적으로 거부되지 않지만, 모든 요청은 묵시적으로 거부됩니다.)

> Warning
>
> `ForAllValues` 조건 연산자를 사용하면 요청에 키가 없거나 키 값이 빈 문자열과 같은 null 데이터 세트로 확인되면 true를 반환합니다. 요청에 하나 이상의 값이 포함되도록 하려면 정책에서 다른 조건을 사용해야 합니다. 문제 해결 예는 AWS 요청 중 액세스 제어 (p. 386) 단원을 참조하십시오.

조건 집합 연산자를 사용하는 다수의 값에 대한 평가 로직

이 단원에서는 `ForAllValues` 및 `ForAnyValue` 연산자와 함께 사용되는 평가 로직의 세부 사항을 다룹니다. 요청에 포함될 수 있는 키(`PostDateTime` 및 `UserName`)와 `PostDateTime`, `Message` 및 `Tags` 값을 포함하는 정책 조건이 아래 표에 나와 있습니다.

키(요청)	조건 값(정책)
`PostDateTime`	`PostDateTime`
`UserName`	`Message`
	`Tags`

조합에 대한 평가는 다음과 같습니다.

`PostDateTime` matches `PostDateTime`?
`PostDateTime` matches `Message`?
`PostDateTime` matches `Tags`?
`UserName` matches `PostDateTime`?
`UserName` matches `Message`?
`UserName` matches `Tags`?

조건 연산자의 결과는 정책 조건에 사용된 변경자에 따라 달라집니다.

- `ForAllValues`를 선택하십시오. 요청의 모든 키(`PostDateTime` 또는 `UserName`)가 최소 한 개의 정책 조건 값(`PostDateTime`, `Message`, `Tags`)과 일치하면, 조건 연산자는 true를 반환합니다. 다시 말해, 조건이 true가 되려면 (`PostDateTime`은 `PostDateTime`, `Message` 또는 `Tags`와 일치) 그리고 (`UserName`은 `PostDateTime`, `Message` 또는 `Tags`와 일치) 둘 다 만족해야 합니다.
- `ForAnyValue`. 요청 값과 정책 값의 여섯 가지 조합 중 하나에서 true를 반환하면 조건 연산자는 true를 반환합니다.

다음 정책은 `ForAllValues` 한정자를 포함합니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "dynamodb:GetItem",
        "Resource": "arn:aws:dynamodb:*:*:table/Thread",
        "Condition": {
            "ForAllValues:StringEquals": {
                "dynamodb:Attributes": [
```

```
                    "PostDateTime",
                    "Message",
                    "Tags"
                ]
            }
        }
    }
}
```

사용자가 PostDateTime 및 UserName 속성을 가져오기 위해 DynamoDB에 요청을 한다고 가정하겠습니다. 조합에 대한 평가는 다음과 같습니다.

PostDateTime matches PostDateTime?	True
PostDateTime matches Message?	False
PostDateTime matches Tags?	False
UserName matches PostDateTime?	False
UserName matches Message?	False
UserName matches Tags?	False

이 정책에는 ForAllValues 조건 연산 변경자가 포함되어 있는데, 이는 PostDateTime 일치 항목과 UserName 일치 항목이 최소한 하나는 있어야 한다는 것을 뜻합니다. UserName과 일치하는 항목이 없으므로 조건 연산자는 false를 반환하며, 정책은 요청을 허용하지 않습니다.

다음 정책은 ForAnyValue 한정자를 포함합니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "dynamodb:PutItem",
        "Resource": "arn:aws:dynamodb:*:*:table/Thread",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "dynamodb:Attributes": [
                    "ID",
                    "PostDateTime"
                ]
            }
        }
    }
}
```

이 정책은 "Effect":"Deny"를 포함하며, 작업은 PutItem입니다. 사용자가 PutItem, UserName 및 Message 속성을 포함하는 PostDateTime 요청을 한다고 가정하겠습니다. 평가는 다음과 같습니다.

UserName matches ID?	False
UserName matches PostDateTime?	False
Messages matches ID?	False
Message matches PostDateTime?	False
PostDateTime matches ID?	False

PostDateTime matches PostDateTime?	True

ForAnyValue 변경자에 따라, 이러한 테스트 중 하나가 true를 반환하면 조건은 true를 반환합니다. 마지막 테스트가 true를 반환하므로 조건은 true입니다. Effect 요소가 Deny로 설정되어 있으므로 요청은 거부됩니다.

> Note
>
> 요청의 키 값이 빈 데이터 세트(예: 빈 문자열)로 확인되면 ForAllValues에서 수정한 조건 연산자는 true를 반환합니다. 또한 ForAnyValue에서 수정한 조건 연산자는 false를 반환합니다.

IAM 정책 요소: 변수 및 태그

정책 작성 시 리소스나 조건 키의 정확한 값을 모를 경우 AWS Identity and Access Management(IAM) 정책 변수를 자리 표시자로 사용하십시오.

> Note
>
> AWS에서 변수를 확인할 수 없는 경우 전체 문이 잘못되는 문제가 발생할 수 있습니다. 예를 들어 aws:TokenIssueTime 번수를 사용하는 경우 변수는 요청자가 임시 자격 증명을 사용하여 인증된 경우(IAM 역할)에만 값을 확인합니다. 잘못된 문을 유발하는 변수를 방지하려면 ...IfExists 조건 연산자 (p. 607)를 사용하십시오.

주제

소개

IAM 정책에서는 다양한 작업을 통해 액세스를 제어하려는 특정 리소스에 이름을 지정할 수 있습니다. 예를 들어 다음은 사용자가 Amazon S3 버킷 mybucket에서 접두사 David가 사용된 객체를 표시하거나, 읽거나, 쓸 수 있는 정책입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::mybucket"],
      "Condition": {"StringLike": {"s3:prefix": ["David/*"]}}
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::mybucket/David/*"]
    }
  ]
}
```

정책을 작성하다 보면 정확한 리소스 이름을 모를 때도 있습니다. 사용자마다 고유한 정책 사본을 만들 필요 없이 여러 사용자에게 작용하도록 정책을 일반화해야 할 수 있습니다. 예를 들어 앞의 예와 마찬가지로 사용

자마다 Amazon S3 버킷에 자신의 객체를 액세스하도록 허용하는 정책을 쓸 수도 있습니다. 그러나 리소스의 일부로 사용자의 이름을 명시적으로 지정하는 각 사용자에 대해 별도의 정책을 만들지 마십시오. 대신 해당 그룹의 모든 사용자에 대해 작동하는 단일 그룹 정책을 만듭니다.

이때는 정책에 자리 표시자를 지정할 수 있는 정책 변수 기능을 사용하면 가능합니다. 정책을 평가할 때는 이 정책 변수가 요청 자체의 맥락에서 온 값으로 바뀝니다.

다음은 Amazon S3 버킷에서 정책 변수를 사용하는 정책을 나타낸 예제입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::mybucket"],
      "Condition": {"StringLike": {"s3:prefix": ["${aws:username}/*"]}}
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::mybucket/${aws:username}/*"]
    }
  ]
}
```

이 정책을 평가할 때는 IAM이 `${aws:username}` 변수를 실제 현재 사용자의 알기 쉬운 이름 (p. 563)으로 대체합니다. 이 말은 사용자 그룹에 단일 정책을 적용하여 사용자 이름을 리소스 이름 일부로 사용함으로써 버킷에 대한 액세스 제어가 가능함을 의미합니다.

변수는 `$` 접두사 뒤에 중괄호(`{ }`)를 사용하여 표시합니다. `${ }` 문자 안에는 정책에서 사용할 요청 값의 이름을 추가할 수 있습니다. 사용할 수 있는 값은 이 페이지 후반에서 다루겠습니다.

> **Note**
>
> 정책 변수를 사용하려면 `Version` 요소를 문에 추가해야 하며, 이때 버전은 정책 변수를 지원하는 버전으로 설정해야 합니다. 변수는 버전 `2012-10-17`에서 도입되었습니다. 정책 언어의 조기 버전은 정책 변수를 지원하지 않기 때문입니다. `Version` 요소를 추가하지 않고 해당 버전 날짜로 설정하면 `${aws:username}` 같은 변수가 정책에서 리터럴 문자열로 처리됩니다.
> `Version` 정책 요소는 정책 버전과 다릅니다. `Version` 정책 요소는 정책 내에서 사용되며 정책 언어의 버전을 정의합니다. 반면에 정책 버전은 IAM에서 고객 관리형 정책을 변경할 때 생성됩니다. 변경된 정책은 기존 정책을 덮어쓰지 않습니다. 대신 IAM에서 관리형 정책의 새 버전을 만듭니다. `Version` 정책 요소에 대한 자세한 내용은 the section called “Version” (p. 587) 단원을 참조하십시오. 정책 버전에 대한 자세한 내용은 the section called “IAM 정책 버전 관리” (p. 458) 단원을 참조하십시오.

비슷한 방식으로 정책 변수를 사용하여 각 사용자가 자신의 액세스 키를 관리할 수 있도록 할 수 있습니다. 사용자가 프로그래밍 방식으로 `David` 사용자의 액세스 키를 변경할 수 있는 정책은 아래와 유사합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": ["iam:*AccessKey*"],
    "Effect": "Allow",
    "Resource": ["arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:user/David"]
  }]
}
```

이 정책이 `David` 사용자에게 추가되면 해당 사용자는 자신의 액세스 키를 변경할 수 있습니다. 사용자별 Amazon S3 객체에 대한 정책과 마찬가지로 사용자 이름을 포함하는 각 사용자에 대해 별도의 정책을 생성합니다. 그런 다음 각 정책을 개별 사용자에 연결합니다.

정책 변수를 사용하여 생성할 수 있는 정책은 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": ["iam:*AccessKey*"],
    "Effect": "Allow",
    "Resource": ["arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:user/${aws:username}"]
  }]
}
```

이처럼 사용자 이름에 정책 변수를 사용할 때는 개별 사용자마다 별도의 정책을 생성할 필요가 없습니다. 대신에 이 새로운 정책을 자신의 액세스 키를 직접 관리해야 하는 사용자가 모두 포함된 IAM 그룹에 추가하면 됩니다. 이후 사용자가 자신의 액세스 키 변경을 요청하면 IAM이 현재 요청의 사용자 이름을 `${aws:username}` 변수에 치환한 후 정책을 평가합니다.

정책 변수로서의 태그

일부 AWS 서비스에서는 사용자 지정 속성을 해당 서비스가 생성한 리소스에 연결할 수 있습니다. 예를 들어, Amazon S3 버킷 또는 IAM 사용자 및 역할에 태그를 적용할 수 있습니다. 이러한 태그는 키–값 페어입니다. 태그 키 이름과 해당 키 이름과 연관된 값을 정의합니다. 예를 들어 **`department`** 키와 **`Human Resources`** 값으로 태그를 만들 수 있습니다. IAM 엔터티 태그 지정에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오. 다른 AWS 서비스에서 생성한 리소스에 대한 태그 지정 정보는 해당 서비스의 문서 단원을 참조하십시오. Tag Editor에 대한 자세한 내용은 AWS Management 콘솔 사용 설명서의 Tag Editor 작업 단원을 참조하십시오.

IAM 자격 증명에 태그를 추가하면 IAM 리소스를 쉽게 찾고, 구성하고, 추적할 수 있습니다. 또한 IAM 자격 증명에 태그를 지정하여 리소스에 대한 액세스를 제어하거나 자체 태그를 지정할 수 있습니다. 태그를 사용하여 액세스를 제어하는 방법에 대한 자세한 내용은 IAM 리소스 태그를 사용하여 IAM 사용자 및 역할에 대한 액세스 제어 (p. 382) 단원을 참조하십시오.

정책 변수를 사용할 수 있는 경우

정책 변수는 `Resource` 요소를 비롯해 `Condition` 요소의 문자열 비교에 사용할 수 있습니다.

리소스 요소

정책 변수는 리소스 식별자인 ARN (p. 564)의 마지막 부분에 표시됩니다. 다음은 그룹에 추가할 수 있는 정책입니다. 이 정책은 그룹 내 각 사용자에게 Amazon S3의 사용자별 객체(자신의 "홈 디렉터리")에 프로그래밍 방식으로 완전히 액세스할 수 있는 권한을 부여하고 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::mybucket"],
      "Condition": {"StringLike": {"s3:prefix": ["${aws:username}/*"]}}
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::mybucket/${aws:username}/*"]
```

```
    }
  ]
}
```

> **Note**
>
> 위 예제는 `aws:username` 키를 사용하여 알기 쉬운 사용자 이름("Adele" 또는 "David" 등)을 반환합니다. 하지만 글로벌 고유 값인 `aws:userid` 키를 사용해야 하는 경우도 있습니다. 자세한 내용은 고유 식별자 (p. 567) 단원을 참조하십시오.

다음은 IAM 그룹에 사용할 수 있는 정책입니다. 이 정책에 따라 해당 그룹의 사용자들은 자신의 이름이 포함된 대기열과 us-east-2 리전에 속한 대기열을 생성, 사용 및 삭제할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListForConsole",
            "Effect": "Allow",
            "Action": "sqs:ListQueues",
            "Resource": "*"
        },
        {
            "Sid": "AllQueueActions",
            "Effect": "Allow",
            "Action": "sqs:*",
            "Resource": "arn:aws:sqs:us-east-2:*:${aws:username}-queue"
        }
    ]
}
```

ARN의 일부를 태그 값으로 바꾸려면 접두사와 키 이름을 ${}로 묶습니다. 예를 들어 다음 `Resource` 요소는 요청한 사용자의 `department` 태그 값과 동일한 이름의 버킷만 참조합니다.

```
    "Resource": ["arn:aws:s3:::bucket/${aws:PrincipalTag/department}"]
```

조건 요소

정책 변수는 문자열 연산자(`Condition`, `StringEquals`, `StringLike` 등) 또는 ARN 연산자(`StringNotLike`, `ArnEquals` 등)이 추가된 모든 조건에서 `ArnLike` 값으로도 사용할 수 있습니다. 다음 Amazon SNS 주제 정책은 AWS 계정 `999999999999`의 사용자들에게 URL이 AWS 사용자 이름과 일치하는 경우에만 이러한 주제를 관리할 수 있도록 권한(모든 작업 실행)을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Principal": {"AWS": "999999999999"},
    "Effect": "Allow",
    "Action": "sns:*",
    "Condition": {"StringLike": {"sns:endpoint": "https://example.com/${aws:username}/*"}}
  }]
}
```

`Condition` 요소 표현식에서 태그를 참조할 때는 관련 접두사와 키 이름을 조건 키로 사용하십시오. 그런 다음 조건 값에서 테스트할 값을 사용합니다. 예를 들어, 다음 정책 예제에서는 `costCenter` 태그가 리소스에 연결된 경우에만 IAM 리소스에 대한 모든 액세스를 허용합니다. 태그의 값은 `12345` 또는 `67890`이어야 합니다. 태그에 값이 없거나 다른 값이 있으면 요청이 실패합니다.

```
{
  "Version": "2015-01-01",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:ResourceTag/costCenter": [ "12345", "67890" ]
        }
      }
    }
  ]
}
```

정책 변수로 사용할 수 있는 요청 정보

정책 변수의 치환 값은 현재 요청 컨텍스트 (p. 623)에서 나와야 합니다.

모든 요청에 사용할 수 있는 정보

정책에는 정책 변수로 사용할 수 있는 값의 키가 포함됩니다. (일부 값이 포함되지 않는 키도 있습니다. 자세한 내용은 이번 목록 다음의 정보 단원을 참조하십시오).

- **`aws:CurrentTime`** 날짜와 시간을 확인하는 조건에 사용할 수 있습니다.
- **`aws:EpochTime`** epoch의 날짜 또는 Unix 시간으로, 날짜/시간 조건에 사용합니다.
- **`aws:TokenIssueTime`** 임시 보안 자격 증명이 발급된 날짜와 시간으로, 날짜/시간 조건에 사용할 수 있습니다. 참고: 이 키는 임시 보안 자격 증명을 사용해 서명된 요청에만 사용할 수 있습니다. 임시 보안 자격 증명에 대한 자세한 내용은 임시 보안 자격 증명 (p. 302) 단원을 참조하십시오.
- **`aws:principaltype`** 이 값은 계정, 사용자, 연동된 역할 또는 위임된 역할 등 보안 주체가 무엇인지를 나타냅니다. 뒤에 나오는 설명 단원을 참조하십시오.
- **`aws:SecureTransport`** 요청이 SSL을 사용하여 전송되었는지 여부를 나타내는 부울 값입니다.
- **`aws:SourceIp`** 요청자의 IP 주소로, IP 주소 조건에 사용합니다. 언제 IP 주소 조건 연산자 (p. 605)가 유효한지와 언제 VPC 전용 키를 대신 사용해야 하는지에 대한 정보는 `SourceIp` 단원을 참조하십시오.
- **`aws:UserAgent`** 이 값은 요청자의 클라이언트 애플리케이션에 대한 정보를 포함하는 문자열입니다. 이 문자열은 클라이언트에 의해 생성되며 신뢰성이 떨어질 수 있습니다. AWS CLI에서는 이 컨텍스트 키를 사용만 할 수 있습니다.
- **`aws:userid`** 이 값은 현재 사용자의 고유 ID입니다. 다음에 나오는 차트 단원을 참조하십시오.
- **`aws:username`** 현재 사용자의 알기 쉬운 이름 (p. 563)을 포함하는 문자열입니다. 다음에 나오는 차트 단원을 참조하십시오.
- **`ec2:SourceInstanceARN`** 요청이 이루어진 Amazon EC2 인스턴스의 Amazon 리소스 이름(ARN)입니다. 이 키는 EC2 인스턴스 프로필과 연결된 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 해당 요청이 들어오는 경우에만 존재합니다.

> **Important**
>
> 키 이름은 대/소문자를 구분합니다. 예를 들어, `aws:CurrentTime`은 `AWS:currenttime`과 같습니다.

보안 주체 키 값

`aws:username`, `aws:userid` 및 `aws:principaltype` 값은 요청을 시작한 보안 주체 유형에 따라 다릅니다. 예를 들어 요청은 IAM 사용자, IAM 역할 또는 AWS 계정 루트 사용자의 자격 증명을 사용하여 가능합니다. 다음은 다른 유형의 보안 주체에 사용되는 키 값을 나타낸 목록입니다.

- AWS 계정 루트 사용자
  - `aws:username`: (없음)
  - `aws:userid`: AWS 계정 ID

  - `aws:principaltype`: `Account`
- IAM 사용자
  - `aws:username`: *`IAM-user-name`*
  - `aws:userid`: 고유 ID (p. 567)
  - `aws:principaltype`: `User`
- 연동 사용자
  - `aws:username`: (없음)
  - `aws:userid`: *`account`*:*`caller-specified-name`*
  - `aws:principaltype`: `FederatedUser`
- 웹 연동 사용자 및 SAML 연동 사용자

  Note

  웹 자격 증명 연동을 사용할 때 사용 가능한 정책 키에 대한 자세한 내용은 웹 자격 증명 연동을 사용해 사용자 식별하기 (p. 186) 단원을 참조하십시오.

  - `aws:username`: (없음)
  - `aws:userid`: (없음)
  - `aws:principaltype`: `AssumedRole`
- 위임된 역할
  - `aws:username`: (없음)
  - `aws:userid`: *`role-id`*:*`caller-specified-role-name`*
  - `aws:principaltype`: `Assumed role`
- Amazon EC2 인스턴스에 할당된 역할
  - `aws:username`: (없음)
  - `aws:userid`: *`role-id`*:*`ec2-instance-id`*
  - `aws:principaltype`: `Assumed role`
- 익명 호출자(Amazon SQS Amazon SNS 및 Amazon S3)
  - `aws:username`: (없음)
  - `aws:userid`: (없음)
  - `aws:principaltype`: `Anonymous`

이 목록에 있는 항목의 경우 다음을 참고하십시오.

- 없음이란 현재 요청 정보에 값이 없다는 의미이며, 이때 일치시키려고 하면 실패하고 문이 잘못됩니다.
- *`role-id`*는 각 역할 생성 시 할당되는 고유 식별자입니다. 역할 ID는 AWS CLI 명령 `aws iam get-role --role-name` *`rolename`*으로 표시할 수 있습니다.
- *`caller-specified-name`* 및 *`caller-specified-role-name`*은 임시 자격 증명을 가져오기 위해 호출할 때 호출 프로세스(예: 애플리케이션 또는 서비스 등)에서 전달되는 이름입니다.
- *`ec2-instance-id`*는 실행 시 인스턴스에 할당되는 값으로서 Amazon EC2 콘솔의 인스턴스 페이지에 표시됩니다. 그 밖에 AWS CLI 명령 `aws ec2 describe-instances`를 실행해도 인스턴스 ID를 표시할 수 있습니다.

연동 사용자 요청에 사용할 수 있는 정보

연동 사용자란 IAM 외에 다른 시스템을 사용하여 인증된 사용자를 말합니다. 예를 들어 AWS 호출 시 자체적으로 애플리케이션을 사용하는 회사가 있다고 가정하겠습니다. 이때는 회사의 애플리케이션 사용자 모두에게 IAM 자격 증명을 제공하는 것이 현실적으로 어렵습니다. 대신에 단일 IAM 자격 증명을 갖춘 프록시(미들 티어) 애플리케이션을 사용하거나, SAML 자격 증명 공급자(IdP)를 사용할 수 있습니다. 프록시 애플리케이션이나 SAML IdP는 회사 네트워크를 사용해 각 사용자를 인증합니다. 그런 다음 프록시 애플리케이션이 IAM 자격 증명을 사용하여 개별 사용자에 대한 임시 보안 자격 증명을 얻을 수 있습니다. SAML IdP는 AWS

임시 보안 자격 증명에 대한 ID 정보를 사실상 교환할 수 있습니다. 이후 임시 자격 증명을 사용하면 AWS 리소스에 액세스할 수 있습니다.

이와 유사한 방식으로 앱을 통해 AWS 리소스에 액세스해야 하는 모바일 디바이스용 앱을 개발하는 것도 가능합니다. 이런 경우에는 웹 자격 증명 연동을 사용할 수 있습니다. 웹 자격 증명 연동에서는 앱이 Login with Amazon, Amazon Cognito, Facebook 또는 Google처럼 잘 알려진 자격 증명 공급자를 통해 사용자를 인증합니다. 인증이 완료되면 앱이 공급자의 사용자 인증 정보를 사용하여 임시 보안 자격 증명을 가져온 후 AWS 리소스에 액세스합니다.

웹 자격 증명 연동을 위해 가장 바람직한 방법은 Amazon Cognito와 AWS 모바일 SDK를 이용하는 것입니다. 자세한 내용은 다음 단원을 참조하십시오.

- Android용 AWS Mobile SDK Developer Guide의 Amazon Cognito 개요
- AWS Mobile SDK for iOS Developer Guide의 Amazon Cognito 개요
- 임시 자격 증명과 관련된 일반적인 시나리오 (p. 302).

서비스별 정보

요청에는 서비스에 따른 키와 값이 요청 컨텍스트에 추가될 수 있습니다. 예는 다음과 같습니다.

- `s3:prefix`
- `s3:max-keys`
- `s3:x-amz-acl`
- `sns:Endpoint`
- `sns:Protocol`

정책 변수 값을 가져오는 데 사용할 수 있는 서비스별 키에 대한 자세한 내용은 각 서비스 설명서 단원을 참조하십시오. 예를 들어 다음 주제를 참조하시면 됩니다.

- Amazon Simple Storage Service 개발자 가이드의 버킷 정책 및 사용자 정책 사용.
- Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 키.

특수 문자

정책 변수 중에는 다른 특별한 의미를 갖는 문자를 나타낼 수 있도록 사전에 정의되어 있는 고정 값의 변수들도 몇 가지 있습니다. 이 특수 문자들은 일치시키려는 문자열의 일부이지만 리터럴로 삽입하였다면 오해할 가능성이 있습니다. 예를 들어 문자열에 별표(*)를 삽입하면 리터럴(*)이 아닌 모든 문자와 일치하는 와일드카드로 해석될 수 있습니다. 이 경우에는 다음과 같이 사전에 정의된 정책 변수를 사용할 수 있습니다.

- ${*} - 별표(*) 문자가 필요한 경우에 사용
- ${?} - 물음표(?)가 필요한 경우에 사용
- ${$} - 달러 문자($)가 필요한 경우에 사용

위처럼 사전 정의된 정책 변수들은 정규 정책 변수를 사용할 수 있는 문자열이라면 어디든지 사용 가능합니다.

자세한 정보

정책에 대한 자세한 정보는 다음 단원을 참조하십시오.

- 정책 및 권한 (p. 349)
- IAM 자격 증명 기반 정책 예제 (p. 387)
- IAM JSON 정책 요소 참조 (p. 586)

- 정책 평가 로직 (p. 622)
- 웹 자격 증명 연동에 대하여 (p. 183)

IAM JSON 정책 요소: 지원되는 데이터 형식

이 단원에서는 JSON 정책에서 값을 지정할 때 지원되는 데이터 형식을 설명합니다. 정책 언어는 각 정책 요소마다 모든 형식을 지원하지 않기 때문에 각 요소에 대한 자세한 내용은 이전 단원을 참조하십시오.

- 문자열
- 숫자(정수 및 부동 소수점)
- 부울
- Null
- 목록
- 맵
- 구조(중첩 맵)

다음은 각 데이터 형식을 직렬화로 매핑한 표입니다. 모든 정책은 UTF-8 형식을 따라야 합니다. JSON 데이터 형식에 대한 자세한 내용은 RFC 4627에서 확인할 수 있습니다.

유형	JSON
문자열	문자열
정수	번호
부동 소수점	번호
부울	true false
Null	null
날짜	ISO 8601의 W3C 프로파일을 준수하는 문자열
IpAddress	RFC 4632를 준수하는 문자열
List	배열
Object	Object

정책 평가 로직

보안 주체가 AWS Management 콘솔, AWS API 또는 AWS CLI를 사용하려고 시도하면 해당 보안 주체가 요청을 AWS에 전송합니다. AWS 서비스가 요청을 받으면 AWS는 여러 단계를 완료하여 요청을 허용할지 거부할지 여부를 결정합니다.

1. 인증 – AWS는 먼저 필요하다면 요청을 생성하는 보안 주체를 인증합니다. 이 단계는 익명 사용자의 요청을 허용하는 Amazon S3와 같은 몇몇 서비스에서는 필요하지 않습니다.
2. 요청 콘텍스트 처리 (p. 623) – AWS는 요청에 담긴 내용을 처리하여 어떤 정책을 요청에 적용할지 결정합니다.
3. 단일 계정 내에서 정책 평가 (p. 623) – AWS는 정책의 평가 순서에 영향을 받는 모든 정책 유형을 평가합니다.
4. 계정 내에서 요청 허용 여부 결정 (p. 625) – 이때 AWS는 요청에 따른 정책을 처리하여 요청을 허용할지 거부할지 여부를 결정합니다.

요청 콘텍스트 처리

AWS는 요청을 처리하여 다음 정보를 요청 콘텍스트에 모읍니다.

- 작업(또는 작동) – 보안 주체가 수행하고자 하는 작업 또는 작동입니다.
- 리소스 – 수행된 작업 또는 작동에 따른 AWS 리소스 객체입니다.
- 보안 주체 – 요청을 보내는 사용자, 역할, 연합된 사용자 또는 애플리케이션입니다. 보안 주체에 대한 정보는 보안 주체와 관련된 정책을 포함합니다.
- 환경 데이터 – IP 주소, 사용자 에이전트, SSL 사용 상태 또는 시간대와 같은 정보입니다.
- 리소스 데이터 – 요청되는 리소스와 관련된 데이터. 여기에는 DynamoDB 테이블 이름 또는 Amazon EC2 인스턴스 태그와 같은 정보가 포함될 수 있습니다.

AWS는 이러한 정보를 사용하여 요청 콘텍스트에 적용되는 정책을 찾습니다.

단일 계정 내에서 정책 평가

AWS는 요청 콘텍스트에 적용되는 정책 유형에 따라 정책을 평가합니다. 빈도 순으로 나열된 다음 정책 유형을 단일 AWS 계정 내에서 사용할 수 있습니다. 이러한 정책 유형에 대한 자세한 정보는 정책 및 권한 (p. 349)를 참조하십시오. AWS에서 교차 계정 액세스에 대한 정책을 평가하는 방법에 대한 자세한 내용은 교차 계정 정책 평가 로직 (p. 630) 단원을 참조하십시오.

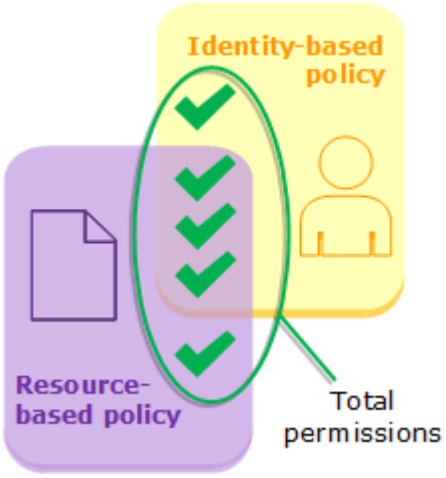
1. 자격 증명 기반 정책 – 자격 증명 기반 정책은 IAM 자격 증명(사용자, 사용자 그룹 또는 역할)에 연결되어 IAM 엔터티(사용자 및 역할)에 권한을 부여합니다. 자격 증명 기반 정책만 요청에 적용되는 경우 AWS에서는 하나 이상의 `Allow`에 대해 이러한 정책을 모두 확인합니다.
2. 리소스 기반 정책 – 리소스 기반 정책을 통해 보안 주체로서 지정된 보안 주체(계정, 사용자, 역할 또는 연합된 사용자)에 권한을 부여합니다. 권한은 보안 주체가 정책이 연결된 리소스를 사용하여 수행할 수 있는 작업을 정의합니다. 리소스 기반 정책 및 자격 증명 기반 정책 둘 다 요청에 적용되는 경우 AWS에서는 하나 이상의 `Allow`에 대해 이러한 정책을 모두 확인합니다.
3. IAM 권한 경계 – 권한 경계는 자격 증명 기반 정책을 통해 IAM 엔터티(사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 엔터티에 대한 권한 경계를 설정할 경우 해당 엔터티는 자격 증명 기반 정책 및 관련 권한 경계 모두에서 허용되는 작업만 수행할 수 있습니다. 권한 경계의 암시적 거부는 리소스 기반 정책에서 부여한 권한을 제한하지 않습니다.
4. AWS Organizations 서비스 제어 정책(SCP) – 조직 SCP는 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정합니다. SCP 최대값은 각 AWS 계정 루트 사용자을 포함하여 멤버 계정의 보안 주체에 적용됩니다. SCP가 있는 경우 자격 증명 기반 및 리소스 기반 정책이 이러한 정책과 SCP에서 해당 작업을 허용하는 경우에 한해서만 멤버 계정의 보안 주체에게 권한을 부여합니다. 권한 경계와 SCP가 둘 다 있는 경우 권한 경계, SCP 및 자격 증명 기반 정책 모두에서 해당 작업을 허용해야 합니다.
5. 세션 정책 – 세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 역할 세션을 프로그래밍 방식으로 생성하려면 `AssumeRole*` API 작업 중 하나를 사용합니다. 이를 수행하고 세션 정책을 전달할 때 결과적으로 얻는 세션의 권한은 IAM 엔터티의 자격 증명 기반 정책의 교차와 세션 정책입니다. 연합된 사용자 세션을 생성하려면 IAM 사용자의 액세스 키를 사용하여 `GetFederationToken` API 작업을 프로그래밍 방식으로 호출합니다. 리소스 기반 정책에는 세션 정책 권한 평가에 대한 각기 다른 효과가 있습니다. 그 차이는 사용자 또는 역할의 ARN이나 세션의 ARN이 리소스 기반 정책의 보안 주체로 나열되는지 여부에 따라 다릅니다. 자세한 정보는 세션 정책 (p. 351) 단원을 참조하십시오.

이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의함을 명심하십시오.

리소스 기반 정책과 함께 자격 증명 기반 정책 평가

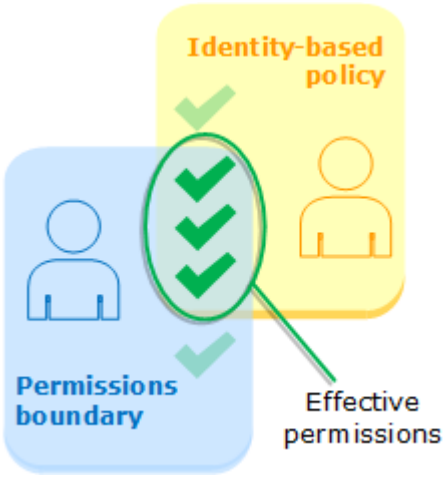
자격 증명 기반 정책 및 리소스 기반 정책은 연결된 자격 증명이나 리소스에 권한을 부여합니다. IAM 엔터티(사용자 또는 역할)가 동일 계정 내에서 리소스에 대한 액세스를 요청할 경우 AWS는 자격 증명 기반 및 리소스 기반 정책을 통해 부여된 모든 권한을 평가합니다. 결과적으로 두 정책 유형의 모든 권한이 권한으로 부여

됩니다. 자격 증명 기반 정책, 리소스 기반 정책 또는 두 정책 모두에 의해 작업이 허용되는 경우 AWS에서는 해당 작업을 허용합니다. 이들 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다.



권한 경계와 함께 자격 증명 기반 정책 평가

AWS에서 사용자의 자격 증명 기반 정책 및 권한 경계를 평가하는 경우 결과적으로 두 범주의 공통된 권한만 권한으로 부여됩니다. 기존 자격 증명 기반 정책으로 사용자에 권한 경계를 추가하면 사용자가 수행할 수 있는 작업을 축소할 수 있습니다. 또는 사용자에게서 권한 경계를 제거하면 사용자가 수행할 수 있는 작업이 늘어날 수 있습니다. 이들 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 다른 정책 유형을 권한 경계와 함께 평가하는 방식에 대해 자세히 알아보려면 경계가 있는 효과적인 권한 평가 (p. 364) 단원을 참조하십시오.



조직 SCP와 함께 자격 증명 기반 정책 평가

사용자가 조직의 멤버인 계정에 속하는 경우 결과로 나온 권한은 사용자의 정책과 SCP의 교집합입니다. 즉, 자격 증명 기반 정책 및 SCP 모두에서 작업이 허용되어야 합니다. 이들 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다.

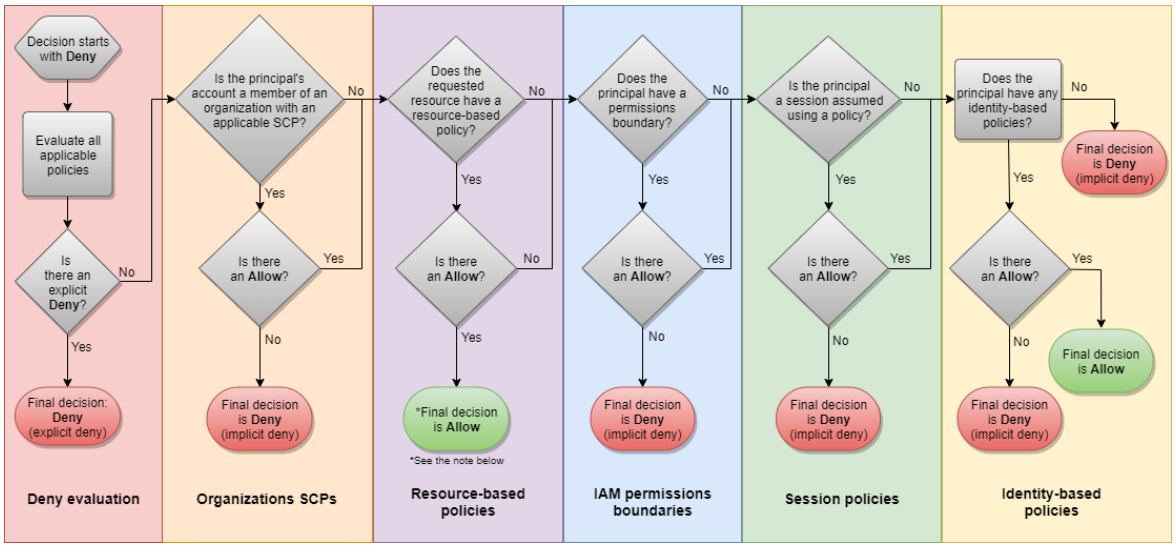
AWS Organizations에서 계정이 조직의 멤버인지 여부를 알아볼 수 있습니다. 조직 멤버가 SCP의 영향을 받을 수 있습니다. AWS CLI 명령 또는 AWS API 작업을 사용하여 이 데이터를 보려면 조직 엔터티에 대해 `organizations:DescribeOrganization` 작업 권한이 있어야 합니다. 조직 콘솔에서 작업을 수행할 추가 권한이 있어야 합니다. SCP가 특정 요청에 대한 액세스를 거부하는지 여부를 확인하거나 유효한 권한을 변경하려면 AWS Organizations 관리자에게 문의하십시오.

계정 내에서 요청 허용 여부 결정

보안 주체가 AWS로 요청을 보내 보안 주체의 엔터티와 동일한 계정에 있는 리소스에 액세스한다고 가정합니다. AWS 시행 코드는 요청의 허용 또는 거부 여부를 결정합니다. AWS에서는 요청 컨텍스트에 적용되는 모든 정책을 수집합니다. 다음은 단일 계정에 적용되는 이러한 정책에 대한 AWS 평가 로직을 간략하게 요약한 것입니다.

- 기본적으로 모든 요청이 묵시적으로 거부됩니다. 또는 기본적으로 AWS 계정 루트 사용자에 모든 권한이 부여됩니다.
- 자격 증명 기반 또는 리소스 기반 정책에 포함된 명시적 허용은 이 기본 작동을 재정의합니다.
- 권한 경계, 조직 SCP 또는 세션 정책이 있는 경우 이러한 정책 유형이 명시적 거부로 허용을 재정의할 수도 있습니다.
- 어떠한 정책의 명시적 거부도 허용을 무시합니다.

다음 순서도에 결정 방법에 대한 세부 정보가 나와 있습니다.



1. 거부 평가 – 기본적으로 모든 요청이 거부됩니다. 이를 묵시적 거부 (p. 629)라고 합니다. AWS 적용 코드는 해당 요청에 적용될 수 있는 계정 내의 모든 정책을 평가합니다. 여기에는 AWS Organizations SCP, 리소스 기반 정책, IAM 권한 경계, 역할 세션 정책 및 자격 증명 기반 정책이 포함됩니다. 이런 모든 정책에서 적용 코드는 해당 요청에 적용되는 `Deny` 설명문을 찾습니다. 이를 명시적 거부 (p. 629)라고 합니다. 적용되는 명시적 거부가 하나라도 발견되면 이 코드는 최종 거부 결정을 반환합니다. 명시적 거부가 없으면 코드 실행이 계속됩니다.
2. 조직 SCP – 그 다음에는 요청에 적용되는 AWS Organizations 서비스 제어 정책(SCP)을 평가합니다. SCP는 SCP가 연결된 계정의 보안 주체에 적용됩니다. 적용 가능한 `Allow` 문이 SCP에 없는 경우 요청이 묵시적으로 거부됩니다. 적용 코드가 최종 거부 결정을 반환합니다. SCP가 없거나 요청한 작업이 SCP에서 허용된 경우 코드 실행이 계속됩니다.
3. 리소스 기반 정책 – 보안 주체에 대해 요청한 작업의 수행을 허용하는 리소스 기반 정책이 요청한 리소스에 지정된 경우 적용 코드는 최종 허용 결정을 반환합니다. 리소스 기반 정책이 없거나 이 정책에 `Allow` 문이 포함되지 않은 경우 코드 실행이 계속됩니다.

   Note

   IAM 역할 또는 사용자의 ARN을 리소스 기반 정책의 보안 주체로 지정한 경우 이 로직은 다르게 동작할 수 있습니다. 세션 정책을 사용하여 해당 역할 또는 연동 역할에 대해 임시 자격 증명 세션을 생성할 수도 있습니다. 이러한 경우 세션에 대해 유효한 권한은 사용자 또는 역할의 자격 증명 기반 정책에서 허용하는 권한을 초과할 수 없습니다. 자세한 정보는 세션 정책을 참조하십시오.
4. IAM 권한 경계 – 다음에는 적용 코드가 보안 주체에 사용되는 IAM 엔터티에 권한 경계가 지정되어 있는지 여부를 확인합니다. 권한 경계를 설정하는 데 사용되는 정책에서 요청한 작업을 허용하지 않는 경우 요청이 묵시적으로 거부됩니다. 적용 코드가 최종 거부 결정을 반환합니다. 권한 경계가 없거나 요청한 작업이 권한 경계에서 허용된 경우 코드 실행이 계속됩니다.
5. 세션 정책 – 그 다음, 적용 코드는 세션 정책을 전달하여 보안 주체에서 위임된 세션을 사용 중인지 확인합니다. AWS CLI 또는 AWS API를 사용하는 동안 세션 정책을 전달하여 역할이나 연합된 사용자에 대한 임시 자격 증명을 가져올 수 있습니다. 세션 정책이 있지만 요청한 작업이 세션 정책에서 허용되지 않는 경우 해당 요청이 묵시적으로 거부됩니다. 적용 코드가 최종 거부 결정을 반환합니다. 세션 정책이 없거나 요청한 작업이 세션 정책에서 허용된 경우 코드 실행이 계속됩니다.
6. 자격 증명 기반 정책 – 그 다음, 적용 코드는 보안 주체에 대한 자격 증명 기반 정책을 확인합니다. IAM 사용자의 경우 이러한 정책에는 사용자 정책과 사용자가 속한 그룹의 정책이 포함됩니다. 적용 가능한 자격 증명 기반 정책에 요청한 작업을 허용하는 설명문이 있는 경우 적용 코드는 최종 허용 결정을 반환합니다. 요청한 작업을 허용하는 설명문이 없는 경우 해당 요청이 묵시적으로 거부되고, 적용 코드는 최종 거부 결정을 반환합니다.
7. 오류 – AWS 적용 코드를 평가하는 도중 오류가 발생할 경우 코드는 예외를 생성한 후 닫힙니다.

자격 증명 기반 정책 및 리소스 기반 정책 평가 예제

가장 일반적인 정책 유형은 자격 증명 정책 및 리소스 기반 정책입니다.

Carlos가 `carlossalazar`라는 사용자 이름을 쓰고 있고 `carlossalazar-logs` Amazon S3 버킷에 파일을 저장하고자 한다고 가정하십시오.

또한 다음 정책이 `carlossalazar` IAM 사용자와 연결되었다고 가정하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3ListRead",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:HeadBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowS3Self",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::carlossalazar/*",
                "arn:aws:s3:::carlossalazar"
            ]
        },
        {
            "Sid": "DenyS3Logs",
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::*log*",
                "arn:aws:s3:::*log*/*"
            ]
        }
    ]
}
```

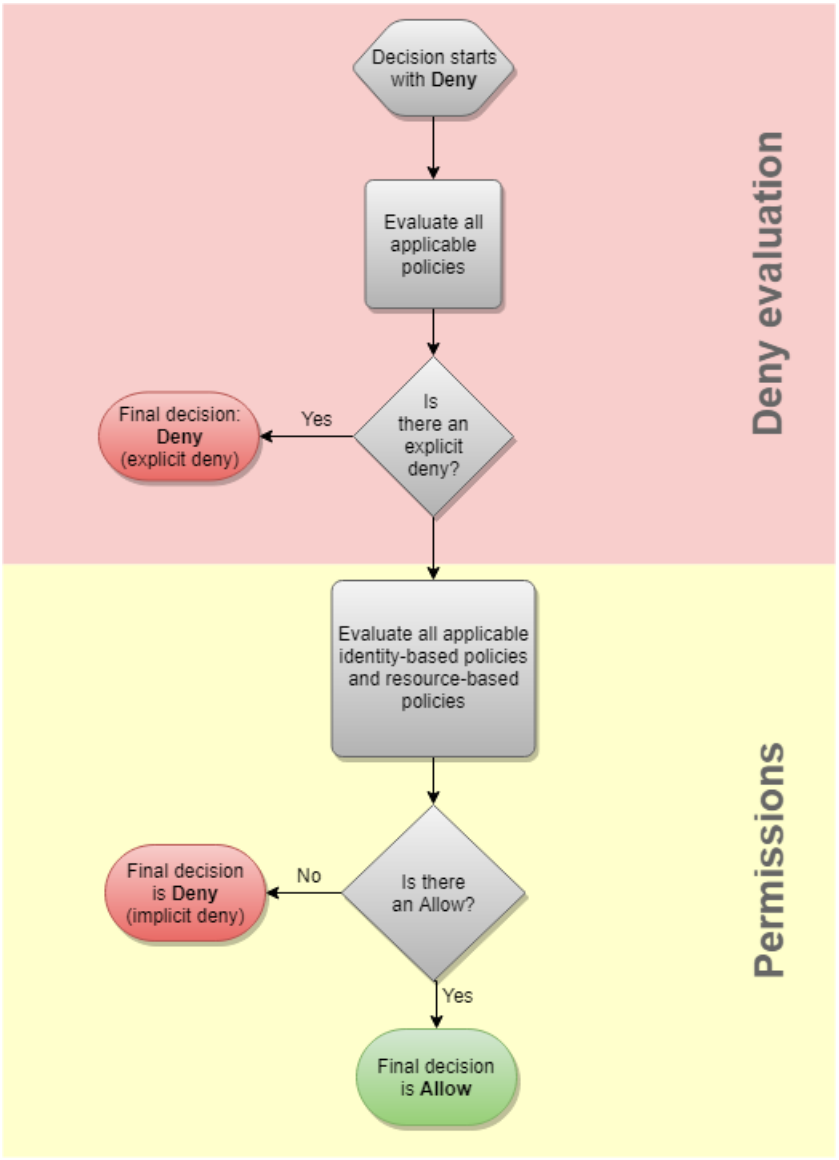
이 정책의 `AllowS3ListRead` 설명문은 카를로스가 계정에 있는 모든 버킷 목록을 보도록 허용합니다. `AllowS3Self` 설명문은 카를로스가 그의 사용자 이름과 동일한 버킷에 모두 액세스할 수 있도록 허용합니다. `DenyS3Logs` 설명문은 카를로스가 그의 이름 아래에 있는 `log`를 통해 모든 S3 버킷의 액세스를 거부합니다.

또한, 다음 리소스 기반 정책(버킷 정책이라고 함)은 `carlossalazar` 버킷에 연결됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Principal": { "AWS": "arn:aws:iam::111122223333:user/carlossalazar" },
            "Resource": "*"
        }
    ]
}
```

이 정책은 `carlossalazar` 사용자만 `carlossalazar` 버킷에 액세스할 수 있도록 지정합니다.

Carlos가 `carlossalazar-logs` 버킷에 파일을 저장하도록 요청하면 AWS는 해당 요청에 어떤 정책을 적용할지 결정합니다. 이 경우, 자격 증명 기반 정책과 리소스 기반 정책만 적용합니다. 이들은 모두 권한 정책입니다. 어떠한 권한 경계도 적용되지 않기 때문에 평가 로직은 다음 로직으로 줄어듭니다.



AWS는 먼저 요청 콘텍스트에 적용되는 `Deny` 설명문을 확인합니다. 자격 증명 기반 정책은 카를로스의 로깅을 통한 모든 S3 버킷의 액세스를 명시적으로 거부하기 때문에 이를 찾습니다. 카를로스의 액세스가 거부됩니다.

Carlos가 실수를 알아차리고 `carlossalazar` 버킷에 파일을 저장하고자 한다고 가정하십시오. AWS는 `Deny` 설명문을 확인하지만 찾지 못합니다. 그러면 권한 정책을 확인합니다. 자격 증명 기반 정책과 리소스 기반 정책 모두 요청을 허용합니다. 따라서 AWS는 요청을 허용합니다. 이들 중 하나라도 설명문을 명시적으로 거부한다면 요청은 거부됩니다. 정책 유형 중 하나는 요청을 허용하고 다른 하나는 요청을 허용하지 않는 경우에도 요청은 허용됩니다.

명시적 거부와 묵시적 거부 차이

적용 가능한 정책이 `Deny` 설명문을 포함한다면 요청은 명시적으로 거부됩니다. 정책이 `Allow` 설명문과 `Deny` 설명문을 포함한 요청에 적용된다면 `Deny` 설명문은 `Allow` 설명문에 우선합니다. 이 요청은 명시적으로 거부됩니다.

적용 가능한 `Deny` 설명문이 없고 적용 가능한 `Allow` 설명문도 없다면 묵시적 거부가 발생합니다. IAM 사용자, 역할 또는 연합된 사용자가 기본적으로 액세스를 거부하기 때문에 명시적으로 작업을 허용해야 합니다. 그렇지 않으면 액세스는 묵시적으로 거부됩니다.

권한 부여 전략을 설계한다면 `Allow` 설명문으로 정책을 생성하여 보안 주체가 성공적으로 요청하도록 허용합니다. 그러나 명시적 또는 묵시적 거부 조합을 선택할 수 있습니다. 예를 들어, 다음 정책을 생성하여 AWS의 모든 리소스에 관리자가 완전히 액세스하도록 허용하지만 결제 액세스를 명시적으로 거부할 수 있습니다. 다른 사람이 관리자에게 다른 정책을 추가하여 결제를 허용하려고 해도 이 명시적 거부 때문에 결제는 여전히 거부됩니다.

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

또한, 다음 정책을 생성하여 그룹 또는 IAM의 기타 리소스가 아닌 사용자가 사용자를 관리할 수 있도록 허용합니다. 이러한 작업은 기타 서비스의 작업처럼 묵시적으로 거부됩니다. 그러나 다른 사람이 정책을 이런 다른 작업을 수행하도록 허용하는 사용자에게 추가한다면 이런 작업이 허용됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:AttachUserPolicy",
            "iam:CreateUser",
            "iam:DeleteUser",
            "iam:DeleteUserPolicy",
            "iam:DetachUserPolicy",
            "iam:GetUser",
            "iam:GetUserPolicy",
            "iam:ListAttachedUserPolicies",
            "iam:ListUserPolicies",
            "iam:ListUsers",
            "iam:PutUserPolicy",
            "iam:UpdateUser"
        ],
        "Resource": "*"
    }
}
```

교차 계정 정책 평가 로직

한 계정의 보안 주체가 두 번째 계정의 리소스에 액세스하도록 허용할 수 있습니다. 이를 교차 계정 액세스라고 합니다. 교차 계정 액세스를 허용할 때 보안 주체가 존재하는 계정을 신뢰할 수 있는 계정이라고 합니다. 리소스가 존재하는 계정을 신뢰하는 계정이라고 합니다.

교차 계정 액세스를 허용하려면 공유하려는 리소스에 리소스 기반 정책을 연결해야 합니다. 또한 요청에서 보안 주체 역할을 하는 자격 증명에 자격 증명 기반 정책을 연결해야 합니다. 신뢰하는 계정의 리소스 기반 정책은 리소스에 액세스할 수 있는 신뢰할 수 있는 계정의 보안 주체를 지정해야 합니다. 전체 계정이나 해당 IAM 사용자, 연동 사용자, IAM 역할 또는 위임된 역할 세션을 지정할 수 있습니다. AWS 서비스를 보안 주체로 지정할 수도 있습니다. 자세한 내용은 보안 주체 지정 (p. 589) 단원을 참조하십시오.

보안 주체의 자격 증명 기반 정책은 신뢰 서비스의 리소스에 대한 요청된 액세스를 허용해야 합니다. 리소스의 ARN을 지정하거나 모든 리소스에 대한 액세스를 허용하여 이 작업을 수행할 수 있습니다(*).

IAM에서는 리소스 기반 정책을 IAM 역할에 연결하여 다른 계정의 보안 주체가 해당 역할을 수임하도록 허용할 수 있습니다. 역할의 리소스 기반 정책을 역할 신뢰 정책이라고 합니다. 이 역할을 가정하면 허용된 보안 주체는 결과로 생성되는 임시 자격 증명을 사용하여 계정의 여러 리소스에 액세스할 수 있습니다. 이러한 액세스 권한은 역할의 자격 증명 기반 권한 정책에 정의되어 있습니다. 자세한 내용은

아래는 역할을 시작하는 데 도움이 되는 몇 가지 기본 용어들입니다.

역할

특정 권한을 가진 계정에 생성할 수 있는 IAM 자격 증명. IAM 역할은 IAM 사용자와 몇 가지 점에서 유사합니다. 역할과 사용자 모두 AWS에서 자격 증명으로 할 수 있는 것과 할 수 없는 것을 결정하는 권한 정책을 포함하는 AWS 자격 증명입니다. 그러나 역할은 한 사람과만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다. 또한 역할에는 그와 연관된 암호 또는 액세스 키와 같은 표준 장기 자격 증명이 없습니다. 그 대신, 역할을 수임하면 역할 세션을 위한 임시 보안 자격 증명을 제공합니다.

역할은 다음의 주체들이 사용할 수 있습니다.

- 동일한 AWS 계정의 IAM 사용자
- 역할과 다른 AWS 계정의 IAM 사용자
- Amazon Elastic Compute Cloud(Amazon EC2)와 같은 AWS가 제공하는 웹 서비스
- SAML 2.0, OpenID Connect 또는 사용자 지정 구축 자격 증명 브로커와 호환되는 외부 자격 증명 공급자(IdP) 서비스에 의해 인증된 외부 사용자

AWS 서비스 역할

서비스가 사용자를 대신하여 사용자 계정에서 작업을 수행하기 위해 수임한 역할입니다. 일부 AWS 서비스 환경을 설정할 때, 서비스에서 맡을 역할을 정의해야 합니다. 이 서비스 역할에는 서비스가 AWS 리소스에 액세스하는 데 필요한 모든 권한이 포함되어야 합니다. 서비스 역할은 서비스마다 다르지만, 해당 서비스에 대한 문서화된 요구 사항을 충족하는 한 대부분의 경우 권한을 선택할 수 있습니다. 서비스 역할은 해당 계정 내에서만 액세스를 제공하며 다른 계정의 서비스에 대한 액세스를 부여하는 데 사용할 수 없습니다. IAM 내에서 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다.

EC2 인스턴스의 AWS 서비스 역할

Amazon EC2 인스턴스에서 실행 중인 애플리케이션이 계정에서 작업을 수행하기 위해 맡을 수 있는 특수한 유형의 서비스 역할 이 역할은 시작된 EC2 인스턴스에 할당됩니다. 해당 인스턴스에서 실행 중인 애플리케이션은 임시 보안 자격 증명을 검색하고 역할이 허용하는 작업을 수행할 수 있습니다. EC2 인스턴스의 서비스 역할 사용에 대한 세부 정보는 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기 (p. 265)를 참조하십시오.

AWS 서비스 연결 역할

AWS 서비스에 직접 연결된 고유한 유형의 서비스 역할입니다. 서비스 연결 역할은 해당 서비스에서 사전 정의하며 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모

든 권한을 포함합니다. 또한 연결된 서비스는 서비스 연결 역할을 만들고 수정하며 삭제하는 방법을 정의합니다. 서비스는 역할을 자동으로 만들거나 삭제할 수 있습니다. 서비스의 프로세스나 마법사를 사용하여 사용자가 역할을 만들거나 수정하거나 삭제하도록 허용할 수도 있습니다. 또는 사용자가 IAM을 사용하여 역할을 만들거나 삭제하도록 요구할 수도 있습니다. 방법이 어떻든, 서비스 연결 역할은 필요한 권한을 수동으로 추가할 필요가 없으므로 서비스를 더 쉽게 설정할 수 있습니다.

> **Note**
>
> 서비스 연결 역할 지원을 시작할 때 이미 서비스를 사용하는 중이라면 계정의 새 역할에 대해 알려주는 이메일을 받게 될 수 있습니다. 이 경우 서비스에서 계정에 서비스 연결 역할을 자동으로 생성합니다. 이 역할을 지원하기 위해 어떤 작업도 수행할 필요가 없으며, 이 역할을 수동으로 삭제할 수 없습니다. 자세한 내용은 내 AWS 계정에 표시되는 새 역할 (p. 553) 단원을 참조하십시오.

서비스 연결 역할의 사용을 지원하는 서비스에 대한 자세한 내용은 IAM로 작업하는 AWS 서비스 (p. 573)를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾으십시오. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [Yes] 링크를 선택합니다. 서비스에 서비스 연결 역할 만들기, 수정 또는 삭제에 대한 설명서가 포함되어 있지 않으면 IAM 콘솔, AWS CLI 또는 API를 사용하면 됩니다. 자세한 내용은 서비스 연결 역할 사용 (p. 218) 단원을 참조하십시오.

역할 함께 묶기

역할 함께 묶기는 AWS CLI 또는 API를 통해 역할을 사용하여 두 번째 역할을 수임하는 경우 발생합니다. 예를 들어, `User1`에게 `RoleA` 및 `RoleB`를 맡을 권한이 있다고 가정해 보겠습니다. 또한 `RoleA`에는 `RoleB`를 맡을 권한이 있습니다. `AssumeRole` API 작업에서 `User1`의 장기 사용자 자격 증명을 사용하여 `RoleA`를 맡을 수 있습니다. 이 작업은 `RoleA`의 단기 자격 증명을 반환합니다. 역할 체인에 참여하기 위해 `RoleA`의 단기 자격 증명을 사용하여 `RoleB`를 맡을 수 있습니다.

역할을 맡을 때 세션 태그를 전달하고 태그를 전이적으로 설정할 수 있습니다. 전이적 세션 태그는 역할 체인의 모든 후속 세션에 전달됩니다. 세션 태그에 대한 자세한 내용은 AWS STS에서 세션 태그 전달 (p. 294) 단원을 참조하십시오.

역할 체인을 사용하면 AWS CLI 또는 AWS API 역할 세션이 최대 1시간으로 제한됩니다. AssumeRole API 작업을 사용하여 역할을 수임할 때 `DurationSeconds` 파라미터를 사용하여 역할 세션 길이를 지정할 수 있습니다. 역할에 대한 최대 세션 기간 설정 (p. 251)에 따라 파라미터 값을 최대 43200초(12시간)까지 지정할 수 있습니다. 그러나 역할 함께 묶기를 사용해 역할을 수임하고 1시간보다 큰 `DurationSeconds` 파라미터 값을 지정하면 작업이 실패합니다.

AWS에서는 역할을 사용하여 EC2 인스턴스에서 실행되는 애플리케이션에 권한을 부여 (p. 265)하는 것을 역할 함께 묶기로 간주하지 않습니다.

위임

제어하는 리소스에 대한 액세스를 허용하는 권한을 누군가에게 부여하는 것입니다. 위임은 두 계정 간에 신뢰를 설정하는 것을 포함합니다. 첫 번째는 리소스를 소유한 계정입니다(신뢰하는 계정). 두 번째는 리소스에 액세스해야 하는 사용자가 포함된 계정입니다(신뢰되는 계정). 신뢰받는 계정과 신뢰하는 계정은 다음 중 하나가 될 수 있습니다.

- 동일 계정
- 조직에서 통제하는 별도의 계정
- 서로 다른 조직이 소유한 2개의 계정

리소스에 대한 액세스 권한을 위임하려면, 2개의 정책 (p. 177)이 연결되어 있는 IAM 역할을 생성 (p. 226)합니다. 권한 정책은 역할 사용자에게 리소스에 대해 의도한 작업을 수행하는 데 필요한 권한을 부여합니다. 신뢰 정책은 역할을 위임하도록 허용된 신뢰할 수 있는 계정 멤버를 지정합니다.

신뢰 정책을 생성할 때 와일드카드(*)를 보안 주체로 지정할 수 없습니다. 신뢰 정책은 신뢰하는 계정의 역할에 연결되어 있고 권한의 절반에 해당합니다. 나머지 절반은 사용자에게 역할 전환 또는 위임을 허용하는 (p. 252) 신뢰받는 계정의 사용자에게 연결된 권한 정책입니다. 임시로 역할을 위임하는 사용자는 자신의 고유 권한을 포기하고 대신 해당 역할의 권한을 위임합니다. 사용자가 역할을 끝내거나 역할 사용을 중지하면 원래 사용자 권한이 자동으로 회복됩니다. 외부 ID (p. 229)라 불리는 부가적인 파라미터는 동일한 조직에 의해 제어되지 않는 계정 사이에서 역할을 안전하게 사용하도록 하는 데 도움이 됩니다.

연동

외부 자격 증명 공급자와 AWS 사이에 신뢰 관계를 생성하는 것입니다. 사용자들은 Login with Amazon, Facebook, Google 또는 OpenID Connect(OIDC)와 호환되는 IdP 등의 웹 자격 증명 공급자에 로그인할 수 있습니다. 또한, 사용자는 Microsoft Active Directory 연동 서비스와 같은 Security Assertion Markup Language(SAML) 2.0과 호환되는 엔터프라이즈 자격 증명 시스템에 로그인할 수 있습니다. OIDC 및 SAML 2.0을 사용해 이 외부 자격 증명 공급자와 AWS 사이에 신뢰 관계를 구성할 때, 사용자에게는 IAM 역할이 할당됩니다. 사용자는 임시 보안 자격 증명을 부여받아 AWS 리소스에 대한 액세스가 가능합니다.

연합된 사용자

IAM 사용자를 만드는 대신 AWS Directory Service의 기존 자격 증명, 엔터프라이즈 사용자 디렉터리 또는 웹 자격 증명 공급자를 사용할 수 있습니다. 이 사용자를 연합된 사용자라고 합니다. AWS에서는 자격 증명 공급자 (p. 183)를 통해 액세스가 요청되면 연합된 사용자에게 역할을 할당합니다. 연합된 사용자에 대한 자세한 내용은 IAM 사용 설명서의 연합된 사용자 및 역할 (p. 12)을 참조하십시오.

신뢰 정책

역할을 맡기 위해 신뢰할 보안 주체를 정의하는 JSON 정책 문서 (p. 637)입니다. 역할 신뢰 정책은 IAM의 역할에 연결된 필수 리소스 기반 정책 (p. 350)입니다. 신뢰 정책에서 지정할 수 있는 보안 주체 (p. 589)에는 사용자, 역할, 계정 및 서비스가 포함됩니다.

권한 정책

JSON 형식의 권한 문서로, 역할이 사용할 수 있는 리소스와 작업을 정의합니다. 이 문서는 IAM 정책 언어 (p. 586)의 규칙에 따라 작성됩니다.

권한 경계

자격 증명 기반 정책이 역할에 부여할 수 있는 최대 권한을 제한하는 정책을 사용하는 고급 기능입니다. 서비스 연결 역할에 권한 경계를 적용할 수 없습니다. 자세한 내용은 IAM 엔터티에 대한 권한 경계 (p. 363) 단원을 참조하십시오.

Principal

작업을 수행하고 리소스에 액세스할 수 있는 AWS의 개체입니다. 보안 주체는 AWS 계정 루트 사용자, IAM 사용자 또는 역할입니다. 리소스에 액세스할 수 있는 권한을 다음 두 가지 중 한 가지 방식으로 부여할 수 있습니다.

- 권한 정책을 사용자에게(직접 또는 그룹을 통해 간접적으로) 또는 역할에게 연결할 수 있습니다.
- 리소스 기반 정책 (p. 12)을 지원하는 서비스의 경우 해당 리소스에 연결된 정책의 `Principal` 요소에서 보안 주체를 식별할 수 있습니다.

AWS 계정을 보안 주체로 참조하는 경우 그 보안 주체는 일반적으로 해당 계정 내에서 정의된 모든 보안 주체를 의미합니다.

Note

역할의 신뢰 정책에서 `Principal` 요소에 와일드카드(*)를 사용할 수 없습니다.

교차 계정 액세스를 위한 역할

한 계정의 리소스에 대한 액세스 권한을 다른 계정의 신뢰할 수 있는 보안 주체에 부여하는 역할. 역할은 교차 계정 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 제

품을 사용하면 (역할을 프록시로 사용하는 대신) 리소스에 직접 정책을 연결할 수 있습니

다. 이를 리소스 기반 정책이라고 하며, 이 정책을 사용하여 다른 AWS 계정의 보안 주체에게 리소스에 대한 액세스 권한을 부여할 수 있습니다. 이러한 리소스에는 Amazon Simple Storage Service(S3) 버킷, S3 Glacier 볼트, Amazon Simple Notification Service(SNS) 주제 및 Amazon Simple Queue Service(SQS) 대기열이 포함됩니다. 리소스 기반 정책을 지원하는 서비스에 대한 자세한 내용은 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오. 리소스 기반 정책에 대한 자세한 내용은 IAM 역할과 리소스 기반 정책의 차이 (p. 287) 단원을 참조하십시오.
(p. 177) 단원을 참조하십시오. 역할을 사용하여 교차 계정 액세스를 허용하는 것과 다른 리소스 기반 정책을 사용하여 교차 계정 액세스를 허용하는 것이 어떻게 다른지 알아보려면 IAM 역할과 리소스 기반 정책의 차이 (p. 287) 단원을 참조하십시오.

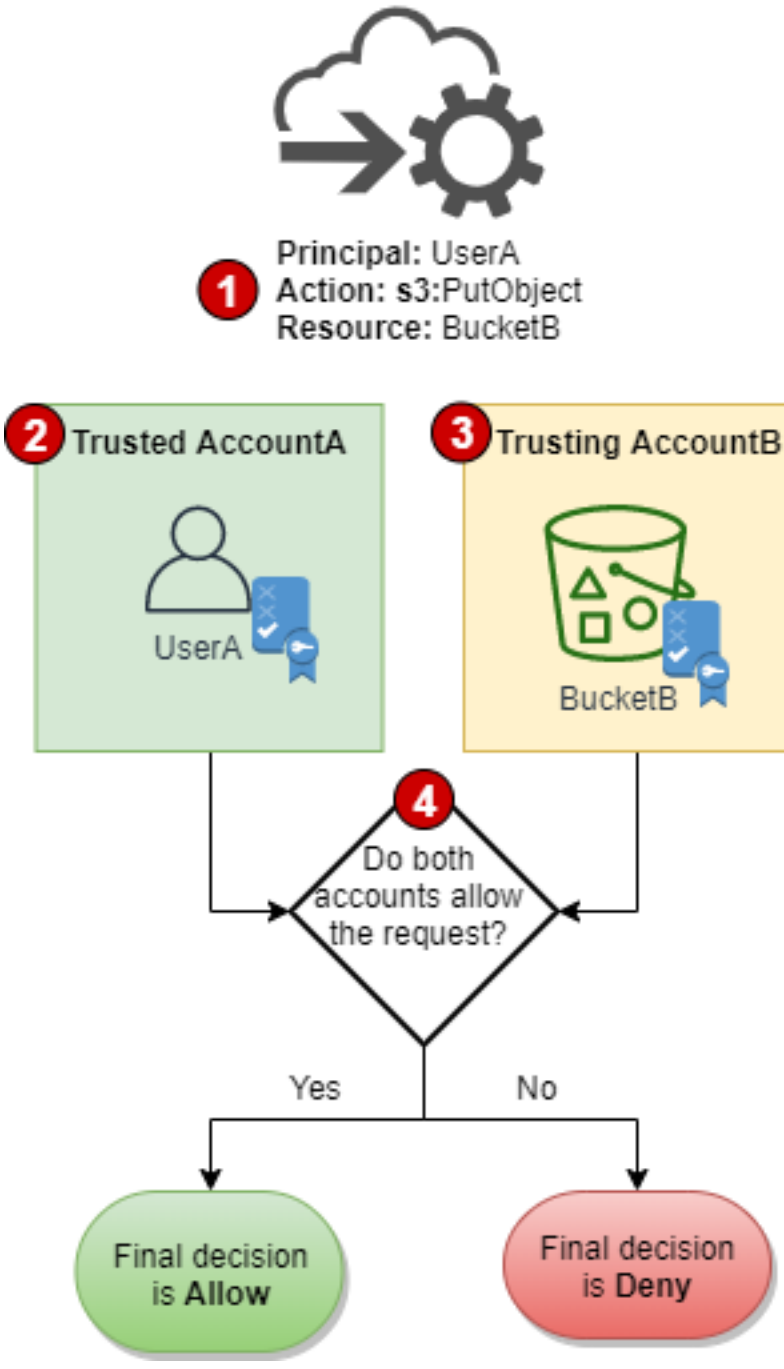
Important

다른 서비스는 정책 평가 로직에 영향을 줄 수 있습니다. 예를 들어 AWS Organizations에서는 하나 이상의 보안 주체 계정에 서비스 제어 정책을 적용할 수 있도록 지원합니다. AWS 리소스 액세스 관리자에서는 보안 주체가 공유되는 리소스에서 수행할 수 있는 작업을 제어하는 정책 조각을 지원합니다.

교차 계정 요청의 허용 여부 결정

교차 계정 요청의 경우 신뢰할 수 있는 `AccountA`의 요청자가 자격 증명 기반 정책을 가지고 있어야 합니다. 이 정책은 신뢰하는 `AccountB`에서 리소스에 대한 요청을 생성할 수 있도록 허용해야 합니다. 또한 `AccountB`의 리소스 기반 정책은 `AccountA`의 요청자가 리소스에 액세스할 수 있도록 허용해야 합니다.

사용자가 교차 계정 요청을 하면 AWS에서는 두 가지 평가를 수행합니다. AWS는 신뢰하는 계정 및 신뢰할 수 있는 계정에서 요청을 평가합니다. 단일 계정 내에서 요청을 평가하는 방법에 대한 자세한 내용은 계정 내에서 요청 허용 여부 결정 (p. 625) 단원을 참조하십시오. 두 평가에서 모두 `Allow`라는 결정을 반환하는 경우에만 요청이 허용됩니다.



1. 한 계정의 보안 주체가 다른 계정의 리소스에 액세스하도록 요청하는 경우 이는 교차 계정 요청입니다.
2. 요청한 보안 주체는 신뢰할 수 있는 계정(`AccountA`)에 존재합니다. AWS는 이 계정을 평가할 때 자격 증명 기반 정책 및 자격 증명 기반 정책을 제한할 수 있는 정책을 확인합니다. 자세한 내용은 단일 계정 내에서 정책 평가 (p. 623) 단원을 참조하십시오.
3. 요청된 리소스가 신뢰하는 계정(`AccountB`)에 존재합니다. AWS는 이 계정을 평가할 때 요청된 리소스에 연결된 리소스 기반 정책과 리소스 기반 정책을 제한할 수 있는 정책을 확인합니다. 자세한 내용은 단일 계정 내에서 정책 평가 (p. 623) 단원을 참조하십시오.
4. AWS에서는 두 계정 정책 평가에서 모두 요청을 허용하는 경우에만 요청을 허용합니다.

교차 계정 정책 평가의 예

다음 예제에서는 한 계정의 사용자에게 두 번째 계정의 리소스 기반 정책에 의해 권한이 부여되는 시나리오를 보여 줍니다.

카를로스가 계정 1111111111111에 `carlossalazar`라는 이름의 IAM 사용자가 있는 개발자라고 가정합니다. 그는 계정 222222222222에 있는 `Production-logs` Amazon S3 버킷에 파일을 저장하려고 합니다.

또한 다음 정책이 `carlossalazar` IAM 사용자와 연결되었다고 가정하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3ListRead",
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Sid": "AllowS3ProductionObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object*",
            "Resource": "arn:aws:s3:::Production/*"
        },
        {
            "Sid": "DenyS3Logs",
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::*log*",
                "arn:aws:s3:::*log*/*"
            ]
        }
    ]
}
```

이 정책의 `AllowS3ListRead` 문은 카를로스가 Amazon S3에 있는 모든 버킷의 목록을 보도록 허용합니다. `AllowS3ProductionObjectActions` 문은 Carlos에게 `Production` 버킷의 객체에 대한 전체 액세스를 허용합니다. `DenyS3Logs` 설명문은 카를로스가 그의 이름 아래에 있는 `log`를 통해 모든 S3 버킷의 액세스를 거부합니다. 또한 해당 버킷의 모든 객체에 대한 액세스를 거부합니다.

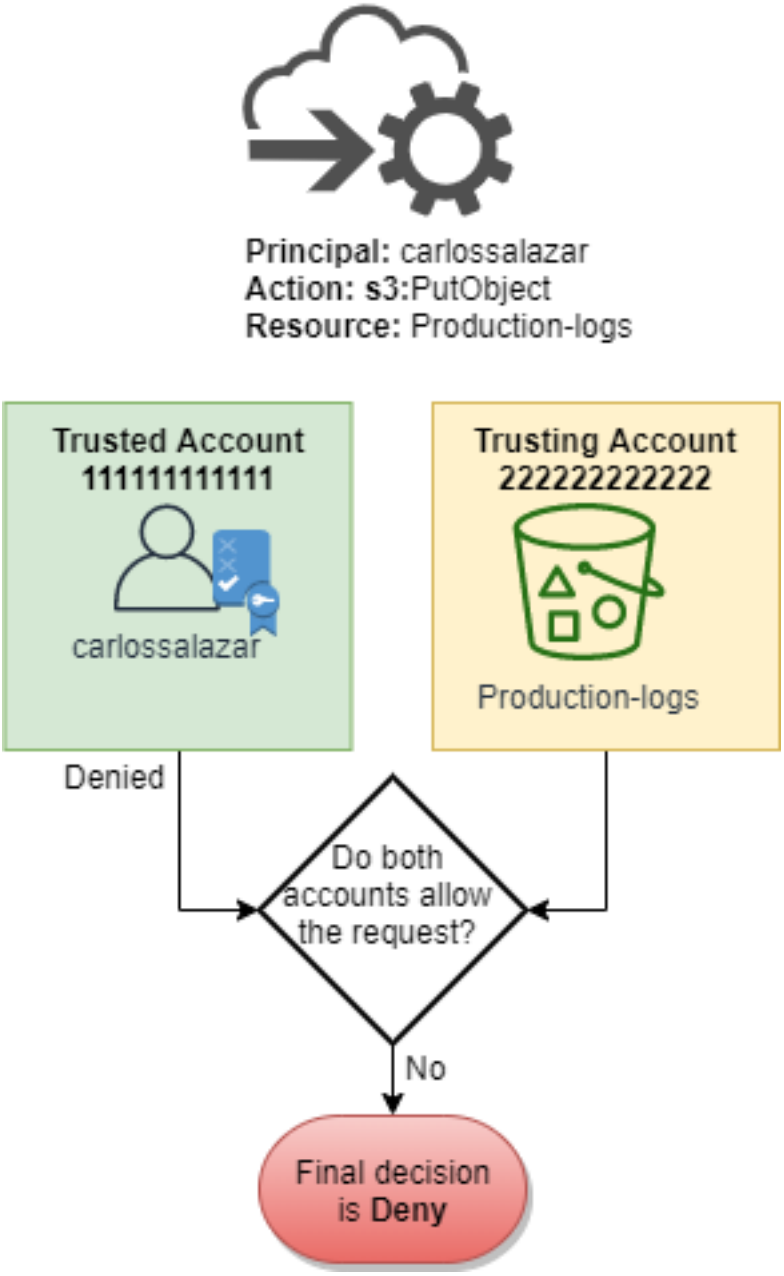
또한, 다음 리소스 기반 정책(버킷 정책이라고 함)은 계정 222222222222의 `Production` 버킷에 연결됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject*",
                "s3:PutObject*",
                "s3:ReplicateObject",
                "s3:RestoreObject"
            ],
            "Principal": { "AWS": "arn:aws:iam::111111111111:user/carlossalazar" },
            "Resource": "arn:aws:s3:::Production/*"
        }
    ]
}
```

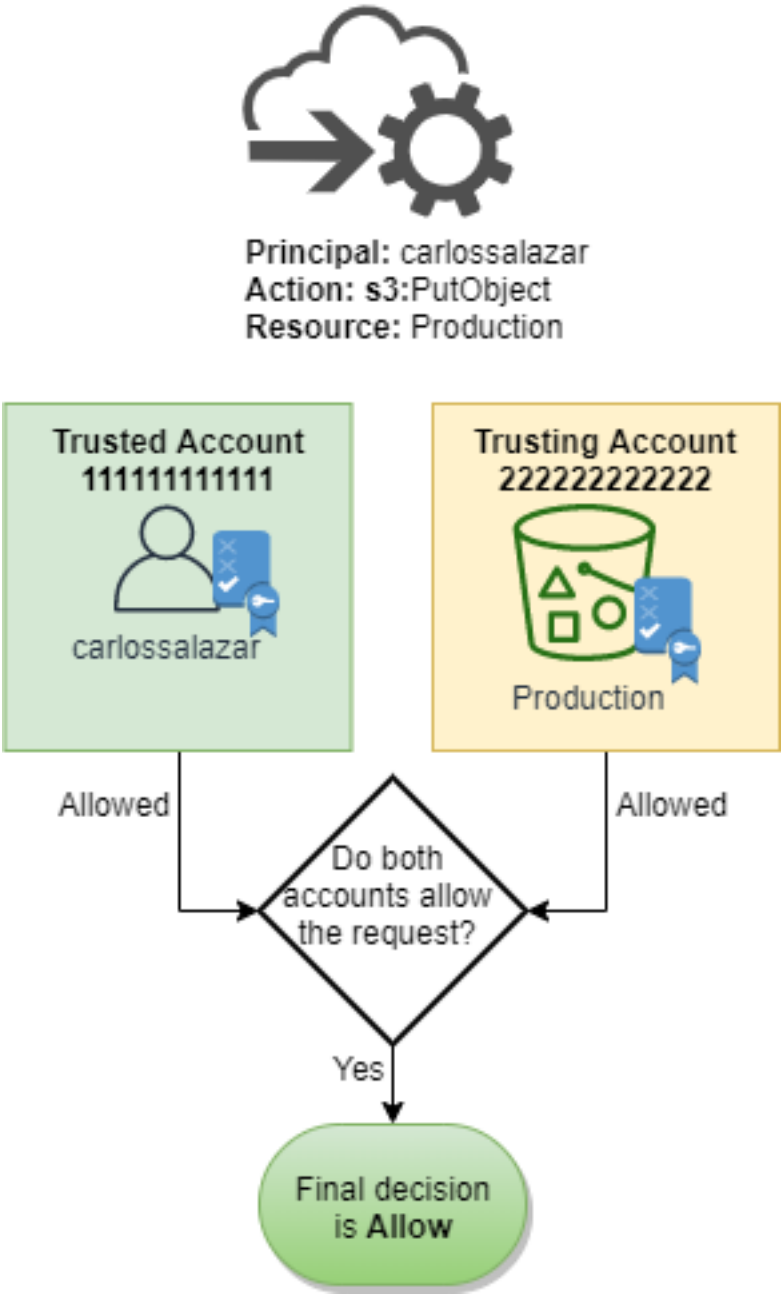
이 정책은 `carlossalazar` 사용자에게 `Production` 버킷의 객체에 대한 액세스를 허용합니다. 그는 버킷의 객체를 생성하고 편집할 수는 있지만 삭제할 수는 없습니다. 그는 버킷 자체를 관리할 수 없습니다.

카를로스가 `Production-logs` 버킷에 파일을 저장하도록 요청하면 AWS는 해당 요청에 어떤 정책을 적용할지 결정합니다. 이 경우 `carlossalazar` 사용자에게 연결된 자격 증명 기반 정책이 계정 `111111111111`에 적용되는 유일한 정책입니다. 계정 `222222222222`에서는 `Production-logs` 버킷에 연결된 리소스 기반 정책이 없습니다. AWS은 계정 `111111111111`을 평가할 때 `Deny`의 결정을 반환합니다. 이는 자격 증명 기반 정책의 `DenyS3Logs` 문이 모든 로그 버킷에 대한 액세스를 명시적으로 거부하기 때문입니다. 단일 계정 내에서 요청을 평가하는 방법에 대한 자세한 내용은 계정 내에서 요청 허용 여부 결정 (p. 625) 단원을 참조하십시오.

요청이 계정 중 하나에서 명시적으로 거부되기 때문에 최종 결정은 요청을 거부하는 것입니다.



카를로스가 자신의 실수를 깨닫고 `Production` 버킷에 파일을 저장하려고 시도한다고 가정합니다. AWS는 먼저 계정 `111111111111`을 확인하여 요청이 허용되는지 여부를 확인합니다. 자격 증명 기반 정책만 적용되며 요청을 허용합니다. 그리고 AWS는 계정 `222222222222`를 확인합니다. `Production` 버킷에 연결된 리소스 기반 정책만 적용되며 요청을 허용합니다. 두 계정 모두 요청을 허용하므로 최종 결정은 요청을 허용하는 것입니다.



IAM JSON 정책 언어의 문법

이 페이지에서는 IAM에서 JSON 정책 생성 시 사용되는 언어의 정규 문법에 대해 살펴보겠습니다. 이 문법에 대해 살펴본 후 정책의 체계적 작성 및 검증 방법에 대해 이해할 수 있게 될 것입니다.

정책 예는 다음 주제를 참조하십시오.

- 정책 및 권한 (p. 349)
- IAM 자격 증명 기반 정책 예제 (p. 387)
- Linux 인스턴스용 Amazon EC2 사용 설명서의 Amazon EC2 콘솔 작업을 위한 예제 정책 및 AWS CLI, Amazon EC2 CLI 또는 AWS SDK 작업을 위한 예제 정책
- Amazon Simple Storage Service 개발자 가이드의 버킷 정책 예제 및 사용자 정책 예제

다른 AWS 서비스의 정책 예는 해당 서비스 설명서를 참조하십시오.

주제

- 정책 언어 및 JSON (p. 638)
- JSON 문법에 사용되는 규칙 (p. 638)
- 문법 (p. 639)
- 정책 문법 참고 사항 (p. 640)

정책 언어 및 JSON

정책은 JSON으로 작성됩니다. 정책을 IAM에 제출하면 먼저 검증을 통해 JSON 구문의 정확성을 확인합니다. 여기에서는 유효한 JSON 구성에 대해 자세히 설명하지는 않지만 다음과 같이 몇 가지 기본 JSON 규칙을 소개합니다.

- 각 개체 간에 공백을 넣을 수 있습니다.
- 값은 인용 부호로 묶입니다. 숫자나 부울(Boolean) 값에서 인용 부호는 옵션입니다.
- 대부분 요소(예: `action_string_list`, `resource_string_list`)는 JSON 배열을 값으로 사용할 수 있습니다. 배열은 하나 이상의 값을 갖습니다. 값이 2개 이상 추가되면 배열은 다음 예제와 같이 대괄호([및])로 묶여 쉼표로 구분됩니다.

  ```
  "Action" : ["ec2:Describe*","ec2:List*"]
  ```
- 기본 JSON 데이터 형식(부울, 숫자, 문자열)은 RFC 7159에 정의되어 있습니다.

정책 구문은 JSON 검증기를 사용해 검사합니다. 검증기는 온라인에서 찾아볼 수 있으며, 그 밖에 JSON 검증 기능을 지원하는 코드 편집기나 XML 편집 도구도 많습니다.

JSON 문법에 사용되는 규칙

JSON 문법에는 다음과 같은 규칙이 사용됩니다.

- 다음 문자는 JSON 토큰으로서 정책에 추가됩니다.

  ```
  { } [ ] " , :
  ```
- 다음은 문법에 사용되는 특수 문자로서 정책에는 추가되지 않습니다.

  ```
  = < > ( ) |
  ```
- 한 요소에 여러 값을 추가할 수 있는 경우에는 반복되는 값, 쉼표 구분자, 그리고 줄임표(`...`)를 사용하여 나타냅니다. 예:

  ```
  [<action_string>, <action_string>, ...]
  ```

  ```
  <principal_map> = { <principal_map_entry>, <principal_map_entry>, ... }
  ```

  여러 값이 허용되면 단일 값을 추가하는 것도 유효합니다. 값이 단 하나인 경우에는 마지막 쉼표를 반드시 생략해야 합니다. 요소가 배열([ ]로 표시)로 이루어지더라도 추가된 값이 단 하나일 때는 괄호가 선택 사항입니다. 예:

```
"Action": [<action_string>]

"Action": <action_string>
```

- 요소 뒤에 나오는 물음표(?)는 요소가 선택 사항인 것을 나타냅니다. 예:

```
<version_block?>
```

  하지만 선택 요소에 대한 자세한 내용은 문법 목록 이후에 나오는 참고 사항을 반드시 확인하시기 바랍니다.
- 요소 사이의 수직선(|)은 다자간 택일을 나타냅니다. 이 문법에서는 괄호로 다자간 택일의 범위를 정의합니다. 예:

```
("Principal" | "NotPrincipal")
```

- 리터럴 문자열 요소는 큰따옴표(")로 묶습니다. 예:

```
<version_block> = "Version" : ("2008-10-17" | "2012-10-17")
```

기타 참고 사항은 문법 목록 다음 정책 문법 참고 사항 (p. 640) 단원을 참조하십시오.

문법

다음 목록은 정책 언어 문법에 대한 설명입니다. 문법 목록에 사용된 규칙에 대해서는 앞의 단원을 참조하십시오. 그리고, 추가 정보는 이후 참고 사항을 참조하십시오.

> **Note**
>
> 이 문법은 버전이 `2008-10-17` 및 `2012-10-17`이라고 표시된 정책에 대한 설명입니다. `Version` 정책 요소는 정책 버전과 다릅니다. `Version` 정책 요소는 정책 내에서 사용되며 정책 언어의 버전을 정의합니다. 반면에 정책 버전은 IAM에서 고객 관리형 정책을 변경할 때 생성됩니다. 변경된 정책은 기존 정책을 덮어쓰지 않습니다. 대신 IAM에서 관리형 정책의 새 버전을 만듭니다. `Version` 정책 요소에 대한 자세한 내용은 IAM JSON 정책 요소: Version (p. 587)을 참조하십시오. 정책 버전에 대한 자세한 내용은 the section called “IAM 정책 버전 관리” (p. 458) 단원을 참조하십시오.

```
policy  = {
     <version_block?>
     <id_block?>
     <statement_block>
}

<version_block> = "Version" : ("2008-10-17" | "2012-10-17")

<id_block> = "Id" : <policy_id_string>

<statement_block> = "Statement" : [ <statement>, <statement>, ... ]

<statement> = {
    <sid_block?>,
    <principal_block?>,
    <effect_block>,
    <action_block>,
    <resource_block>,
    <condition_block?>
}

<sid_block> = "Sid" : <sid_string>

<effect_block> = "Effect" : ("Allow" | "Deny")

<principal_block> = ("Principal" | "NotPrincipal") : ("*" | <principal_map>)
```

```
<principal_map> = { <principal_map_entry>, <principal_map_entry>, ... }

<principal_map_entry> = ("AWS" | "Federated" | "Service" | "CanonicalUser") :
    [<principal_id_string>, <principal_id_string>, ...]

<action_block> = ("Action" | "NotAction") :
    ("*" | [<action_string>, <action_string>, ...])

<resource_block> = ("Resource" | "NotResource") :
    ("*" | [<resource_string>, <resource_string>, ...])

<condition_block> = "Condition" : { <condition_map> }
<condition_map> = {
  <condition_type_string> : { <condition_key_string> : <condition_value_list> },
  <condition_type_string> : { <condition_key_string> : <condition_value_list> }, ...
}
<condition_value_list> = [<condition_value>, <condition_value>, ...]
<condition_value> = ("string" | "number" | "Boolean")
```

정책 문법 참고 사항

- 단일 정책에는 다수의 문이 배열로 추가될 수 있습니다.
- 정책은 추가되는 개체에 따라 2,048~10,240 사이에서 최대 문자 수를 갖습니다. 자세한 내용은 IAM 및 STS 제한 (p. 569) 단원을 참조하십시오. 정책 크기 계산에 공백 문자는 포함되지 않습니다.
- 개별 요소에는 동일한 키 인스턴스를 여러 개 추가할 수 없습니다. 예를 들어 동일한 문에 `Effect` 블록을 2개 추가할 수는 없습니다.
- 블록은 순서에 상관없이 표시됩니다. 예를 들어 정책에서 `version_block`은 `id_block` 뒤에 올 수 있습니다. 마찬가지로 `effect_block`, `principal_block` 및 `action_block` 역시 동일 문에서 순서에 상관없이 표시됩니다.
- 리소스 기반 정책에서는 `id_block`이 선택 사항입니다. ID 기반 정책에는 포함시킬 수 없습니다.
- `principal_block` 요소는 리소스 기반 정책(예: Amazon S3 버킷 정책)과 IAM 역할의 신뢰 정책에 필요합니다. ID 기반 정책에는 포함시킬 수 없습니다.
- Amazon S3 버킷 정책의 `principal_map` 요소에는 `CanonicalUser` ID가 포함될 수 있습니다. 대부분 리소스 기반 정책은 이러한 매핑을 지원하지 않습니다. 버킷 정책에서 정식 사용자 ID를 사용하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 정책에서 보안 주체 지정 단원을 참조하십시오.
- 각 문자열 값(`policy_id_string`, `sid_string`, `principal_id_string`, `action_string`, `resource_string`, `condition_type_string`, `condition_key_string`, 그리고 `condition_value`의 문자열 버전)은 자체적인 최소/최대 길이 제한, 특정 허용 값 또는 필수 내부 포맷을 가질 수 있습니다.

문자열 값에 대한 참고 사항

이 섹션에서는 정책에서 각각 다른 요소에 사용되는 문자열 값에 대한 추가 정보에 대해 살펴보겠습니다.

`action_string`

서비스 네임스페이스, 콜론 및 작업 이름으로 구성됩니다. 작업 이름에는 와일드카드를 추가할 수 있습니다. 예:

```
"Action":"ec2:StartInstances"

"Action":[
  "ec2:StartInstances",
  "ec2:StopInstances"
]
```

```
"Action":"cloudformation:*"

"Action":"*"

"Action":[
  "s3:Get*",
  "s3:List*"
]
```

policy_id_string

정책 관련 정보를 전체적으로 추가하는 방법을 제공합니다. Amazon SQS나 Amazon SNS 같은 일부 서비스는 `Id` 요소를 예약 방식으로 사용합니다. 개별 서비스에서 달리 제한하지 않는다면 policy_id_string에 공백을 추가할 수 있습니다. AWS 계정 내에서 이 값의 고유성을 요구하는 서비스도 있습니다.

> **Note**
>
> `id_block`은 리소스 기반 정책에서는 허용되지만 ID 기반 정책에서는 사용할 수 없습니다.

이 문자열이 제한된 전체 정책 길이에 영향을 끼치기는 하지만 문자열 길이에 제한은 없습니다.

```
"Id":"Admin_Policy"

"Id":"cd3ad3d9-2776-4ef1-a904-4c229d1642ee"
```

sid_string

개별 문에 대한 정보를 추가하는 방법을 제공합니다. IAM 정책의 경우 기본 영숫자 문자(A-Z,a-z,0-9)만 `Sid` 값의 문자로 허용됩니다. 리소스 정책을 지원하는 다른 AWS 서비스는 `Sid` 값 요구 사항이 다를 수 있습니다. 예를 들어 일부 서비스는 이 값이 특정 AWS 계정에서 고유할 것을 요구하며, 일부 서비스는 `Sid` 값으로 공백과 같은 문자를 추가로 허용합니다.

```
"Sid":"1"

"Sid": "ThisStatementProvidesPermissionsForConsoleAccess"
```

principal_id_string

AWS 계정, IAM 사용자, IAM 역할, 연동 사용자 또는 위임된 역할 사용자의 Amazon 리소스 이름(ARN) (p. 564)을 사용해 보안 주체를 지정하는 방법을 제공합니다. AWS 계정의 경우, 전체 ARN 대신 짧은 형식인 `AWS:`*`accountnumber`*를 사용할 수도 있습니다. AWS 서비스, 위임된 역할 등을 포함한 모든 옵션에 대해서는 보안 주체 지정 (p. 589) 단원을 참조하십시오.

"모든 사용자/익명 사용자"를 지정할 때만 *를 사용할 수 있습니다. 이름이나 ARN의 일부를 지정하기 위해 사용할 수는 없습니다.

resource_string

대부분의 경우 Amazon 리소스 이름 (p. 564)(ARN)으로 구성됩니다.

```
"Resource":"arn:aws:iam::123456789012:user/Bob"

"Resource":"arn:aws:s3:::examplebucket/*"
```

condition_type_string

`StringEquals`, `StringLike`, `NumericLessThan`, `DateGreaterThanEquals`, `Bool`, `BinaryEquals`, `IpAddress`, `ArnEquals` 등 테스트할 조건 형식을 식별합니다. 조건 형식에 대한 전체 목록은 IAM JSON; 정책 요소: 조건 연산자 (p. 601) 단원을 참조하십시오.

```
"Condition": {
```

```
  "NumericLessThanEquals": {
    "s3:max-keys": "10"
  }
}

"Condition": {
  "Bool": {
    "aws:SecureTransport": "true"
  }
}

"Condition": {
  "StringEquals": {
      "s3:x-amz-server-side-encryption": "AES256"
   }
}
```

condition_key_string

값을 테스트하여 조건 충족 여부를 판단할 수 있는 조건 키를 식별합니다. AWS는 `aws:principaltype`, `aws:SecureTransport` 및 `aws:userid`를 포함하여 모든 AWS 서비스에서 사용할 수 있는 조건 키 집합을 정의합니다.

AWS 조건 키 목록에 대한 자세한 내용은 AWS 전역 조건 컨텍스트 키 (p. 650) 단원을 참조하십시오. 서비스별 조건 키에 대한 자세한 내용은 다음과 같은 서비스 설명서를 참조하십시오.

- Amazon Simple Storage Service 개발자 가이드의 정책에서 조건 지정
- Linux 인스턴스용 Amazon EC2 사용 설명서의 Amazon EC2에 대한 IAM 정책.

```
"Condition":{
  "Bool": {
      "aws:SecureTransport": "true"
   }
}

"Condition": {
  "StringNotEquals": {
      "s3:x-amz-server-side-encryption": "AES256"
   }
}

"Condition": {
  "StringEquals": {
    "ec2:ResourceTag/purpose": "test"
  }
}
```

직무 기능에 대한 AWS 관리형 정책

직무에 관한 AWS 관리형 정책은 IT 업계의 일반적인 직무 기능과 긴밀하게 연결되도록 구성됩니다. 이 정책을 적용하면 특정 직무 담당자에게 기대되는 작업 수행에 필요한 권한을 쉽게 부여할 수 있습니다. 이 정책은 여러 서비스에 대한 권한을 정책 하나에 통합하기 때문에, 여러 정책에 권한이 분산되어 있는 경우보다 업무 절차가 간소합니다.

직무 기능에 관한 이 정책은 모든 그룹, 사용자 또는 역할에 연결할 수 있습니다.

역할을 이용한 서비스 결합

일부 정책은 IAM 서비스 역할을 이용하여 다른 AWS 서비스에 포함된 기능을 활용할 수 있도록 지원합니다. 이 정책은 `iam:passrole`에 대한 액세스를 허용하여, 정책에 정의된 사용자가 역할을 AWS 서비스에 전달할 수 있도록 합니다. 이 역할은 AWS 서비스에서 사용자를 대행할 수 있도록 IAM 권한을 위임합니다.

필요에 따라 역할을 만들어야 합니다. 예를 들어 네트워크 관리자 정책의 경우, 정책에 정의된 사용자가 "flow-logs-vpc"라는 역할을 Amazon CloudWatch 서비스로 전달하도록 허용합니다. CloudWatch는 이 역할을 이용해 사용자가 생성한 VPC의 IP 트래픽을 기록하고 캡처합니다.

보안 모범 사례를 따르기 위해 직무 기능에 관한 정책에는 전달할 수 있는 유효한 역할의 이름을 제한하는 필터가 포함되어 있습니다. 따라서 불필요한 권한을 부여할 가능성이 없습니다. 사용자가 선택적 서비스 역할을 필요로 할 경우, 정책에 정의된 명명 규칙에 따라 역할을 만들어야 합니다. 그런 다음 해당 역할에 권한을 부여합니다. 그러면 사용자는 역할이 제공하는 모든 권한을 부여해 서비스에서 이 역할을 사용하도록 구성할 수 있습니다.

최신 정보 유지

이러한 정책은 모두 AWS가 유지하며, AWS에서 정책을 추가할 때 새로운 서비스와 새로운 기능에 대한 지원을 포함시켜 모든 것을 최신 상태로 유지합니다. 이러한 정책은 고객이 수정할 수 없습니다. 정책 사본을 만든 후 이를 수정할 수 있으나 AWS가 새로운 서비스와 API 작업을 도입할 때 이 사본이 자동으로 업데이트되지는 않습니다.

직무 기능

정책 이름

다음 섹션에서 각 정책의 이름에는 AWS Management 콘솔의 정책 세부 정보 페이지로 이동하는 링크가 연결되어 있습니다. 해당 페이지에서 정책 문서를 확인하고 부여된 권한을 검토할 수 있습니다.

Administrator

AWS 관리형 정책 이름: AdministratorAccess

사용 사례: 이 사용자는 모든 액세스를 가지며 AWS 내 모든 서비스와 리소스에 권한을 위임할 수 있습니다.

정책 설명: 이 정책은 모든 AWS 서비스와 계정 내 모든 리소스에 대한 모든 작업을 허용합니다.

> Note
>
> IAM 사용자 또는 역할이 이 정책의 권한을 통해 AWS Billing and Cost Management 콘솔에 액세스할 수 있으려면, 먼저 IAM 사용자 및 역할 액세스를 활성화해야 합니다. 이를 위해 결제 콘솔에 액세스를 위임하기 위한 자습서 1단계 (p. 27)의 지침을 따르십시오.

결제

AWS 관리형 정책 이름: Billing

사용 사례: 이 사용자는 결제 정보를 확인하고 지불을 설정 및 승인해야 합니다. 사용자가 전체 AWS 서비스에 누적된 비용을 모니터링할 수 있습니다.

정책 설명: 이 정책은 결제 관리, 비용, 결제 방법, 예산, 보고서 등에 필요한 모든 권한을 부여합니다.

Note

IAM 사용자 또는 역할이 이 정책의 권한을 통해 AWS Billing and Cost Management 콘솔에 액세스할 수 있으려면, 먼저 IAM 사용자 및 역할 액세스를 활성화해야 합니다. 이를 위해 결제 콘솔에 액세스를 위임하기 위한 자습서 1단계 (p. 27)의 지침을 따르십시오.

데이터베이스 관리자

AWS 관리형 정책 이름: DatabaseAdministrator

사용 사례: 이 사용자는 AWS 클라우드에서 데이터베이스를 설정, 구성, 유지합니다.

정책 설명: 이 정책은 데이터베이스를 생성, 구성, 유지할 수 있는 권한을 부여합니다. 여기에는 Amazon DynamoDB, Amazon Relational Database Service(RDS) 및 Amazon Redshift 등 AWS 데이터베이스 서비스에 대한 액세스가 포함됩니다. 이 정책이 지원하는 데이터베이스 서비스의 전체 목록에 대한 정책을 봅니다.

이 직무 정책은 AWS 서비스로 역할을 전달할 수 있는 기능을 지원합니다. 이 정책은 다음 표에 명시된 역할에만 `iam:PassRole` 작업을 허용합니다. 자세한 정보는 이 주제의 후반부에서 역할 생성 및 정책 연결(콘솔) (p. 647) 단원을 참조하십시오.

데이터베이스 관리자 직무에 대한 선택적 IAM 서비스 역할

사용 사례	역할 이름(*는 와일드카드)	선택할 서비스 역할 유형	이 AWS 관리형 정책 선택
사용자가 RDS 데이터베이스를 모니터링하도록 허용	rds-monitoring-role	Enhanced Monitoring을 위한 Amazon RDS 역할	AmazonRDSEnhancedMonitoringRole
AWS Lambda의 데이터베이스 모니터링과 외부 데이터베이스 액세스를 허용	rdbms-lambda-access	Amazon EC2	AWSLambdaFullAccess
Lambda이 DynamoDB를 이용해 Amazon S3와 Amazon Redshift 클러스터에 파일을 업로드하도록 허용	lambda_exec_role	AWS Lambda	AWS 빅 데이터 블로그에 정의된 대로 새로운 관리형 정책 구성
Lambda 기능이 DynamoDB 테이블의 트리거 역할을 하도록 허용	lambda-dynamodb-*	AWS Lambda	AWSLambdaDynamoDBExecutionRole
Lambda 기능이 VPC에서 Amazon RDS에 액세스하도록 허용	lambda-vpc-execution-role	AWS Lambda Developer Guide에 정의된 대로 신뢰 정책으로 역할 생성	AWSLambdaVPCAccessExecutionRole
AWS Data Pipeline가 AWS 리소스에 액세스하도록 허용	DataPipelineDefaultRole	AWS Data Pipeline 개발자 안내서에 정의된 대로 신뢰 정책으로 역할 생성	AWSDataPipelineRole
Amazon EC2 인스턴스에서 실행 중인 애플리케이션이 AWS 리소스에 액세스하도록 허용	DataPipelineDefaultResourceRole	AWS Data Pipeline 개발자 안내서에 정의된 대로 신뢰 정책으로 역할 생성	AmazonEC2RoleforDataPipelineRole

데이터 과학자

AWS 관리형 정책 이름: DataScientist

사용 사례: 이 사용자는 하둡 작업과 쿼리를 실행합니다. 또한 데이터 분석 및 비즈니스 인텔리전스에 관한 정보에 액세스하고 이를 분석합니다.

정책 설명: 이 정책은 Amazon EMR 클러스터에서 쿼리를 생성, 관리, 실행하고 Amazon QuickSight 같은 도구로 데이터 분석을 수행할 수 있는 권한을 부여합니다. 정책에는 AWS Data Pipeline, Amazon EC2, Amazon Kinesis, Amazon Machine Learning 및 Amazon SageMaker 등 추가 데이터 과학자 서비스에 대한 액세스가 포함됩니다. 이 정책이 지원하는 데이터 과학자 서비스의 전체 목록에 대한 정책을 봅니다.

이 직무 정책은 AWS 서비스로 역할을 전달할 수 있는 기능을 지원합니다. 한 개의 문이 역할을 Amazon SageMaker에 전달하도록 허용합니다. 또 다른 문은 다음 표에 명시된 역할에만 `iam:PassRole` 작업을 허용합니다. 자세한 정보는 이 주제의 후반부에서 역할 생성 및 정책 연결(콘솔) (p. 647) 단원을 참조하십시오.

데이터 과학자 직무에 대한 선택적 IAM 서비스 역할

사용 사례	역할 이름(*는 와일드카드)	선택할 서비스 역할 유형	선택할 AWS 관리형 정책
클러스터에 적합한 서비스와 리소스에 대한 Amazon EC2 인스턴스 액세스를 허용	EMR-EC2_DefaultRole	EC2의 경우 Amazon EMR	AmazonElasticMapReduceforEC2Ro
클러스터의 Amazon EC2 서비스와 리소스에 액세스할 수 있는 Amazon EMR 액세스를 허용	EMR_DefaultRole	Amazon EMR	AmazonElasticMapReduceRole
Kinesis Kinesis Data Analytics가 스트리밍 데이터 소스에 액세스하도록 허용	kinesis-*	AWS 빅 데이터 블로그에 정의된 대로 신뢰 정책으로 역할을 생성합니다.	사용 사례에 따라 네 가지 가능한 옵션을 소개한 AWS 빅 데이터 블로그 참조
AWS Data Pipeline가 AWS 리소스에 액세스하도록 허용	DataPipelineDefaultRole	AWS Data Pipeline 개발자 안내서에 정의된 대로 신뢰 정책으로 역할 생성	AWSDataPipelineRole
Amazon EC2 인스턴스에서 실행 중인 애플리케이션이 AWS 리소스에 액세스하도록 허용	DataPipelineDefaultResourceRole	AWS Data Pipeline 개발자 안내서에 정의된 대로 신뢰 정책으로 역할 생성	AmazonEC2RoleforDataPipelineRol

개발자 파워 유저

AWS 관리형 정책 이름: PowerUserAccess

사용 사례: 이 사용자는 애플리케이션 개발 작업을 수행하며, AWS 인식 애플리케이션 개발을 지원하는 리소스와 서비스를 생성하고 구성할 수 있습니다.

정책 설명: 이 정책의 첫 번째 설명문은 `NotAction` (p. 595) 요소를 사용하여 모든 AWS 서비스와 모든 리소스(AWS Identity and Access Management 및 AWS Organizations 제외)에 대해 모든 작업을 허용합니다. 두 번째 설명문은 서비스에 연결된 역할을 생성할 수 잇는 IAM 권한을 부여합니다. 이것은 Amazon S3 버킷처럼 다른 서비스에서 리소스에 액세스해야 하는 서비스에 필요합니다. 또한 조직에게 마스터 계정 이메일과 조직 한도 등 사용자 조직에 대한 정보를 볼 권한을 부여합니다.

네트워크 관리자

AWS 관리형 정책 이름: NetworkAdministrator

사용 사례: 이 사용자는 AWS 네트워크 리소스를 설정하고 유지하는 작업을 담당합니다.

정책 설명: 이 정책은 Auto Scaling, Amazon EC2, AWS Direct Connect, Route 53, Amazon CloudFront, Elastic Load Balancing, AWS Elastic Beanstalk, Amazon SNS, CloudWatch, CloudWatch Logs, Amazon S3, IAM, Amazon Virtual Private Cloud에서 네트워크 리소스를 생성하고 유지할 수 있는 권한을 부여합니다.

이 직무는 AWS 서비스로 역할을 전달할 수 있는 기능을 필요로 합니다. 이 정책은 다음 표에 명시된 역할에만 `iam:GetRole` 및 `iam:PassRole`을 허용합니다. 자세한 정보는 이 주제의 후반부에서 역할 생성 및 정책 연결(콘솔) (p. 647) 단원을 참조하십시오.

네트워크 관리자 직무에 대한 선택적 IAM 서비스 역할

사용 사례	역할 이름(*는 와일드카드)	선택할 서비스 역할 유형	선택할 AWS 관리형 정책
Amazon VPC가 사용자를 대신해 CloudWatch Logs의 로그를 생성하고 관리하여 VPC로 들어오고 나가는 IP 트래픽을 모니터링하도록 허용	flow-logs-*	Amazon VPC 사용 설명서에 정의된 대로 신뢰 정책으로 역할 생성	이 사용 사례에는 기존 AWS 관리형 정책이 없지만 설명서에는 필요한 권한이 나열되어 있습니다. Amazon VPC 사용 설명서 단원을 참조하십시오.

보안 감사

AWS 관리형 정책 이름: SecurityAudit

사용 사례: 이 사용자는 보안 요구 사항을 준수하기 위해 계정을 모니터링합니다. 이 사용자는 로그와 이벤트에 액세스하여 잠재적인 보안 위반이나 악의적인 활동을 조사할 수 있습니다.

정책 설명: 이 정책은 많은 AWS 서비스에 대한 구성 데이터를 확인하고, 해당 로그를 검토할 수 있는 권한을 부여합니다.

지원 사용자

AWS 관리형 정책 이름: SupportUser

사용 사례: 이 사용자는 AWS 지원을 통해 지원 사례를 생성하고 기존 사례의 상태를 확인합니다.

정책 설명: 이 정책은 AWS 지원 사례를 생성하고 업데이트할 수 있는 권한을 부여합니다.

시스템 관리자

AWS 관리형 정책 이름: SystemAdministrator

사용 사례: 이 사용자는 개발 작업에 필요한 리소스를 설정하고 유지합니다.

정책 설명: 이 정책은 AWS CloudTrail, Amazon CloudWatch, AWS CodeCommit, AWS CodeDeploy, AWS Config, AWS Directory Service, Amazon EC2, AWS Identity and Access Management, AWS Key Management Service, AWS Lambda, Amazon RDS, Route 53, Amazon S3, Amazon SES, Amazon SQS, AWS Trusted Advisor, Amazon VPC 등 다양한 AWS 서비스에서 리소스를 생성하고 유지할 수 있는 권한을 부여합니다.

이 직무는 AWS 서비스로 역할을 전달할 수 있는 기능을 필요로 합니다. 이 정책은 다음 표에 명시된 역할에만 `iam:GetRole` 및 `iam:PassRole`을 허용합니다. 자세한 정보는 이 주제의 후반부에서 역할 생성 및 정책 연결(콘솔) (p. 647) 단원을 참조하십시오.

시스템 관리자 직무에 대한 선택적 IAM 서비스 역할

사용 사례	역할 이름(*는 와일드 카드)	선택할 서비스 역할 유형	선택할 AWS 관리형 정책
Amazon ECS 클러스터 내 EC2 인스턴스에서 실행 중인 앱이 Amazon ECS에 액세스하도록 허용	ecr-sysadmin-*	EC2 Container Service에 대한 Amazon EC2 역할	AmazonEC2ContainerServiceforEC2
사용자가 데이터베이스를 모니터링하도록 허용	rds-monitoring-role	Enhanced Monitoring을 위한 Amazon RDS 역할	AmazonRDSEnhancedMonitoringRo
EC2 인스턴스에서 실행 중인 앱이 AWS 리소스에 액세스하도록 허용합니다.	ec2-sysadmin-*	Amazon EC2	Linux 인스턴스용 Amazon EC2 사용 설명서에서와 같이 S3 버킷에 대한 액세스를 부여하는 역할의 정책 표본. 필요에 따라 사용자 지정
Lambda이 DynamoDB 스트림을 읽고 CloudWatch 로그에 기록하도록 허용	lambda-sysadmin-*	AWS Lambda	AWSLambdaDynamoDBExecutionR

보기 전용 사용자

AWS 관리형 정책 이름: ViewOnlyAccess

사용 사례: 이 사용자는 모든 서비스에 걸쳐 계정 내 AWS 리소스와 기본 메타데이터 목록을 확인할 수 있습니다. 하지만 할당량을 초과하는 리소스 콘텐츠나 메타데이터, 리소스의 목록 정보를 읽을 수 없습니다.

정책 설명: 이 정책은 대부분의 AWS 서비스 리소스에 대한 `List*`, `Describe*`, `Get*`, `View*`, `Lookup*` 액세스를 부여합니다. 각 서비스에 대해 이 정책에 포함된 작업을 보려면 ViewOnlyAccess 단원을 참조하십시오.

역할 생성 및 정책 연결(콘솔)

앞서 나열한 여러 가지 정책은 AWS 서비스에서 사용자 대신 작업을 수행할 수 있도록 해주는 역할을 이용해 해당 서비스를 구성할 수 있는 권한을 부여합니다. 직무 정책은 반드시 사용해야 하는 정확한 역할 이름을 정의하거나, 사용할 수 있는 이름의 앞부분을 지정하는 접두사만이라도 포함합니다. 이러한 역할 중 하나를 생성하려면 다음 절차의 단계를 따릅니다.

AWS 제품에 대한 역할을 생성하려면(IAM 콘솔)

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. AWS 서비스 역할 유형을 선택한 후 이 역할을 수행하도록 허용하려는 서비스를 선택합니다.
4. 서비스의 사용 사례를 선택합니다. 지정한 서비스에 사용 사례가 하나뿐이면 자동으로 선택됩니다. 사용 사례는 서비스에 필요한 신뢰 정책을 포함하기 위해 서비스에서 정합니다. 그런 다음 [Next: Permissions]를 선택합니다.
5. 가능하면 권한 정책에 사용할 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 정책 생성 절차의 4단계를 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아갑니다. 서비스에게 부여하려는 권한 정책 옆의 확인란을 선택합니다.

선택한 사용 사례에 따라 서비스에서 다음을 수행할 수 있습니다.

- 서비스에서 역할에 대한 권한을 정의하기 때문에 할 일이 아무것도 없습니다.
- 제한된 권한 집합에서 선택할 수 있습니다.
- 모든 권한 집합에서 선택할 수 있도록 허용
- 여기서 정책을 선택하지 않고, 나중에 정책을 만들어 역할에 연결할 수 있도록 허용

6. (선택 사항) 권한 경계를 설정합니다. 이는 서비스 역할에서 사용할 수 있는 고급 기능이며 서비스 연결 역할은 아닙니다.

   Set permissions boundary(권한 경계 설정) 섹션을 확장하고 Use a permissions boundary to control the maximum role permissions(권한 경계를 사용하여 최대 역할 권한 제어)를 선택합니다. IAM에는 계정의 AWS 관리형 정책 및 고객 관리형 정책 목록이 있습니다. 권한 경계에 사용할 정책을 선택하거나 정책 생성을 선택하여 새 브라우저 탭을 열고 완전히 새로운 정책을 생성합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 정책 생성 절차의 4단계를 참조하십시오. 정책을 생성하면 탭을 닫고 원래 탭으로 돌아와 권한 경계에 사용할 정책을 선택합니다.
7. Next: Tags(다음: 태그)를 선택합니다.
8. (선택 사항) 태그를 키-값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서 태그 사용에 대한 자세한 내용은 IAM 사용 설명서의 IAM 개체 태그 지정을 참조하십시오.
9. Next: Review(다음: 검토)를 선택합니다.
10. 역할 이름의 경우 역할 이름 사용자 지정 수준은 서비스에서 정합니다. 서비스에서 역할 이름을 정의하는 경우 이 옵션을 편집할 수 없습니다. 다른 경우에는 서비스에서 역할 이름의 접두사를 정의하고 사용자가 선택적 접미사를 입력할 수 있습니다. 일부 서비스에서는 사용자가 역할의 전체 이름을 지정할 수 있습니다.

    가능한 경우 이 역할의 목적을 식별하는 데 도움이 되는 역할 이름이나 역할 이름 접미사를 입력합니다. 역할 이름은 AWS 계정 내에서 고유해야 합니다. 대소문자는 구별하지 않습니다. 예를 들어 이름이 **`PRODROLE`**과 **`prodrole`** 모두로 지정된 역할은 만들 수 없습니다. 다양한 엔티티에서 해당 역할을 참조할 수 있으므로 역할이 생성된 후에는 해당 역할의 이름을 편집할 수 없습니다.
11. (선택 사항) Role description(역할 설명)에 새 역할에 대한 설명을 입력합니다.
12. 역할을 검토한 다음 역할 생성을 선택합니다.

예제 1: 사용자를 데이터베이스 관리자로 구성(콘솔)

이 예제는 IAM 사용자 Alice를 데이터베이스 관리자 (p. 644)로 구성하는 데 필요한 단계를 보여줍니다. 이 섹션에서 테이블 첫 번째 행의 정보를 사용하여 사용자가 Amazon RDS 모니터링을 지원하도록 허용합니다. Alice가 Amazon 데이터베이스 서비스를 관리할 수 있도록 DatabaseAdministrator 정책을 Alice의 IAM 사용자에게 연결합니다. 이 정책을 통해 Alice는 `rds-monitoring-role`라는 역할을 Amazon RDS 서비스로 전달할 수도 있습니다. 그러면 Alice를 대신해 RDS 데이터베이스를 모니터링합니다.

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 정책을 선택한 후 검색 상자에 **`database`**를 입력합니다.
3. DatabaseAdministrator 정책 확인란과 Policy actions(정책 작업), 연결을 차례로 선택합니다.
4. 사용자 목록에서 Alice를 선택한 후 정책 연결을 선택합니다. 이제 Alice가 AWS 데이터베이스를 관리할 수 있습니다. 하지만 Alice가 이 데이터베이스를 모니터링하도록 허용하려면 서비스 역할을 구성해야 합니다.
5. IAM 콘솔의 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
6. AWS 서비스 역할 유형을 선택한 후 Amazon RDS를 선택합니다.
7. Amazon RDS Role for Enhanced Monitoring(확장 모니터링을 위한 RDS 역할) 사용 사례를 선택합니다.
8. Amazon RDS는 역할에 대한 권한을 정의합니다. 계속하려면 Next: Review(다음: 검토)를 선택합니다.

9. 역할 이름은 현재 Alice가 적용하는 DatabaseAdministrator 정책에 지정된 것 중 하나여야 합니다. 그중 하나는 **rds-monitoring-role**입니다. 이 이름을 역할 이름에 입력합니다.
10. (선택 사항) [Role description]에 새 역할에 대한 설명을 입력합니다.
11. 세부 정보를 검토한 후 역할 생성을 선택합니다.
12. 이제 Alice는 Amazon RDS 콘솔의 모니터링 섹션에서 RDS Enhanced Monitoring(RDS 확장 모니터링)을 활성화할 수 있습니다. 예를 들어, DB 인스턴스 또는 읽기 전용 복제본을 생성하거나 DB 인스턴스를 수정할 때 이렇게 합니다. Alice는 확장 모니터링 활성화를 예로 설정하면서 역할 모니터링 텍스트 상자에 본인이 생성한 역할 이름(rds-monitoring-role)을 입력해야 합니다.

예제 2: 사용자를 네트워크 관리자로 구성(콘솔)

이 예제는 IAM 사용자 Juan을 네트워크 관리자 (p. 645)로 구성하는 데 필요한 단계를 보여줍니다. 해당 섹션에서 테이블의 정보를 사용하여 Juan이 VPC로 들어오고 나가는 IP 트래픽을 모니터링하도록 허용합니다. 또한 Juan이 CloudWatch Logs의 로그에서 해당 정보를 캡처하도록 허용합니다. Juan이 AWS 네트워크 리소스를 구성할 수 있도록 Juan의 IAM 사용자에게 NetworkAdministrator 정책을 연결합니다. 또한 이 정책 덕분에 흐름 로그를 작성할 때 Juan이 `flow-logs*`로 시작하는 역할을 Amazon EC2로 전달하도록 설정할 수 있습니다. 예제 1과 달리 이 시나리오에서는 사전 정의된 서비스 역할 유형이 없기 때문에 몇 가지 단계를 다르게 수행해야 합니다.

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택한 후 검색 상자에 **network**를 입력합니다.
3. NetworkAdministrator 정책 옆의 확인란에 이어 Policy actions(정책 작업), 연결을 차례로 선택합니다.
4. 사용자 목록에서 Juan 옆에 있는 확인란을 선택한 후 정책 연결을 선택합니다. 이제 Juan이 AWS 네트워크 리소스를 관리할 수 있습니다. 하지만 VPC 내 트래픽을 모니터링하도록 하려면 서비스 역할을 구성해야 합니다.
5. 생성해야 하는 서비스 역할에 사전 정의된 관리형 정책이 없기 때문에 먼저 이 정책부터 생성해야 합니다. 탐색 창에서 정책을 선택한 다음 정책 생성을 선택합니다.
6. JSON 탭을 선택하고 다음 JSON 정책 문서에서 텍스트를 복사합니다. 이 텍스트를 JSON 텍스트 상자에 붙여 넣습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

7. 작업이 완료되면 [Review policy]를 선택합니다. 정책 검사기 (p. 441)가 모든 구문 오류를 보고합니다.

   Note

   언제든지 Visual editor(시각적 편집기) 및 JSON 탭을 전환할 수 있습니다. 그러나 변경을 수행하거나 Visual editor(시각적 편집기) 탭에서 정책 검토를 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 정책 재구성 (p. 538) 단원을 참조하십시오.

8. 검토 페이지에서 정책 이름에 **vpc-flow-logs-policy-for-service-role**을 입력합니다. 정책 요약을 검토하여 정책이 부여한 권한을 확인한 다음 정책 생성을 선택하여 작업을 저장합니다.

   새로운 정책이 관리형 정책 목록에 나타나며 연결 준비가 완료됩니다.
9. IAM 콘솔의 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
10. AWS 서비스 역할 유형을 선택한 후 Amazon EC2를 선택합니다.
11. Amazon EC2 사용 사례를 선택합니다.
12. 권한 정책 연결(Attach permissions policies) 페이지에서 앞서 생성한 정책을 선택하고 vpc-flow-logs-policy-for-service-role과 Next: Review(다음: 검토)를 차례로 선택합니다.
13. 역할 이름은 현재 Juan이 적용하는 NetworkAdministrator 정책에서 허용한 것이어야 합니다. `flow-logs-`로 시작하는 이름은 무엇이든 허용됩니다. 이 예에서는 역할 이름에 **flow-logs-for-juan**을 입력합니다.
14. (선택 사항) [Role description]에 새 역할에 대한 설명을 입력합니다.
15. 세부 정보를 검토한 후 역할 생성을 선택합니다.
16. 이제 이 시나리오에 필요한 신뢰 정책을 구성할 수 있습니다. 역할 페이지에서 flow-logs-for-juan 역할(확인란이 아닌 이름)을 선택합니다. 새 역할의 세부 정보 페이지에서 신뢰 관계 탭을 선택한 다음 Edit trust relationship(신뢰 관계 편집)을 선택합니다.
17. "Service" 라인을 다음과 같이 변경해 `ec2.amazonaws.com`의 항목을 교체합니다.

```
        "Service": "vpc-flow-logs.amazonaws.com"
```

18. 이제 Juan이 Amazon EC2 콘솔에서 VPC나 서브넷의 흐름 로그를 생성할 수 있습니다. 흐름 로그를 생성할 때 flow-logs-for-juan 역할을 지정합니다. 이 역할에는 로그를 생성하고 데이터를 쓸 수 있는 권한이 있습니다.

AWS 전역 조건 컨텍스트 키

보안 주체 (p. 5)가 AWS에 요청 (p. 5)하면 AWS는 요청 정보를 요청 컨텍스트 (p. 5)로 수집합니다. JSON 정책의 `Condition` 요소를 사용하여 요청 컨텍스트의 키를 정책에서 지정한 키 값과 비교할 수 있습니다. 요청 컨텍스트에 전역 키가 포함되는 상황에 대한 자세한 내용은 각 전역 조건 키의 가용성 정보를 참조하십시오. JSON 정책의 `Condition` 요소 사용에 대한 자세한 방법은 IAM JSON 정책 요소: Condition (p. 598) 단원을 참조하십시오.

> **Note**
>
> 일부 상황에서만 사용할 수 있는 조건 키를 사용하는 경우 조건 연산자의 IfExists (p. 607) 버전을 사용할 수 있습니다. 요청 컨텍스트에 조건 키가 누락된 경우 정책이 평가에 실패할 수 있습니다. 예를 들어, 특정 IP 범위 또는 특정 VPC로부터 요청이 오는 경우 `...IfExists` 연산자와 함께 다음 조건 블록을 사용하여 일치시킵니다. 요청 컨텍스트에 두 키 중 하나 또는 둘 다 포함되어 있지 않은 경우에도 조건은 여전히 `true`를 반환합니다. 값은 지정된 키가 요청 컨텍스트에 포함된 경우에만 검사됩니다.

```
"Condition": {
    "IpAddressIfExists": {"aws:SourceIp" : ["xxx"] },
    "StringEqualsIfExists" : {"aws:SourceVpc" : ["yyy"]}
}
```

전역 조건 키는 `aws:` 접두사가 있는 조건 키입니다. AWS 서비스는 전역 조건 키를 지원하거나 서비스 접두사를 포함하는 서비스별 키를 제공할 수 있습니다. 예를 들어, IAM 조건 키에는 `iam:` 접두사가 포함됩니다. 자세한 내용은 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하고 키를 보려는 서비스를 선택하십시오.

aws:CalledVia

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 정책의 서비스를 IAM 보안 주체(사용자 또는 역할)를 대신하여 요청한 서비스와 비교합니다. 보안 주체가 AWS 서비스에 요청을 하면 해당 서비스는 보안 주체의 자격 증명을 사용하여 다른 서비스에 대한 후속 요청을 수행할 수 있습니다. `aws:CalledVia` 키에는 보안 주체를 대신하여 요청을 수행한 체인의 각 서비스 목록이 정렬되어 있습니다.

예를 들어 AWS CloudFormation를 사용하여 Amazon DynamoDB 테이블에서 읽기 및 쓰기를 수행할 수 있습니다. 이제 DynamoDB에서 AWS Key Management Service(AWS KMS)에서 제공하는 암호화를 사용합니다.

- 가용성 – 이 키는 `aws:CalledVia`을 지원하는 서비스가 IAM 보안 주체의 자격 증명을 사용하여 다른 서비스에 요청을 수행할 때 요청에 표시됩니다. 서비스가 서비스 역할 또는 서비스 연결 역할을 사용해 보안 주체를 대신하여 호출을 하는 경우에는 이 키가 나타나지 않습니다. 이 키는 보안 주체가 직접 호출을 할 때도 존재하지 않습니다.

정책에서 `aws:CalledVia` 조건 키를 사용하려면 AWS 서비스 요청을 허용 또는 거부할 서비스 보안 주체를 제공해야 합니다. AWS에서는 `aws:CalledVia`와 함께 다음 서비스를 사용할 수 있도록 지원합니다.

CalledVia 서비스

AWS 서비스	서비스 보안 주체
Amazon Athena	athena.amazonaws.com
AWS CloudFormation	cloudformation.amazonaws.com
Amazon DynamoDB	dynamodb.amazonaws.com
AWS Key Management Service (AWS KMS)	kms.amazonaws.com

어떤 서비스든 보안 주체의 자격 증명을 사용하여 요청을 할 때 액세스를 허용 또는 거부하려면 `aws:ViaAWSService` (p. 663) 조건 키를 사용합니다. 이 조건 키는 모든 AWS 서비스를 지원합니다.

`aws:CalledVia` 키는 다중값 키 (p. 608)입니다. 그러나 조건에서 이 키를 사용하여 주문을 수행할 수는 없습니다. 위의 예제를 사용하여 사용자 1이 DynamoDB를 호출하도록 AWS CloudFormation에 요청하면 AWS KMS이 호출됩니다. 이들은 세 가지의 별도 요청입니다. AWS KMS에 대한 마지막 호출은 사용자 1에 의해 AWS CloudFormation 및 DynamoDB를 통해 수행됩니다.

이 경우 요청 컨텍스트의 `aws:CalledVia` 키에는 `cloudformation.amazonaws.com`와 `dynamodb.amazonaws.com`이 순서대로 포함되어 있습니다. 요청 체인의 어딘가에서 DynamoDB를 통해 통화가 이루어졌다는 것만 유념한다면 정책에서 이 조건 키를 사용할 수 있습니다.

예를 들어 다음 정책에서는 `my-example-key`이라는 AWS KMS 키를 관리할 수 있도록 허용하지만, DynamoDB가 요청 서비스 중 하나인 경우에만 한합니다. `ForAnyValue:StringEquals` (p. 610) 조건 연산자는 DynamoDB가 호출 서비스 중 하나인지 확인합니다. 보안 주체가 AWS KMS에 직접 호출을 하는 경우에는 조건이 `false`을 반환하고 이 요청이 이 정책에서 허용되지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "KmsActionsIfCalledViaDynamodb",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey",
                "kms:DescribeKey"
```

```
            ],
            "Resource": "arn:aws:kms:region:111122223333:key/my-example-key",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": ["dynamodb.amazonaws.com"]
                }
            }
        }
    ]
}
```

체인에서 첫 번째 또는 마지막 호출을 하는 서비스를 적용하려는 경우에는 aws:CalledViaFirst (p. 652) 및 aws:CalledViaLast (p. 652) 키를 사용할 수 있습니다. 예를 들어 다음 정책은 AWS KMS에서 my-example-key이라는 키를 관리할 수 있도록 허용합니다. 이러한 AWS KMS 작업은 체인에 여러 요청이 포함된 경우에만 허용됩니다. 첫 번째 요청은 AWS CloudFormation을 통해, 그리고 마지막으로 DynamoDB을 통해 수행되어야 합니다. 다른 서비스가 체인 중간에 요청을 해도 작업은 계속 허용됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "KmsActionsIfCalledViaChain",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:region:111122223333:key/my-example-key",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "cloudformation.amazonaws.com",
                    "aws:CalledViaLast": "dynamodb.amazonaws.com"
                }
            }
        }
    ]
}
```

aws:CalledViaFirst (p. 652) 및 aws:CalledViaLast (p. 652) 키는 서비스가 IAM 보안 주체의 자격 증명을 사용하여 다른 서비스를 호출할 때 요청에 표시됩니다. 이들 키는 요청 체인에서 호출을 한 첫 번째 서비스와 마지막 서비스를 나타냅니다. 예를 들어 AWS CloudFormation이 X Service라는 다른 서비스를 호출하고, 이 서비스는 다시 DynamoDB를 호출한 다음 AWS KMS를 호출한다고 가정해 보겠습니다. AWS KMS에 대한 마지막 호출은 AWS CloudFormation, X Service 및 DynamoDB을 통해 User 1에서 수행됩니다. 처음 호출은 AWS CloudFormation를 통해, 마지막 호출은 DynamoDB를 통해 이루어졌습니다.

aws:CalledViaFirst

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 정책의 서비스를 IAM 보안 주체(사용자 또는 역할)를 대신하여 요청을 수행한 첫 번째 서비스와 비교합니다. 자세한 내용은 aws:CalledVia (p. 650) 단원을 참조하십시오.

- 가용성 – 이 키는 서비스가 IAM 보안 주체의 자격 증명을 사용하여 다른 서비스에 최소 1개의 요청을 수행할 때 요청에 표시됩니다. 서비스가 서비스 역할 또는 서비스 연결 역할을 사용해 보안 주체를 대신하여 호출을 하는 경우에는 이 키가 나타나지 않습니다. 이 키는 보안 주체가 직접 호출을 할 때도 존재하지 않습니다.

aws:CalledViaLast

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 정책의 서비스를 IAM 보안 주체(사용자 또는 역할)를 대신하여 요청을 수행한 마지막 서비스와 비교합니다. 자세한 내용은 `aws:CalledVia (p. 650)` 단원을 참조하십시오.

- 가용성 – 이 키는 서비스가 IAM 보안 주체의 자격 증명을 사용하여 다른 서비스에 최소 1개의 요청을 수행할 때 요청에 표시됩니다. 서비스가 서비스 역할 또는 서비스 연결 역할을 사용해 보안 주체를 대신하여 호출을 하는 경우에는 이 키가 나타나지 않습니다. 이 키는 보안 주체가 직접 호출을 할 때도 존재하지 않습니다.

aws:CurrentTime

날짜 연산자 (p. 604)를 사용합니다.

이 키를 사용하여 요청의 날짜 및 시간을 정책에서 지정한 날짜 및 시간과 비교합니다.

- 가용성 – 이 키는 항상 요청 컨텍스트에 포함됩니다.

aws:EpochTime

날짜 연산자 (p. 604) 또는 숫자 연산자 (p. 603)와 함께 사용됩니다.

이 키를 사용하여 epoch 또는 Unix 시간의 요청 날짜 및 시간을 정책에서 지정한 값과 비교합니다. 또한 이 키는 1970년 1월 1일 이후의 초 수를 허용합니다.

- 가용성 – 이 키는 항상 요청 컨텍스트에 포함됩니다.

aws:MultiFactorAuthAge

숫자 연산자 (p. 603)를 사용합니다.

이 키를 사용하여 요청한 보안 주체가 MFA를 사용하여 승인된 이후의 시간(초)과 정책에서 지정한 시간을 비교합니다. MFA에 대한 자세한 내용은 AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) 단원을 참조하십시오.

- 가용성 – 이 키는 보안 주체가 MFA를 사용하여 인증된 경우에만 요청 컨텍스트에 포함됩니다. MFA를 사용하지 않으면 이 키는 표시되지 않습니다.

aws:MultiFactorAuthPresent

부울 연산자 (p. 604)를 사용합니다.

이 키를 사용하여 MFA(Multi-Factor Authentication)를 통해 요청을 한 임시 보안 자격 증명의 유효성을 검사했는지 여부를 확인합니다.

- 가용성 – 이 키는 보안 주체가 임시 자격 증명을 사용하여 요청한 경우에만 요청 컨텍스트에 포함됩니다. 장기 자격 증명을 사용하는 AWS CLI, AWS API 또는 AWS SDK 요청에는 이 키가 존재하지 않습니다.

임시 자격 증명은 IAM 역할, 연동 사용자, `sts:GetSessionToken`의 임시 토큰이 있는 IAM 사용자 및 AWS Management 콘솔의 사용자를 인증하는 데 사용됩니다. AWS Management 콘솔의 IAM 사용자는 무의식적으로 임시 자격 증명을 사용합니다. 사용자는 장기 자격 증명인 사용자 이름과 암호를 사용하여 콘솔에 로그인합니다. 하지만 백그라운드에서는 콘솔이 사용자를 대신하여 임시 자격 증명을 생성합니다. 임시 자격

증명의 사용을 지원하는 서비스에 대해 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

`aws:MultiFactorAuthPresent` 키는 사용자 액세스 키 페어와 같은 장기 자격 증명으로 API 또는 CLI 명령을 호출하는 경우 존재하지 않습니다. 따라서 이 키를 확인할 때 조건 연산자의 `...IfExists` (p. 607) 버전을 사용하는 것이 좋습니다.

다음 `Condition` 요소는 MFA를 사용하여 요청을 인증했는지를 확인할 수 있는 신뢰성 있는 방법이 아니라는 점을 이해해야 합니다.

```
#####   WARNING: NOT RECOMMENDED   #####
"Effect" : "Deny",
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : "false" } }
```

`Deny` 효과, `Bool` 요소 및 `false` 값을 이렇게 조합할 경우, MFA를 사용하여 인증 가능하나 인증받지 않은 요청을 거부합니다. 이러한 조합은 MFA의 사용을 지원하는 임시 자격 증명에만 지원됩니다. 이 문은 장기 자격 증명을 사용하는 요청 또는 MFA를 사용하여 인증되는 요청에 대한 액세스를 거부하지 않습니다. 이 예의 로직이 복잡하며 MFA 인증이 실제로 사용되었는지 테스트되지 않으므로 이 예를 사용할 때는 주의해야 합니다.

또한 `Deny` 효과, `Null` 요소 및 `true`의 조합은 동일한 방식으로 작동하며 그 로직이 훨씬 더 복잡하기 때문에 이 조합을 사용하지 말아야 합니다.

권장되는 조합

`BoolIfExists` (p. 607) 연산자를 사용하여, 요청이 MFA를 사용하여 인증되는지 여부를 확인하는 것이 좋습니다.

```
"Effect" : "Deny",
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : "false" } }
```

`Deny`, `BoolIfExists` 및 `false`를 조합할 경우, MFA를 사용해 인증되지 않은 요청을 거부합니다. 특히 MFA를 포함하지 않는 임시 자격 증명의 요청을 거부합니다. 또한 액세스 키를 사용하는 AWS CLI 또는 AWS API 작업과 같은 장기 자격 증명을 사용하는 요청을 거부합니다. `*IfExists` 연산자는 `aws:MultiFactorAuthPresent` 키의 존재성 및 존재 가능성 여부를 해당 키의 존재 여부로 표시된 대로 확인합니다. MFA를 사용해 인증되지 않은 요청을 거부하려면 이 연산자를 사용하십시오. 이 방법이 더욱 안전하기는 하지만 액세스 키를 사용해 AWS CLI 또는 AWS API에 액세스하는 코드나 스크립트를 손상시킬 수 있습니다.

대체 조합

또한 `BoolIfExists` (p. 607) 연산자를 사용하여 MFA로 인증된 요청 및 장기 자격 증명을 사용하는 AWS CLI 또는 AWS API 요청을 허용할 수 있습니다.

```
"Effect" : "Allow",
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : "true" } }
```

이 조건은 키가 존재하든 존재하지 않든 마찬가지로 일치합니다. `Allow`, `BoolIfExists` 및 `true`를 조합할 경우, MFA를 사용해 인증된 요청 또는 MFA를 사용해 인증받지 않은 요청을 허용합니다. 이 말은 요청자가 장기 액세스 키를 사용할 경우 AWS CLI, AWS API 및 AWS SDK 작업이 허용된다는 것을 의미합니다. 이러한 조합은 MFA를 포함할 수도 있지만 실제로 포함하지 않는 임시 자격 증명의 요청을 허용하지 않습니다.

IAM 콘솔 비주얼 편집기를 사용해 정책을 생성한 후 MFA required(MFA 필수)를 선택하면 이 조합이 적용됩니다. 이러한 설정에서는 콘솔 액세스를 위해 MFA가 필요하지만 MFA 없이 프로그래밍 방식으로 액세스하는 방법도 있습니다.

또는 MFA를 사용해 인증되는 경우에 한해서 `Bool` 연산자를 사용해 프로그래밍 방식 요청과 콘솔 요청을 허용할 수도 있습니다.

```
"Effect" : "Allow",
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : "true" } }
```

`Allow`, `Bool` 및 `true`를 조합할 경우, MFA를 사용해 인증된 요청만을 허용합니다. 이러한 조합은 MFA의 사용을 지원하는 임시 자격 증명에만 지원됩니다. 이 문은 장기 액세스 키를 사용하는 요청 또는 MFA 없이 임시 자격 증명을 사용하는 요청에 대한 액세스를 허용하지 않습니다.

MFA 키가 있는지 여부를 확인하는 데 다음과 유사한 정책 구문을 사용하지 마십시오.

```
#####   WARNING: USE WITH CAUTION   #####

"Effect" : "Allow",
"Condition" : { "Null" : { "aws:MultiFactorAuthPresent" : "false" } }
```

`Allow` 효과, `Null` 요소 및 `false` 값을 조합할 경우, 그 요청의 실제 인증 여부와 상관없이, MFA를 사용해 인증받을 수 있는 요청만을 허용합니다. 이렇게 하여 임시 자격 증명을 사용하는 모든 요청을 허용하고 장기 자격 증명에 대한 액세스를 거부합니다. 이 예에서는 MFA 인증이 실제로 사용되었는지 여부를 테스트하지 않으므로 이 예를 사용할 때는 주의해야 합니다.

aws:PrincipalAccount

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청한 보안 주체가 속한 계정과 정책에서 지정한 계정 식별자를 비교합니다.

- 가용성 – 이 키는 항상 요청 컨텍스트에 포함됩니다.

aws:PrincipalArn

ARN 연산자 (p. 606)를 사용합니다.

이 키를 사용하여 요청한 보안 주체의 Amazon 리소스 이름 (p. 564)(ARN)을 정책에서 지정한 ARN과 비교합니다. IAM 역할의 경우 요청 컨텍스트는 역할을 맡은 사용자의 ARN이 아니라 역할의 ARN을 반환합니다. 이 조건 키에 지정할 수 있는 보안 주체의 유형을 알아보려면 보안 주체 지정 (p. 589) 단원을 참조하십시오.

- 가용성 – 이 키는 항상 요청 컨텍스트에 포함됩니다.

aws:PrincipalOrgID

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청한 보안 주체가 속한 AWS Organizations의 조직 식별자와 정책에 지정된 식별자를 비교합니다.

- 가용성 – 이 키는 보안 주체가 조직의 멤버인 경우에만 요청 컨텍스트에 포함됩니다.

이 전역 키는 조직 내 모든 AWS 계정의 계정 ID를 전부 나열하는 대안을 제공합니다. 이 조건 키를 사용하여 리소스 기반 정책 (p. 372)에서 `Principal` 요소를 간단하게 지정할 수 있습니다. 조건 요소에서 조직 ID를 지정할 수 있습니다. 계정을 추가 및 제거할 때 `aws:PrincipalOrgID` 키가 포함된 정책에는 자동으로 올바른 계정이 포함되므로 수동 업데이트가 필요하지 않습니다.

예를 들어, 다음 Amazon S3 버킷 정책을 통해 `o-xxxxxxxxxxx` 조직 내 모든 계정의 멤버는 `policy-ninja-dev` 버킷에 객체를 추가할 수 있습니다.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowPutObject",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::policy-ninja-dev/*",
    "Condition": {"StringEquals":
      {"aws:PrincipalOrgID":["o-xxxxxxxxxxx"]}
    }
  }
}
```

Note

이 전역 조건은 AWS 조직의 마스터 계정에 적용됩니다.

AWS Organizations에 대한 자세한 내용은 AWS Organizations 사용 설명서의 AWS Organizations(이)란 무엇인가? 단원을 참조하십시오.

aws:PrincipalOrgPaths

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청 중인 보안 주체의 AWS Organizations 경로를 정책의 경로와 비교합니다. 이 보안 주체는 IAM 사용자, IAM 역할, 연동 사용자 또는 AWS 계정 루트 사용자일 수 있습니다. 정책에서 이 조건 키는 요청자가 AWS Organizations의 지정된 조직 루트 또는 조직 단위(OU) 내의 계정 멤버인지 확인합니다. AWS Organizations 경로는 조직 엔터티 구조의 텍스트 표현입니다. 경로 사용 및 이해에 대한 자세한 내용은 AWS Organizations 엔터티 경로 이해 (p. 475) 단원을 참조하십시오.

- 가용성 – 이 키는 보안 주체가 조직의 멤버인 경우에만 요청 컨텍스트에 포함됩니다.

Note

조직 ID는 전역적으로 고유하지만 OU ID와 루트 ID는 조직 내에서만 고유합니다. 즉, 두 조직이 동일한 조직 ID를 공유하지 않습니다. 그러나 다른 조직에는 사용자 ID와 동일한 OU 또는 루트가 있을 수 있습니다. OU 또는 루트를 지정할 때는 항상 조직 ID를 포함하는 것이 좋습니다.

예를 들어, 다음 조건은 `ou-jkl0-awsddddd` OU에 직접 연결되지만 하위 OU에는 연결되지 않은 계정의 보안 주체에 대해 `true`를 반환합니다.

```
"Condition" : { "ForAnyValue:StringEquals" : {
     "aws:PrincipalOrgPaths":["o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-
awsddddd/"]
}}
```

다음 조건은 OU 또는 해당 하위 OU에 직접 연결된 계정의 보안 주체에 대해 `true`를 반환합니다. 와일드카드를 포함할 때는 `StringLike` 조건 연산자를 사용해야 합니다.

```
"Condition" : { "ForAnyValue:StringLike" : {
     "aws:PrincipalOrgPaths":["o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-
awsddddd*"]
}}
```

다음 조건은 OU 또는 해당 하위 OU에 직접 연결된 계정의 보안 주체에 대해 `true`를 반환합니다.

```
"Condition" : { "ForAnyValue:StringLike" : {
     "aws:PrincipalOrgPaths":["o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-ghi0-awsccccc/ou-jkl0-
awsddddd/*"]
```

```
}}
```

다음 조건에서는 상위 OU에 관계없이 `o-a1b2c3d4e5` 조직의 모든 보안 주체에 대한 액세스를 허용합니다.

```
"Condition" : { "ForAnyValue:StringLike" : {
     "aws:PrincipalOrgPaths":["o-a1b2c3d4e5/*"]
}}
```

`aws:PrincipalOrgPaths`는 다중 값 조건 키입니다. 다중 값 키에는 하나 이상의 값이 목록 형식으로 포함됩니다. 결과는 논리적 `OR`입니다. `ForAnyValue` 조건 연산자에서 여러 값을 사용하는 경우 보안 주체의 경로는 정책에 나열된 경로 중 하나와 일치해야 합니다. 단일 키에 대해 여러 값을 포함하는 정책의 경우 조건을 배열 ("Key":["Value1", "Value2"])처럼 대괄호로 묶어야 합니다. 단일 값이 있는 경우에도 이 대괄호를 포함해야 합니다. 다중 값 조건 키에 대한 자세한 내용은 다수의 키 또는 값을 사용하는 조건 생성 (p. 608) 단원을 참조하십시오.

```
    "Condition": {
        "ForAnyValue:StringLike": {
            "aws:PrincipalOrgPaths": [
                "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/*",
                "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/*"
            ]
        }
    }
```

aws:PrincipalTag

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청한 보안 주체에 연결된 태그를 정책에서 지정한 태그와 비교합니다. 보안 주체에 둘 이상의 태그가 연결되어 있는 경우 요청 컨텍스트에는 연결된 각 태그 키에 대해 `aws:PrincipalTag` 키가 하나씩 포함됩니다.

- 가용성 – 이 키는 보안 주체가 태그가 연결된 IAM 사용자를 사용하는 경우 요청 컨텍스트에 포함됩니다. 연결된 태그 또는 세션 태그 (p. 294)가 있는 IAM 역할을 사용하는 보안 주체에 포함됩니다.

사용자 또는 역할에 사용자 지정 속성을 키-값 페어의 형태로 추가할 수 있습니다. IAM 태그에 대한 자세한 내용은 IAM 사용자 및 역할 태그 지정 (p. 290) 단원을 참조하십시오. `aws:PrincipalTag`를 사용하여 AWS 보안 주체에 대한 액세스를 제어 (p. 382)할 수 있습니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.를 사용하면 **`tagManager=true`** 태그가 지정된 사용자가 IAM 사용자, 그룹 또는 역할을 관리할 수 있습니다.이 정책을 사용하려면 정책 예제의 *`#### ## ### ###`*를 본인의 정보로 대체하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*",
      "Condition": {"StringEquals": {"aws:PrincipalTag/tagManager": "true"}}
    }
  ]
}
```

aws:PrincipalType

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청을 하는 보안 주체의 유형을 정책에서 지정한 보안 주체 유형과 비교합니다. 다른 보안 주체에 대한 요청 컨텍스트에서 정보가 표시되는 방법에 대한 자세한 내용은 보안 주체 지정 (p. 589) 단원을 참조하십시오.

- 가용성 – 이 키는 항상 요청 컨텍스트에 포함됩니다.

aws:Referer

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 클라이언트 브라우저에서 요청을 참조한 사람과 정책에서 지정한 참조자를 비교합니다. `aws:referer` 요청 컨텍스트 값은 HTTP 헤더의 호출자에 의해 제공됩니다.

- 가용성 – 이 키는 브라우저에서 URL을 사용하여 요청이 호출된 경우에만 요청 컨텍스트에 포함됩니다.

예를 들어, 웹 브라우저를 사용하여 Amazon S3 API 작업을 직접 호출할 수 있습니다. 즉, 웹 브라우저를 통해 직접 이미지 및 문서와 같은 S3 객체를 볼 수 있습니다. 이 `aws:referer` 조건을 사용하면 참조자 헤더의 값을 기준으로 HTTP 또는 HTTPS 요청의 특정 값에 대한 액세스를 제한할 수 있습니다.

> Warning
>
> 이 키를 사용할 때는 주의해야 합니다. 공개적으로 알려진 참조자 헤더 값을 포함하는 것은 위험합니다. 권한이 없는 사용자가 수정된 브라우저나 사용자 지정 브라우저를 사용하여 원하는 `aws:referer` 값을 제공할 수 있습니다. 따라서 무단 사용자의 직접 AWS 요청을 차단할 목적으로 `aws:referer`를 사용해서는 안 됩니다. 이러한 값은 고객이 Amazon S3에 저장된 콘텐츠 등의 디지털 콘텐츠를 권한이 없는 타사 사이트에서 참조하지 못하도록 보호하기 위해서만 사용하십시오.

aws:RequestedRegion

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청에서 호출된 AWS 리전을 정책에서 지정한 리전과 비교합니다. 이 전역 조건 키를 사용하여 요청할 수 있는 리전을 제어할 수 있습니다. 각 서비스에 대한 AWS 리전을 보려면 Amazon Web Services 일반 참조의 AWS 리전 및 엔드포인트 단원을 참조하십시오.

- 가용성 – 이 키는 항상 요청 컨텍스트에 포함됩니다.

IAM 등과 같은 일부 전역 서비스에는 단일 엔드포인트가 있습니다. 그러나 이 엔드포인트는 미국 동부(버지니아 북부) 리전에 실제로 위치하기 때문에 IAM 호출은 항상 us-east-1 리전에 대해 생성됩니다. 예를 들어, 요청된 리전이 us-west-2이 아닌 경우 모든 서비스에 대한 액세스를 거부하는 정책을 생성하면 IAM 호출이 항상 실패합니다. 이 문제에 대한 해결 방법을 보여주는 예는 NotAction 및 Deny (p. 595) 단원을 참조하십시오.

> Note
>
> `aws:RequestedRegion` 조건 키를 사용하면 서비스의 어떤 엔드포인트를 호출할지 제어할 수 있지만 작업의 영향은 제어할 수 없습니다. 일부 서비스의 경우 교차 리전 영향이 있습니다. 예를 들어, Amazon S3에 교차 리전 복제를 제어하는 API 작업이 있습니다. `s3:PutBucketReplication` 조건 키의 영향을 받는 한 리전에서 `aws:RequestedRegion`을 호출할 수 있는데 다른 리전은 복제 구성 설정에 따라 영향을 받습니다.

이 컨텍스트 키를 사용하여 지정된 리전 세트 내에서 AWS 서비스에 대한 액세스를 제한할 수 있습니다. 예를 들어, 다음 정책은 사용자가 AWS Management 콘솔에서 모든 Amazon EC2 인스턴스를 조회하도록 허용합니다. 그러나 이 정책은 아일랜드(eu-west-1), 런던(eu-west-2) 또는 파리(eu-west-3)의 인스턴스만 변경하도록 허용합니다.

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

```
    "Statement": [
        {
            "Sid": "InstanceConsoleReadOnly",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "ec2:Export*",
                "ec2:Get*",
                "ec2:Search*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "InstanceWriteRegionRestricted",
            "Effect": "Allow",
            "Action": [
                "ec2:Associate*",
                "ec2:Import*",
                "ec2:Modify*",
                "ec2:Monitor*",
                "ec2:Reset*",
                "ec2:Run*",
                "ec2:Start*",
                "ec2:Stop*",
                "ec2:Terminate*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1",
                        "eu-west-2",
                        "eu-west-3"
                    ]
                }
            }
        }
    ]
}
```

aws:RequestTag/tag-key

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청에서 전달된 태그 키-값 페어를 정책에서 지정한 태그 페어와 비교합니다. 예를 들어, 요청에 태그 키 "Dept"가 포함되어 있으며 값이 "Accounting"인지 확인할 수 있습니다. 자세한 내용은 AWS 요청 중 액세스 제어 (p. 386) 단원을 참조하십시오.

- 가용성 – 이 키는 요청에 태그가 전달될 때 요청 컨텍스트에 포함됩니다. 요청에 여러 태그가 전달되면 각 태그 키-값 페어에 대해 하나의 컨텍스트 키가 있습니다.

이 컨텍스트 키는 "aws:RequestTag/*tag-key*":"*tag-value*" 형식으로, 여기서 *tag-key* 및 *tag-value*는 한 쌍의 태그 키와 값입니다.

요청에 여러 개의 태그 키-값 페어를 포함할 수 있으므로 요청 콘텐츠는 다중 값 (p. 608) 요청이 될 수 있습니다. 이 경우 ForAllValues 또는 ForAnyValue 설정 연산자 사용을 고려해야 합니다. 자세한 내용은 다수의 키와 값 사용 (p. 610) 단원을 참조하십시오.

aws:ResourceTag/tag-key

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 정책에서 지정한 태그 키-값 페어를 리소스에 연결된 키-값 페어와 비교합니다. 예를 들어 리소스에 값이 `"Marketing"`인 태그 키 `"Dept"`와 연결된 경우에만 리소스에 대한 액세스가 필요할 수 있습니다. 자세한 내용은 AWS 리소스에 대한 액세스 제어 (p. 385) 단원을 참조하십시오.

- 가용성 – 요청된 리소스에 이미 태그가 연결된 경우 이 키는 요청 컨텍스트에 포함됩니다. 이 키는 태그를 기반으로 권한 부여를 지원하는 (p. 573) 리소스에 대해서만 반환됩니다. 각 태그 키-값 페어에는 하나의 컨텍스트 키가 있습니다.

이 컨텍스트 키는 `"aws:ResourceTag/`*`tag-key`*`":"`*`tag-value`*`"` 형식으로, 여기서 *`tag-key`* 및 *`tag-value`*는 한 쌍의 태그 키와 값입니다.

aws:SecureTransport

부울 연산자 (p. 604)를 사용합니다.

이 키를 사용하여 요청이 SSL을 사용하여 전송되었는지 여부를 확인합니다. 요청 컨텍스트는 `true` 또는 `false`를 반환합니다. 정책에서 SSL을 사용하여 요청이 전송된 경우에만 특정 작업을 허용할 수 있습니다.

- 가용성 – 이 키는 항상 요청 컨텍스트에 포함됩니다.

aws:SourceAccount

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 서비스 대 서비스 요청을 하는 리소스의 계정 ID를 정책에서 지정한 계정 ID와 비교합니다.

- 가용성 – 이 키는 리소스에 액세스하여 리소스 소유자를 대신하여 다른 서비스를 호출하도록 AWS 서비스를 트리거하는 경우에만 요청 컨텍스트에 포함됩니다. 호출하는 서비스는 원래 리소스 ARN을 호출된 서비스로 전달해야 합니다. 이 ARN은 원본 계정 ID를 포함합니다.

이 조건 키를 사용하여 Amazon S3가 혼동된 대리자 (p. 231)로 사용되고 있지 않은지 확인할 수 있습니다. 예를 들어 Amazon S3 버킷 업데이트가 Amazon SNS 주제 게시물을 트리거하면 Amazon S3 서비스에서 `sns:Publish` API 작업을 호출합니다. 버킷은 SNS 요청의 소스로 간주되며 키 값은 버킷 ARN의 계정 ID입니다.

aws:SourceArn

ARN 연산자 (p. 606)를 사용합니다.

이 키를 사용하여 서비스 대 서비스 요청을 하는 리소스의 Amazon 리소스 이름(ARN) (p. 564)을 정책에서 지정한 ARN과 비교합니다.

이 키는 요청을 하는 보안 주체의 ARN에서는 작동하지 않습니다. 대신 aws:PrincipalArn (p. 655)를 사용합니다. 소스의 ARN에는 계정 ID가 포함되어 있으므로 `aws:SourceAccount`와 함께 `aws:SourceArn`을 사용할 필요가 없습니다.

- 가용성 – 이 키는 리소스에 액세스하여 리소스 소유자를 대신하여 다른 서비스를 호출하도록 AWS 서비스를 트리거하는 경우에만 요청 컨텍스트에 포함됩니다. 호출하는 서비스는 원래 리소스의 ARN을 호출된 서비스로 전달해야 합니다.

이 조건 키를 사용하여 Amazon S3가 혼동된 대리자 (p. 231)로 사용되지 않는지 확인할 수 있습니다. 예를 들어, Amazon S3 버킷 업데이트가 Amazon SNS 주제 게시물을 트리거하면 Amazon S3 서비스에서 `sns:Publish` API 작업을 호출합니다. 버킷은 SNS 요청의 소스로 간주되며 키 값은 버킷의 ARN입니다.

aws:SourceIp

IP 주소 연산자 (p. 605)를 사용합니다.

이 키를 사용하여 요청자의 IP 주소를 정책에서 지정한 IP 주소와 비교합니다.

- 가용성 – 이 키는 요청자가 VPC 엔드포인트를 사용하여 요청한 경우를 제외하고 요청 컨텍스트에 포함됩니다.

정책 내에서 `aws:SourceIp` 조건 키를 사용하여 보안 주체가 지정된 IP 범위 내에서만 요청하도록 할 수 있습니다. 그러나 AWS 서비스가 보안 주체를 대신하여 호출을 하는 경우 이 정책은 액세스를 거부합니다. 이 경우 `aws:ViaAWSService (p. 663)` 키와 함께 `aws:SourceIp`을 사용하여 소스 IP 제한이 보안 주체가 직접 수행한 요청에만 적용되도록 할 수 있습니다.

예를 들어 다음 정책을 IAM 사용자에게 연결할 수 있습니다. 이 정책은 사용자가 지정된 IP 주소에서 호출을 수행하는 경우 객체를 `my-service-bucket` Amazon S3 버킷에 직접 넣을 수 있도록 허용합니다. 그러나 사용자가 또 다른 요청을 수행하여 서비스에서 Amazon S3를 호출하도록 하는 경우에 IP 주소 제한이 적용되지 않습니다. `PrincipalPutObjectIfIpAddress` 문은 서비스에 의해 요청이 수행되지 않은 경우에만 IP 주소를 제한합니다. `ServicePutObject` 문은 서비스에 의해 요청이 수행되는 경우 IP 주소 제한 없이 작업을 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalPutObjectIfIpAddress",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-service-bucket/*",
            "Condition": {
                "Bool": {"aws:ViaAWSService": "false"},
                "IpAddress": {"aws:SourceIp": "123.45.167.89"}
            }
        },
        {
            "Sid": "ServicePutObject",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-service-bucket/*",
            "Condition": {
                "Bool": {"aws:ViaAWSService": "true"}
            }
        }
    ]
}
```

요청이 Amazon VPC 엔드포인트를 사용하는 호스트로부터 오는 경우, `aws:SourceIp` 키를 사용할 수 없습니다. 대신에 aws:VpcSourceIp (p. 661)와 같은 VPC 전용 키를 사용해야 합니다. VPC 엔드포인트 사용에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트 - 엔드포인트 사용 제어를 참조하십시오.

aws:SourceVpc

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청이 사용자가 정책에서 지정한 VPC에서 왔는지 확인합니다. 정책에서 이 키를 사용하여 특정 VPC에 대한 액세스만 허용할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 특정 VPC에 대한 액세스 제한 단원을 참조하십시오.

- 가용성 – 이 키는 요청자가 VPC 엔드포인트를 사용하여 요청한 경우에만 요청 컨텍스트에 포함됩니다.

aws:SourceVpce

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청의 VPC 엔드포인트 식별자를 정책에서 지정한 엔드포인트 ID와 비교합니다. 정책에서 이 키를 사용하여 특정 VPC에 대한 액세스를 제한할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 특정 VPC 엔드포인트에 대한 액세스 제한 단원을 참조하십시오.

- 가용성 – 이 키는 요청자가 VPC 엔드포인트를 사용하여 요청한 경우에만 요청 컨텍스트에 포함됩니다.

aws:TagKeys

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청의 태그 키를 정책에서 지정한 키와 비교합니다. 정책을 사용하여 태그를 통해 액세스를 제어할 때 `aws:TagKeys` 조건 키를 사용하여 어떤 태그 키가 허용되는지 정의하는 것이 가장 좋습니다. 정책 예제 및 자세한 내용은 the section called “태그 키를 기반으로 액세스 제어” (p. 386) 단원을 참조하십시오.

- 가용성 – 이 키는 작업에서 리소스에 태그를 연결하는 것을 지원하는 경우에만 요청 컨텍스트에 포함됩니다.

이 컨텍스트 키는 `"aws:TagKeys":"`*`tag-key`*`"` 형식이며, 여기서 *`tag-key`*는 값이 없는 태그 키 목록입니다(예: `["Dept","Cost-Center"]`).

요청에 여러 개의 태그 키-값 페어를 포함할 수 있으므로 요청 콘텐츠는 다중 값 (p. 608) 요청이 될 수 있습니다. 이 경우 `ForAllValues` 또는 `ForAnyValue` 설정 연산자 사용을 고려해야 합니다. 자세한 내용은 다수의 키와 값 사용 (p. 610) 단원을 참조하십시오.

일부 서비스는 리소스 생성, 수정 또는 삭제와 같은 리소스 작업을 포함한 태그 지정을 지원합니다. 태그 지정 및 단일 호출과 같은 작업을 허용하려면 태그 지정 작업 및 리소스 수정 작업을 모두 포함하는 정책을 생성해야 합니다. 그런 다음 `aws:TagKeys` 조건 키를 사용하여 요청 내 특정 태그 키 사용을 적용할 수 있습니다. 예를 들어 누군가 Amazon EC2 스냅샷을 생성할 때 태그를 제한하려면 `ec2:CreateSnapshot` 생성 작업 및 `ec2:CreateTags` 태그 지정 작업을 정책에 포함시켜야 합니다. `aws:TagKeys`를 사용하는 이 시나리오에 대한 정책을 보려면 Linux 인스턴스용 Amazon EC2 사용 설명서의 태그를 사용하여 스냅샷 생성 단원을 참조하십시오.

aws:TokenIssueTime

날짜 연산자 (p. 604)를 사용합니다.

이 키를 사용하여 임시 보안 자격 증명이 발급된 날짜와 시간을 정책에서 지정한 날짜 및 시간과 비교할 수 있습니다.

- 가용성 – 이 키는 보안 주체가 임시 자격 증명을 사용하여 요청한 경우에만 요청 컨텍스트에 포함됩니다. 액세스 키를 사용하는 AWS CLI, AWS API 또는 AWS SDK 요청에는 이 키가 존재하지 않습니다.

임시 자격 증명의 사용을 지원하는 서비스에 대해 알아보려면 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

aws:UserAgent

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청자의 클라이언트 애플리케이션을 정책에서 지정한 애플리케이션과 비교합니다.

- 가용성 – 이 키는 항상 요청 컨텍스트에 포함됩니다.

  Warning

  이 키를 사용할 때는 주의해야 합니다. `aws:UserAgent` 값은 HTTP 헤더의 호출자가 제공하기 때문에, 권한이 없는 사용자가 수정된 브라우저나 사용자 지정 브라우저를 사용하여 원하는 `aws:UserAgent` 값을 제공할 수 있습니다. 따라서 무단 사용자의 직접 AWS 요청을 차단할 목적으로 `aws:UserAgent`를 사용해서는 안 됩니다. 특정 클라이언트 애플리케이션을 허용하는 데 사용할 수 있으며 정책을 테스트한 후에만 사용할 수 있습니다.

aws:userid

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청자의 보안 주체 식별자를 정책에서 지정한 ID와 비교합니다. IAM 사용자의 경우 요청 컨텍스트 값은 사용자 ID입니다. IAM 역할의 경우 이 값 형식은 다를 수 있습니다. 다른 보안 주체에 대한 정보가 표시되는 방법에 대한 자세한 내용은 보안 주체 지정 (p. 589) 단원을 참조하십시오.

- 가용성 – 이 키는 서명된 모든 요청에 대한 요청 컨텍스트에 포함됩니다. 익명 요청에는 이 키가 포함되지 않습니다.

aws:username

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청자의 사용자 이름을 정책에서 지정한 사용자 이름과 비교합니다. 다른 보안 주체에 대한 정보가 표시되는 방법에 대한 자세한 내용은 보안 주체 지정 (p. 589) 단원을 참조하십시오.

- 가용성 – 이 키는 항상 IAM 사용자의 요청 컨텍스트에 포함됩니다. 익명 요청 및 AWS 계정 루트 사용자 또는 IAM 역할에서 생성된 요청에는 이 키가 포함되지 않습니다.

aws:ViaAWSService

부울 연산자 (p. 604)를 사용합니다.

이 키를 사용하여 AWS 서비스가 사용자를 대신하여 다른 서비스에 요청을 하는지 여부를 확인합니다.

서비스가 IAM 보안 주체의 자격 증명을 사용해 보안 주체를 대신하여 요청을 수행하면 요청 컨텍스트 키에서 `true`를 반환합니다. 서비스가 서비스 역할 또는 서비스 연결 역할을 사용해 보안 주체를 대신하여 호출을 하는 경우에는 컨텍스트 키에서 `false`를 반환합니다. 보안 주체가 직접 호출을 할 때도 요청 컨텍스트 키에서 `false`를 반환합니다.

- 가용성 – 이 키는 항상 대다수 서비스의 요청 컨텍스트에 포함됩니다.

다음 서비스는 현재 `aws:ViaAWSService`를 지원하지 않습니다.

- Amazon EC2
- AWS Glue
- AWS Lake Formation
- AWS OpsWorks

이 조건 키를 사용하여 서비스에 의해 요청이 수행되었는지 여부에 따라 액세스를 허용하거나 거부할 수 있습니다. 정책에 대한 예제는 AWS: 소스 IP를 바탕으로 AWS에 대한 액세스 거부 (p. 401) 단원을 참조하십시오.

aws:VpcSourceIp

IP 주소 연산자 (p. 605)를 사용합니다.

이 키를 사용하여 요청한 IP 주소를 정책에서 지정한 IP 주소와 비교합니다. 정책에서 이 키는 요청이 지정된 IP 주소에서 시작되고 VPC 엔드포인트를 통과하는 경우에만 일치합니다.

- 가용성 – 이 키는 요청이 VPC 엔드포인트를 사용하여 이루어진 경우에만 요청 컨텍스트에 포함됩니다.

자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어 단원을 참조하십시오.

IAM 및 AWS STS 조건 컨텍스트 키

JSON 정책의 `Condition` 요소를 사용하여 모든 AWS 요청의 요청 컨텍스트에 포함된 키 값을 테스트할 수 있습니다. 이러한 키는 요청 자체 또는 해당 요청이 참조하는 리소스에 대한 정보를 제공합니다. 사용자가 요청한 작업을 허용하기 전에 키에 값이 지정되었는지 확인할 수 있습니다. 이렇게 하면 JSON 정책 문이 수신 요청과 일치 또는 불일치할 경우 보다 세분화된 제어가 가능합니다. JSON 정책의 `Condition` 요소 사용에 대한 자세한 방법은 IAM JSON 정책 요소: Condition (p. 598) 단원을 참조하십시오.

이 주제에서는 IAM 서비스(`iam:` 접두사 포함) 및 AWS Security Token Service(AWS STS) 서비스(`sts:` 접두사 포함)에서 정의 및 제공하는 키에 대해 설명합니다. 다른 여러 AWS 서비스에서도 해당 서비스가 정의한 작업 및 리소스와 관련된 서비스 고유 키를 제공합니다. 자세한 내용은 AWS 서비스에 사용되는 작업, 리소스 및 조건 키 (p. 673) 단원을 참조하십시오. 대개의 경우 조건 키를 지원하는 서비스의 설명서에 추가 정보를 확인할 수 있습니다. 예를 들어 Amazon S3 리소스 정책에서 사용할 수 있는 키에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 정책 키 단원을 참조하십시오.

주제

- IAM에서 사용할 수 있는 키 (p. 664)
- AWS 웹 자격 증명 연동에서 사용할 수 있는 키 (p. 666)
- SAML 기반 AWS STS 연동에 사용할 수 있는 키 (p. 669)
- AWS STS에서 사용할 수 있는 키 (p. 673)

IAM에서 사용할 수 있는 키

IAM 리소스에 대한 액세스 제어 정책에서는 다음과 같은 조건 키를 사용할 수 있습니다.

iam:AssociatedResourceArn

ARN 연산자 (p. 606)를 사용합니다.

대상 서비스에서 이 역할이 연결될 리소스의 ARN을 지정합니다. 리소스는 일반적으로 보안 주체가 역할을 전달하는 서비스에 속합니다. 경우에 따라 리소스는 세 번째 서비스에 속할 수 있습니다. 예를 들어 Amazon EC2 인스턴스에서 사용하는 Amazon EC2 Auto Scaling에 역할을 전달할 수 있습니다. 이 경우 조건은 Amazon EC2 인스턴스의 ARN과 일치합니다.

이 조건 키는 정책의 PassRole (p. 254) 작업에만 적용됩니다. 다른 작업을 제한하는 데 사용할 수 없습니다.

정책에서 이 조건 키를 사용하여 엔터티가 역할을 전달하도록 허용하지만, 해당 역할이 지정된 리소스와 연결된 경우에만 가능합니다. 와일드카드(*)를 사용하면 리전 또는 리소스 ID를 제한하지 않고 특정 유형의 리소스에서 작업을 수행하도록 허용할 수 있습니다. 예를 들어 IAM 사용자 또는 역할이 "us-east-1" 또는 "us-west-1" 리전의 인스턴스에서 사용할 Amazon EC2 서비스에 모든 역할을 전달하도록 허용할 수 있습니다. IAM 사용자 또는 역할은 다른 서비스에 역할을 전달하도록 허용되지 않으며, Amazon EC2가 다른 리전의 인스턴스에서 역할을 사용하도록 허용하지 않습니다.

```
{
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:PassedToService": "ec2.amazonaws.com"},
        "StringLike": {
            "iam:AssociatedResourceARN": [
                "arn:aws:ec2:us-east-1:111122223333:instance/*",
                "arn:aws:ec2:us-west-1:111122223333:instance/*"
            ]
        }
    }
}
```

Note

iam:PassedToService (p. 665)를 지원하는 AWS 서비스는 이 조건 키도 지원합니다.

iam:AWSServiceName

문자열 연산자 (p. 602)를 사용합니다.

이 역할이 연결되는 AWS 서비스를 지정합니다.

iam:OrganizationsPolicyId

문자열 연산자 (p. 602)를 사용합니다.

지정된 AWS Organizations ID가 포함된 정책이 요청에 사용된 정책과 일치하는지 확인합니다. 이 조건 키를 사용하는 예시 IAM 정책을 보려면 IAM: 조직 정책에 대해 서비스에서 마지막으로 액세스한 데이터 보기 (p. 425) 단원을 참조하십시오.

iam:PassedToService

문자열 연산자 (p. 602)를 사용합니다.

역할을 전달할 수 있는 서비스의 서비스 보안 주체를 지정합니다. 이 조건 키는 정책의 PassRole (p. 254) 작업에만 적용됩니다. 다른 작업을 제한하는 데 사용할 수 없습니다.

정책에서 이 조건 키를 사용할 때 서비스 보안 주체를 사용하여 서비스를 지정합니다. 서비스 보안 주체는 정책의 `Principal` 요소에 지정할 수 있는 서비스 이름입니다. `SERVICE_NAME_URL.amazonaws.com`이 일반적인 형식입니다.

`iam:PassedToService`를 사용하여 특정 서비스에만 역할을 전달할 수 있도록 사용자를 제한할 수 있습니다. 예를 들어, 사용자는 Amazon S3 버킷에 로그 데이터를 대신 쓸 수 있도록 CloudWatch를 신뢰하는 서비스 역할 (p. 175)을 생성할 수 있습니다. 그런 다음 사용자는 새 서비스 역할에 권한 정책 및 신뢰 정책을 연결해야 합니다. 이 경우, 신뢰 정책은 `cloudwatch.amazonaws.com` 요소에 `Principal`을 지정해야 합니다. 사용자가 CloudWatch에 역할을 전달하도록 허용하는 정책을 보려면 IAM: IAM 역할을 특정 AWS 서비스로 전달 (p. 419) 단원을 참조하십시오.

이 조건 키를 사용하면 사용자가 여러분이 지정한 서비스에 대해서만 서비스 역할을 생성하도록 할 수 있습니다. 예를 들어, 앞의 정책을 가진 사용자가 Amazon EC2에 대한 서비스 역할을 생성하려고 하면 작업이 실패합니다. 해당 사용자에게 Amazon EC2로 역할을 전달할 권한이 없기 때문입니다.

Note

AWS CodeBuild, AWS CodeCommit 등 일부 서비스는 이러한 조건 키를 지원하지 않습니다.

iam:PermissionsBoundary

문자열 연산자 (p. 602)를 사용합니다.

지정한 정책이 IAM 보안 주체 리소스에 권한 경계로서 연결되어 있는지 확인합니다. 자세한 내용은 IAM 엔터티에 대한 권한 경계 (p. 363) 단원을 참조하십시오.

iam:PolicyARN

ARN 연산자 (p. 606)를 사용합니다.

관리형 정책이 포함된 요청에서 관리형 정책의 Amazon 리소스 이름(ARN)을 확인합니다. 자세한 내용은 정책에 대한 액세스 제어 (p. 378) 단원을 참조하십시오.

iam:ResourceTag/***key-name***

문자열 연산자 (p. 602)를 사용합니다.

자격 검증 리소스(사용자 또는 역할)에 연결된 태그가 지정된 키 이름 및 값과 일치하는지 확인합니다.

Note

IAM은 `aws:ResourceTag (p. 659)` 전역 조건 키 사용을 지원하지 않습니다. AWS STS는 IAM 키와 전역 키를 모두 지원합니다.

사용자 또는 역할에 사용자 지정 속성을 키-값 페어의 형태로 추가할 수 있습니다. IAM 태그에 대한 자세한 내용은 the section called “사용자 및 역할 태그 지정” (p. 290) 단원을 참조하십시오. `iam:ResourceTag`를 사용하여 IAM 사용자 및 역할에 대한 액세스를 제어 (p. 382)할 수 있습니다. 그러나 IAM은 그룹에 대한 태그를 지원하지 않으므로 태그를 사용하여 그룹에 대한 액세스를 제어할 수 없습니다.

이 예제에서는 다음과 같은 정책을 생성할 수 있는 방법을 보여 줍니다.를 사용하면 **`status=terminated`** 태그를 통해 사용자를 삭제할 수 있습니다.이 정책을 사용하려면 정책 예제의 ***`#### ## ### ###`***를 본인의 정보로 대체하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "iam:DeleteUser",
        "Resource": "*",
        "Condition": {"StringLike": {"iam:ResourceTag/status": "terminated"}}
    }]
}
```

AWS 웹 자격 증명 연동에서 사용할 수 있는 키

웹 자격 증명 연동을 사용하여 ID 공급자(IdP)를 통해 인증된 사용자에게 임시 보안 자격 증명을 제공할 수 있습니다. 이러한 공급자의 예로는 Login with Amazon, Amazon Cognito, Google 또는 Facebook 등이 있습니다. 이 경우, 임시 보안 자격 증명을 사용해 요청하는 경우 추가 조건 키를 사용할 수 있습니다. 이러한 키를 사용하여 연동 사용자가 특정 공급자, 앱 또는 사용자와 연결된 리소스에만 액세스할 수 있도록 정책을 작성할 수 있습니다. 이러한 키는 일반적으로 역할에 대한 신뢰 정책에서 사용됩니다.

aws:FederatedProvider

문자열 연산자 (p. 602)를 사용합니다.

`FederatedProvider` 키는 사용자 인증에 사용된 IdP를 식별합니다. 예를 들어 Amazon Cognito를 통해 사용자가 인증된 경우 키에 `cognito-identity.amazonaws.com`이 포함됩니다. 마찬가지로 Login with Amazon을 통해 사용자가 인증된 경우에는 키에 `www.amazon.com` 값이 포함됩니다. 이러한 리소스 키는 다음과 같이 `aws:FederatedProvider` 키를 리소스 ARN의 정책 변수로 사용하는 리소스 정책에서 사용할 수 있습니다. 이 정책은 IdP를 사용하여 인증된 모든 사용자가 Amazon S3 버킷의 폴더에서 객체를 가져올 수 있도록 허용합니다. 그러나 버킷은 사용자를 인증한 공급자마다 달라야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": "*",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::BUCKET-NAME/${aws:FederatedProvider}/*"
  }
}
```

amr

문자열 연산자 (p. 602)를 사용합니다.

예제: `cognito-identity.amazonaws.com.com:amr`

웹 자격 증명 연동에 Amazon Cognito를 사용하는 경우에는 `cognito-identity.amazonaws.com:amr` 키(Authentication Methods Reference)에 사용자 로그인 정보가 포함됩니다. 이 키는 다수의 값을 갖습니다. 이 말은 정책 내에서 조건 설정 연산자 (p. 608)를 사용하여 테스트한다는 것을 의미합니다. 키에 추가되는 값은 다음과 같습니다.

- 사용자 인증 전에는 키에 `unauthenticated` 값만 추가됩니다.
- 사용자 인증 후에는 키에 `authenticated` 값과 호출 시 사용된 로그인 공급자 이름 (`graph.facebook.com`, `accounts.google.com` 또는 `www.amazon.com`)이 추가됩니다.

한 예로, Amazon Cognito 역할의 신뢰 정책에서는 다음 조건에 따라 사용자의 인증 여부를 테스트합니다.

```
"Condition": {
  "StringEquals":
    { "cognito-identity.amazonaws.com:aud": "us-east-2:identity-pool-id" },
  "ForAnyValue:StringLike":
    { "cognito-identity.amazonaws.com:amr": "unauthenticated" }
}
```

aud

문자열 연산자 (p. 602)를 사용합니다.

`aud` 조건 키를 사용하여 Google 클라이언트 ID 또는 Amazon Cognito 자격 증명 풀 ID가 정책에서 지정한 ID와 일치하는지 확인합니다. 동일한 자격 증명 공급자에 대해 `aud` 키와 함께 `sub` 키를 사용할 수 있습니다.

예제:

- `accounts.google.com:aud`
- `cognito-identity.amazonaws.com:aud`

`accounts.google.com:aud` 조건 키는 다음과 같은 Google ID 토큰 필드와 일치합니다.

- `azp` 필드가 설정되지 않은 경우 애플리케이션의 OAuth 2.0 Google 클라이언트 ID에 대한 `aud`. `azp` 필드가 설정되면 `aud` 필드가 `accounts.google.com:oaud` (p. 669) 조건 키와 일치합니다.
- `azp` 필드가 설정된 경우 `azp`. 이러한 경우는 웹 애플리케이션과 Android 앱이 서로 다른 OAuth 2.0 Google 클라이언트 ID를 가지고 있지만 동일한 Google API 프로젝트를 공유하는 하이브리드 앱에서 발생할 수 있습니다.

Google `aud` 및 `azp` 필드에 대한 자세한 내용은 Google ID 플랫폼 OpenID Connect 안내서를 참조하십시오.

`accounts.google.com:aud` 조건 키를 사용하여 정책을 작성할 때 앱이 `azp` 필드를 설정하는 하이브리드 앱인지 여부를 알아야 합니다.

azp 필드가 설정되지 않음

다음 예제 정책은 azp 필드를 설정하지 않는 비 하이브리드 앱에 적용됩니다. 이 경우 Google ID 토큰 aud 필드 값은 accounts.google.com:aud 및 accounts.google.com:oaud 조건 키 값과 일치합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Federated": "accounts.google.com"},
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "accounts.google.com:aud": "aud-value",
                    "accounts.google.com:oaud": "aud-value",
                    "accounts.google.com:sub": "sub-value"
                }
            }
        }
    ]
}
```

azp 필드 세트

다음 예제 정책은 azp 필드를 설정하는 하이브리드 앱에 적용됩니다. 이 경우 Google ID 토큰 aud 필드 값은 accounts.google.com:oaud 조건 키 값과 유일하게 일치합니다. azp 필드 값은 accounts.google.com:aud 조건 키 값과 일치합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Federated": "accounts.google.com"},
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "accounts.google.com:aud": "azp-value",
                    "accounts.google.com:oaud": "aud-value",
                    "accounts.google.com:sub": "sub-value"
                }
            }
        }
    ]
}
```

id

문자열 연산자 (p. 602)를 사용합니다.

예제:

- graph.facebook.com:app_id
- graph.facebook.com:id
- www.amazon.com:app_id
- www.amazon.com:user_id

이러한 키를 사용하여 애플리케이션(또는 사이트) ID 또는 사용자 ID가 정책에서 지정한 ID와 일치하는지 확인합니다. 이는 Facebook 또는 Login with Amazon에 사용됩니다. 동일한 자격 증명 공급자에 대해 app_id 키와 함께 id 키를 사용할 수 있습니다.

oaud

문자열 연산자 (p. 602)를 사용합니다.

예제: `accounts.google.com:oaud`

웹 자격 증명 연동을 위해 Google을 사용하는 경우 이 키는 이 ID 토큰의 용도인 Google 대상(`aud`)을 지정합니다. 애플리케이션의 OAuth 2.0 클라이언트 ID 중 하나여야 합니다.

sub

문자열 연산자 (p. 602)를 사용합니다.

예제:

- `accounts.google.com:sub`
- `cognito-identity.amazonaws.com:sub`

이러한 키를 사용하여 사용자 ID가 정책에서 지정한 ID와 일치하는지 확인합니다. 동일한 자격 증명 공급자에 대해 `sub` 키와 함께 `aud` 키를 사용할 수 있습니다.

웹 자격 증명 연동에 대한 자세한 내용

웹 자격 증명 연동에 대한 자세한 내용은 다음 주제 단원을 참조하십시오.

- Android용 AWS Mobile SDK Developer Guide 안내서의 Amazon Cognito 개요
- AWS Mobile SDK for iOS Developer Guide 안내서의 Amazon Cognito 개요
- 웹 자격 증명 연동에 대하여 (p. 183)

SAML 기반 AWS STS 연동에 사용할 수 있는 키

AWS Security Token Service(AWS STS)를 사용하여 SAML 기반 연동으로 작업하는 경우 정책에 조건 키를 추가할 수 있습니다.

SAML 역할 신뢰 정책

역할 신뢰 정책에서는 다음과 같은 키를 추가하여 호출자의 역할 위임 가능 여부를 구성할 수 있습니다. `saml:doc`를 제외한 모든 값은 SAML 어설션에서 가져옵니다. 조건에 따라 정책을 생성하거나 편집할 때 목록의 모든 항목을 IAM 콘솔의 시각적 편집기에서 사용할 수 있습니다. []가 표시된 항목은 지정된 유형의 목록을 값으로 가질 수 있습니다.

saml:aud

문자열 연산자 (p. 602)를 사용합니다.

SAML 어설션이 전송되는 엔드포인트 URL입니다. 이 키에 대한 값은 `Audience` 필드가 아닌 어설션의 `SAML Recipient` 필드에서 얻습니다.

saml:commonName[]

문자열 연산자 (p. 602)를 사용합니다.

`commonName` 속성입니다.

saml:cn[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduOrg` 속성입니다.

saml:doc

문자열 연산자 (p. 602)를 사용합니다.

이 키는 역할 위임 시 사용한 보안 주체를 나타냅니다. 형식은 *account-ID*/*provider-friendly-name*(예: `123456789012/SAMLProviderName`)을 따릅니다. account-ID 값은 SAML 공급자 (p. 198)가 속한 계정을 참조합니다.

saml:edupersonaffiliation[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonassurance[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonentitlement[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonnickname[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonorgdn

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonorgunitdn[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonprimaryaffiliation

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonprimaryorgunitdn

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonprincipalname

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersonscopedaffiliation[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:edupersontargetedid[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduPerson` 속성입니다.

saml:eduorghomepageuri[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduOrg` 속성입니다.

saml:eduorgidentityauthnpolicyuri[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduOrg` 속성입니다.

saml:eduorglegalname[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduOrg` 속성입니다.

saml:eduorgsuperioruri[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduOrg` 속성입니다.

saml:eduorgwhitepagesuri[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `eduOrg` 속성입니다.

saml:givenName[]

문자열 연산자 (p. 602)를 사용합니다.

`givenName` 속성입니다.

saml:iss

문자열 연산자 (p. 602)를 사용합니다.

발급자로서 URN으로 표시됩니다.

saml:mail[]

문자열 연산자 (p. 602)를 사용합니다.

`mail` 속성입니다.

saml:name[]

문자열 연산자 (p. 602)를 사용합니다.

`name` 속성입니다.

saml:namequalifier

문자열 연산자 (p. 602)를 사용합니다.

SAML 공급자의 표시 이름을 기준으로 하는 해시 값입니다. 이 값은 다음 값을 순서대로 연결하며 '/' 문자로 구분합니다.

1. `Issuer` 응답 값(`saml:iss`)
2. `AWS` 계정 ID
3. IAM에서 SAML 공급자의 표시 이름(ARN의 마지막 부분)

계정 ID, SAML 공급자 표시 이름의 연속값은 IAM 정책에서 키 `saml:doc`으로 사용 가능합니다. 자세한 내용은 SAML 기반 연동에서 사용자를 고유하게 식별하기 (p. 191) 단원을 참조하십시오.

saml:organizationStatus[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `organizationStatus` 속성입니다.

saml:primaryGroupSID[]

문자열 연산자 (p. 602)를 사용합니다.

`primaryGroupSID` 속성입니다.

saml:sub

문자열 연산자 (p. 602)를 사용합니다.

이것은 클레임의 주체로서 여기에는 조직 내 사용자 개개인을 식별할 수 있는 고유 값이 포함됩니다(예: `_cbb88bf52c2510eabe00c1642d4643f41430fe25e3`).

saml:sub_type

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `persistent`, `transient` 값을 갖거나 SAML 어설션에서 사용되는 `Format` 및 `Subject` 요소의 전체 `NameID` URI로 구성될 수 있습니다. `persistent`의 값은 `saml:sub`의 값이 세션 간 사용자에서도 동일하다는 것을 나타냅니다. 값이 `transient`인 경우 각 세션마다 사용자의 `saml:sub` 값이 다릅니다. `NameID` 요소의 `Format` 속성에 대한 자세한 내용은 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오.

saml:surname[]

문자열 연산자 (p. 602)를 사용합니다.

`surnameuid` 속성입니다.

saml:uid[]

문자열 연산자 (p. 602)를 사용합니다.

`uid` 속성입니다.

saml:x500UniqueIdentifier[]

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `x500UniqueIdentifier` 속성입니다.

`eduPerson` 및 `eduOrg` 속성에 대한 일반적인 정보는 Internet2 웹사이트 단원을 참조하십시오. `eduPerson` 속성 목록은 eduPerson Object Class Specification(201203) 단원을 참조하십시오.

형식이 목록인 조건 키에는 다수의 값이 추가될 수 있습니다. 목록 값 정책에서 조건을 생성하려면 설정 연산자 (p. 608)(`ForAllValues`, `ForAnyValue`)를 사용하면 됩니다. 예를 들어, 소속이 "faculty", "staff"("student" 제외)인 사용자를 모두 허용하려면 다음과 같은 조건을 사용할 수 있습니다.

```
"Condition": {
   "ForAllValues:StringLike": {
     "saml:edupersonaffiliation":[ "faculty", "staff"]
   }
}
```

SAML 역할 권한 정책

역할 권한 정책에서 SAML 연동으로 액세스 가능한 AWS 서비스를 정의할 때는 다음과 같은 키를 추가할 수 있습니다.

saml:namequalifier

문자열 연산자 (p. 602)를 사용합니다.

이 키에는 `saml:doc`와 `saml:iss` 값의 조합을 나타내는 해시 값이 저장됩니다. 이 해시 값은 네임스페이스 한정자로 사용되어 `saml:namequalifier`와 `saml:sub`의 조합으로 사용자를 식별합니다.

saml:sub

문자열 연산자 (p. 602)를 사용합니다.

이것은 클레임의 주체로서 여기에는 조직 내 사용자 개개인을 식별할 수 있는 고유 값이 포함됩니다(예: `_cbb88bf52c2510eabe00c1642d4643f41430fe25e3`).

saml:sub_type

문자열 연산자 (p. 602)를 사용합니다.

이 키는 `persistent`, `transient` 값을 갖거나 SAML 어설션에서 사용되는 `Format` 및 `Subject` 요소의 전체 `NameID` URI로 구성될 수 있습니다. `persistent`의 값은 `saml:sub`의 값이 세션 간 사용자에서도 동일하다는 것을 나타냅니다. 값이 `transient`인 경우 각 세션마다 사용자의 `saml:sub` 값이 다릅니다. `NameID` 요소의 `Format` 속성에 대한 자세한 내용은 인증 응답을 위한 SAML 어설션 구성 (p. 203) 단원을 참조하십시오.

이러한 키를 사용하는 방법은 SAML 2.0 기반 연동에 대하여 (p. 188) 단원을 참조하십시오.

AWS STS에서 사용할 수 있는 키

AWS Security Token Service(AWS STS) 작업을 사용하여 맡는 역할에 대한 IAM 역할 신뢰 정책에서는 다음 조건 키를 사용할 수 있습니다.

sts:ExternalId

문자열 연산자 (p. 602)를 사용합니다.

다른 계정에서 역할을 맡을 때 필요할 수도 있는 고유한 식별자. 역할이 속한 계정의 관리자가 외부 ID를 제공한 경우에는 해당 값을 `ExternalId` 파라미터에 제공하십시오. 이 값은 암호 또는 계정 번호와 같은 어떤 문자열도 가능합니다. 외부 ID의 주된 기능은 혼동된 대리자 문제를 해결하고 방지하는 것입니다. 외부 ID와 혼동된 대리자 문제에 대해 자세히 알아보려면 AWS 리소스에 대한 액세스를 타사에 부여할 때 외부 ID를 사용하는 방법 (p. 229) 단원을 참조하십시오.

`ExternalId` 값은 최소 2자, 최대 1,224자여야 합니다. 이 값은 공백 없이 영숫자여야 합니다. 이 값은 더하기(+), 등호(=), 쉼표(,) 마침표(.), 기호(@), 콜론(:), 슬래시(/) 및 하이픈(-)과 같은 기호도 포함할 수 있습니다.

sts:TransitiveTagKeys

문자열 연산자 (p. 602)를 사용합니다.

이 키를 사용하여 요청의 전이적 세션 태그 키와 정책에 지정된 전이적 세션 태그 키를 비교합니다. 임시 보안 자격 증명을 사용하여 요청하면 요청 컨텍스트 (p. 599)에 `aws:PrincipalTag (p. 657)` 컨텍스트 키가 포함됩니다. 이 키에는 세션 태그 (p. 294), 전이적 세션 태그 (p. 300) 및 역할 태그 목록이 포함됩니다. 전이적 세션 태그를 사용하면 세션 자격 증명을 사용하여 다른 역할을 맡은 경우 모든 후속 세션에서 유지됩니다. 한 역할에서 다른 역할을 맡는 것을 역할 체인 (p. 176)이라고 합니다.

정책에서 이 조건 키를 사용하여 역할을 맡거나 사용자를 연동할 때 특정 세션 태그를 전이적으로 설정하도록 요구할 수 있습니다.

AWS 서비스에 사용되는 작업, 리소스 및 조건 키

각 AWS 서비스는 IAM 정책에서 사용할 수 있는 작업, 리소스 및 조건 컨텍스트 키를 정의할 수 있습니다. 이 주제에서는 각 서비스에 대해 제공되는 요소가 문서화되는 방법을 설명합니다.

각 주제는 사용할 수 있는 작업, 리소스 및 조건 키의 목록을 제공하는 테이블로 구성되어 있습니다.

작업 테이블

작업 테이블은 IAM 정책 설명의 `Action` 요소에서 사용할 수 있는 모든 작업을 나열합니다. 서비스에서 정의된 모든 API 작업을 IAM 정책의 작업으로 사용할 수 있는 것은 아닙니다. 또한 서비스에서는 API 작업에 직접 해당하지 않는 일부 작업을 정의할 수 있습니다. 이 목록을 사용하여 IAM 정책에서 사용할 수 있는 작업을 확인합니다. `Action`, `Resource` 또는 `Condition` 요소에 대한 자세한 내용은 IAM 정책 요소 참조를 참조하십시오. 작업 및 설명 테이블 열은 자체 설명이 포함되어 있습니다.

- 액세스 레벨 열은 작업이 분류되는 방법(나열, 읽기, 쓰기, 권한 관리 또는 태그 지정)을 설명합니다. 이 분류는 정책에서 사용하는 작업이 부여하는 액세스 레벨을 이해하는 데 도움이 될 수 있습니다. 액세스 레벨에 대한 자세한 내용은 정책 요약에서 액세스 레벨 요약 이해하기를 참조하십시오.
- 리소스 유형 열은 작업의 리소스 수준 권한 지원 여부를 나타냅니다. 리소스 유형 열이 비어있으면 작업이 리소스 수준 권한을 지원하지 않는 것이기 때문에 정책에서 모든 리소스("*")를 지정해야 합니다. 리소스 유형 열에 리소스 유형이 포함되어 있으면 정책의 `Resource` 요소에서 리소스 ARN을 지정할 수 있습니다. 해당 리소스에 대한 자세한 내용은 리소스 유형 테이블의 해당 행을 참조하십시오. 하나의 문에 포함된 모든 작업 및 리소스는 서로 호환되어야 합니다. 작업에 유효하지 않은 리소스를 지정하면 해당 작업을 사용하기 위한 요청이 실패하고 문의 `Effect`가 적용되지 않습니다.

  필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.
- 조건 키 열에는 정책 문의 `Condition` 요소에서 지정할 수 있는 키가 포함됩니다. 조건 키는 작업에서, 혹은 작업과 특정 리소스에서 지원될 수도 있습니다. 따라서 키가 특정 리소스 유형과 동일한 행에 있는지 주의해서 살펴봐야 합니다. 이 테이블에는 모든 작업에서 혹은 관련 없는 상황에서도 사용할 수 있는 전역 조건 키가 포함되어 있지 않습니다. 전역 조건 키에 대한 자세한 내용은 AWS 전역 조건 컨텍스트 키를 참조하십시오.
- 종속 작업 열에는 작업을 성공적으로 호출하기 위해 작업 자체에 대한 권한 외에도 보유해야 하는 추가 권한이 포함됩니다. 이는 작업이 둘 이상의 리소스에 액세스하는 경우에 필요할 수 있습니다.

리소스 유형 테이블

Resource Types(리소스 유형) 테이블에는 `Resource` 정책 요소에서 ARN으로 지정할 수 있는 리소스 유형이 모두 나열됩니다. 모든 리소스 유형을 모든 작업에서 지정할 수 있는 것은 아닙니다. 일부 리소스 유형은 특정 작업에서만 유효합니다. 리소스 유형을 지원하지 않는 작업을 하면서 리소스 유형을 문에서 지정하면 해당 문에서 액세스를 허용하지 않습니다. `Resource` 요소에 대한 자세한 내용은 IAM JSON 정책 요소: 리소스를 참조하십시오.

- ARN 열은 이 유형의 리소스를 참조하는 데 사용해야 하는 Amazon 리소스 이름(ARN) 형식을 지정합니다. $가 앞에 오는 부분은 시나리오의 실제 값으로 대체해야 합니다. 예를 들어 ARN에서 `$user-name`이 표시되면 해당 문자열을 실제 IAM 사용자의 이름 또는 IAM 사용자의 이름이 포함된 정책 변수로 대체해야 합니다. ARN에 대한 자세한 내용은 IAM ARN 단원을 참조하십시오.
- Condition Keys(조건 키) 열은 위 테이블에서 이 리소스와 리소스를 지원하는 작업이 모두 문에 포함된 경우에만 IAM 정책 문에 포함할 수 있는 조건 컨텍스트 키를 지정합니다.

조건 키 테이블

Condition Keys(조건 키) 테이블은 IAM 정책 문의 `Condition` 요소에서 사용할 수 있는 모든 조건 컨텍스트 키를 나열합니다. 모든 키를 모든 작업 또는 리소스와 함께 지정할 수 있는 것은 아닙니다. 특정 키는 특정 유형의 작업 및 리소스에서만 작동합니다. `Condition` 요소에 대한 자세한 내용은 IAM JSON 정책 요소: 조건을 참조하십시오.

- 유형 열은 조건 키의 데이터 유형을 지정합니다. 이 데이터 유형은 요청의 값을 정책 설명의 값과 비교하는 데 사용할 수 있는 조건 연산자를 결정합니다. 데이터 유형에 적합한 연산자를 사용해야 합니다. 잘못된 연산자를 사용하면 매치가 항상 실패하고 정책 설명이 적용되지 않습니다.

유형 열이 단순한 유형 중 하나인 "List of …"를 지정하면 정책에서 여러 키와 값을 사용할 수 있습니다. 조건 설정 접두사를 연산자와 함께 사용하여 이 작업을 수행합니다. `ForAllValues` 접두사를 사용하여 요청의 모든 값이 정책 설명의 값과 일치하도록 지정합니다. `ForAnyValue` 접두사를 사용하여 요청의 하나 이상의 값이 정책 설명의 값 중 하나와 일치하도록 지정합니다.

주제

AWS Accounts에 사용되는 작업, 리소스 및 조건 키

AWS Accounts(서비스 접두사: `account`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Accounts에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DisableRegion	리전을 비활성화할 수 있는 권한을 부여합니다.	쓰기		account:TargetRegion (p. 681)	
EnableRegion	리전을 활성화할 수 있는 권한을 부여합니다.	쓰기		account:TargetRegion (p. 681)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListRegions	리전을 나열할 수 있는 권한을 부여합니다.	List			

AWS Accounts에서 정의한 리소스 유형

AWS Accounts는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Accounts에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Accounts에 사용되는 조건 키

AWS Accounts는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
account:TargetRegion	리전 목록을 기준으로 액세스를 필터링합니다.	문자열

Alexa for Business에 사용되는 작업, 리소스 및 조건 키

Alexa for Business(서비스 접두사: `a4b`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

Alexa for Business에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ApproveSkill	고객의 AWS 계정 내 조직에 스킬을 연결합니다. 이 스킬이 프라이빗 스킬인 경우 사용자는 묵시적으로 구현 도중 이 스킬에 대한 액세스를 수락합니다.	쓰기			
AssociateContactWithAddressBook	연락처를 지정된 주소록과 연결합니다.	쓰기	addressbook* (p. 687)		
			contact* (p. 687)		
AssociateDeviceWithRoom	디바이스를 지정된 공간과 연결합니다.	쓰기	device* (p. 687)		
			room* (p. 687)		
AssociateSkillGroupWithRoom	스킬 그룹을 지정된 공간과 연결합니다. SkillGroup ARN 및 Room ARN을 지정해야 합니다.	쓰기	room* (p. 687)		
			skillgroup* (p. 687)		
AssociateSkillWithSkillGroup	스킬을 스킬 그룹과 연결합니다.	쓰기	skillgroup* (p. 687)		
AssociateSkillWithUsers	등록된 사용자가 디바이스에서 프라이빗 스킬을 구현할 수 있도록 스킬 사용을 허용합니다.	쓰기			
CompleteRegistration [권한만 해당]	Alexa 디바이스 등록 작업을 완료합니다.	쓰기			
CreateAddressBook	지정된 세부 정보로 주소록을 생성합니다.	쓰기			
CreateBusinessReportSchedule	지정된 일 또는 주 간격으로 지정된 S3 위치에 전송할 사용 보고서의 반복 일정을 생성합니다.	쓰기			
CreateConferenceProvider	사용자의 AWS 계정 아래에 새 회의 공급자를 추가합니다.	쓰기			
CreateContact	지정된 세부 정보로 연락처를 생성합니다.	쓰기			
CreateProfile	새 프로필을 생성합니다.	쓰기			
CreateRoom	지정된 세부 정보로 공간을 생성합니다.	쓰기	profile* (p. 687)		
CreateSkillGroup	지정된 이름 및 설명으로 스킬 그룹을 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateUser	사용자를 생성합니다.	쓰기	user* (p. 687)		
DeleteAddressBook	주소록 ARN을 기준으로 주소록을 삭제합니다.	쓰기	addressbook* (p. 687)		
DeleteBusinessReportSchedule	지정된 일정 ARN을 갖는 보고서 전달 반복 일정을 삭제합니다.	쓰기	schedule* (p. 688)		
DeleteConferenceProvider	회의 공급자를 삭제합니다.	쓰기	conferenceprovider* (p. 687)		
DeleteContact	연락처 ARN을 기준으로 연락처를 삭제합니다.	쓰기	contact* (p. 687)		
DeleteDevice	Alexa For Business에서 디바이스를 제거합니다.	쓰기	device* (p. 687)		
DeleteProfile	프로필 ARN을 기준으로 프로필을 삭제합니다.	쓰기	profile* (p. 687)		
DeleteRoom	공간을 삭제합니다.	쓰기	room* (p. 687)		
DeleteRoomSkillParameter	스킬 및 공간에서 파라미터를 삭제합니다.	쓰기	room* (p. 687)		
DeleteSkillAuthorization	스킬에서 타사 계정에 대한 링크를 제거합니다.	쓰기	room* (p. 687)		
DeleteSkillGroup	스킬 그룹 ARN으로 스킬 그룹을 삭제합니다. SkillGroup ARN을 지정해야 합니다.	쓰기	skillgroup* (p. 687)		
DeleteUser	사용자를 삭제합니다.	쓰기	user* (p. 687)		
DisassociateContactFromAddressBook	지정된 주소록에서 연락처를 연결 해제합니다.	쓰기	addressbook* (p. 687)		
			contact* (p. 687)		
DisassociateDeviceFromRoom	현재 공간에서 디바이스를 연결 해제합니다.	쓰기	device* (p. 687)		
DisassociateSkillFromSkillGroup	스킬 그룹에서 스킬을 연결 해제합니다.	쓰기	skillgroup* (p. 687)		
DisassociateSkillFromUsers	등록된 사용자가 디바이스에서 프라이빗 스킬을 구현할 수 없도록 스킬 사용을 금지합니다.	쓰기	user* (p. 687)		
DisassociateSkillGroupFromRoom	지정된 공간에서 스킬 그룹을 연결 해제합니다. SkillGroup ARN 및 Room ARN을 지정해야 합니다.	쓰기	room* (p. 687)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			skillgroup* (p. 687)		
ForgetSmartHomeAppliances	공간에 연결된 스마트 홈 어플라이언스를 잊어버립니다.	쓰기	room* (p. 687)		
GetAddressBook	주소록 ARN을 기준으로 주소록 세부 정보를 가져옵니다.	Read	addressbook* (p. 687)		
GetConferencePreference	기존의 회의 기본 설정을 검색합니다.	Read			
GetConferenceProvider	특정 회의 공급자의 세부 정보를 가져옵니다.	Read	conferenceprovider* (p. 687)		
GetContact	연락처 ARN을 기준으로 연락처 세부 정보를 가져옵니다.	Read	contact* (p. 687)		
GetDevice	디바이스 세부 정보를 가져옵니다.	Read	device* (p. 687)		
GetNetworkProfile	네트워크 프로파일 ARN별로 네트워크 프로파일 세부 정보를 가져옵니다.	Read	networkprofile* (p. 688)		
GetProfile	프로필 ARN과 함께 제공된 프로필을 가져옵니다.	Read	profile* (p. 687)		
GetRoom	공간 세부 정보를 가져옵니다.	Read	room* (p. 687)		
GetRoomSkillParameter	스킬 및 공간에 대해 설정된 기존 파라미터를 가져옵니다.	Read	room* (p. 687)		
GetSkillGroup	스킬 그룹 ARN으로 스킬 그룹 세부 정보를 가져옵니다. SkillGroup ARN을 지정해야 합니다.	Read	skillgroup* (p. 687)		
ListBusinessReportSchedules	사용자가 구성한 일정의 세부 정보를 나열합니다.	List			
ListConferenceProviders	특정 AWS 계정의 회의 공급자를 나열합니다.	List			
ListDeviceEvents	디바이스 연결 상태를 포함하여 최대 30일간의 디바이스 이벤트 기록을 나열합니다.	List	device* (p. 687)		
ListSkills	스킬을 나열합니다.	List			
ListSkillsStoreCategories	Alexa 스킬 스토어의 모든 범주를 나열합니다.	List			
ListSkillsStoreSkillsByCategory	Alexa 스킬 스토어의 모든 스킬을 범주별로 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListSmartHomeAppliances	공간과 연결된 모든 스마트 홈 어플라이언스를 나열합니다.	List	room* (p. 687)		
ListTags	리소스의 모든 태그를 나열합니다.	Read	device (p. 687)		
			room (p. 687)		
			user (p. 687)		
PutConferencePreference	계정 수준에서 특정 회의 공급자에 대한 회의의 기본 설정을 지정합니다.	쓰기			
PutDeviceSetupEvents [권한만 해당]	Alexa 디바이스 설정 이벤트를 게시합니다.	쓰기			
PutRoomSkillParameter	스킬에 대해 공간 고유의 파라미터를 적용합니다.	쓰기	room* (p. 687)		
PutSkillAuthorization	타사 스킬 공급자에 사용자 계정을 연결합니다. 수임된 IAM 역할이 이 API 작업을 호출하는 경우 연결되는 스킬은 프라이빗 스킬이어야 합니다. 또한 IAM 역할을 수임한 AWS 계정이 해당 스킬을 소유해야 합니다.	쓰기	room* (p. 687)		
RegisterAVSDevice	원장비 제조업체(OEM)가 Alexa Voice Service(AVS)를 사용하여 제작한 Alexa 지원 디바이스를 등록합니다.	쓰기			
RegisterDevice [권한만 해당]	Alexa 디바이스를 등록합니다.	쓰기			
RejectSkill	사용자의 AWS 계정 내 조직에서 스킬을 연결 해제합니다. 이 스킬이 프라이빗 스킬인 경우 AcceptStatus를 PENDING으로 변경합니다.	쓰기			
ResolveRoom	해결된 공간 정보를 반환합니다.	Read			
RevokeInvitation	초대를 취소합니다.	쓰기	user* (p. 687)		
SearchAddressBooks	주소록을 검색하여 필터 집합 및 정렬 기준을 충족하는 주소록을 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SearchContacts	연락처를 검색하여 필터 집합 및 정렬 기준을 충족하는 연락처를 나열합니다.	List			
SearchDevices	디바이스를 검색합니다.	List			
SearchNetworkProfiles	네트워크 프로파일을 검색하여 필터 세트 및 정렬 기준을 충족하는 프로파일을 나열합니다.	List			
SearchProfiles	프로필을 검색합니다.	List			
SearchRooms	공간을 검색합니다.	List			
SearchSkillGroups	스킬 그룹을 검색합니다.	List			
SearchUsers	사용자를 검색합니다.	List			
SendInvitation	사용자에게 초대를 전송합니다.	쓰기	user* (p. 687)		
StartDeviceSync	이전 사용자가 설정한 모든 정보 및 설정을 지워 디바이스 및 계정을 알려진 기본 설정으로 복원합니다.	쓰기			
StartSmartHomeApplianceDiscovery	공간과 연결된 모든 스마트 홈 어플라이언스의 검색을 시작합니다.	Read	room* (p. 687)		
TagResource	메타데이터 태그를 리소스에 추가합니다.	태그 지정	device (p. 687)		
			room (p. 687)		
			user (p. 687)		
UntagResource	리소스에서 메타데이터 태그를 제거합니다.	태그 지정	device (p. 687)		
			room (p. 687)		
			user (p. 687)		
UpdateAddressBook	주소록 ARN을 기준으로 주소록 세부 정보를 업데이트합니다.	쓰기	addressbook* (p. 687)		
UpdateBusinessReportSchedule	지정된 일정 ARN으로 보고서 전달 일정에 대한 구성을 업데이트합니다.	쓰기	schedule* (p. 688)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateConferenceProvider	기존 회의 공급자의 설정을 업데이트합니다.	쓰기	conferenceprovider* (p. 687)		
UpdateContact	연락처 ARN을 기준으로 연락처 세부 정보를 업데이트합니다.	쓰기	contact* (p. 687)		
UpdateDevice	디바이스 이름을 업데이트합니다.	쓰기	device* (p. 687)		
UpdateProfile	기존 프로필을 업데이트합니다.	쓰기	profile* (p. 687)		
UpdateRoom	공간 세부 정보를 업데이트합니다.	쓰기	room* (p. 687)		
UpdateSkillGroup	스킬 그룹 ARN으로 스킬 그룹 세부 정보를 업데이트합니다. SkillGroup ARN을 지정해야 합니다.	쓰기	skillgroup* (p. 687)		

Alexa for Business에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 681)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
profile	`arn:${Partition}:a4b:${Region}:${Account}:profile/${Resource_id}`	
room	`arn:${Partition}:a4b:${Region}:${Account}:room/${Resource_id}`	aws:ResourceTag/${TagKey} (p. 688)
device	`arn:${Partition}:a4b:${Region}:${Account}:device/${Resource_id}`	aws:ResourceTag/${TagKey} (p. 688)
skillgroup	`arn:${Partition}:a4b:${Region}:${Account}:skill-group/${Resource_id}`	
user	`arn:${Partition}:a4b:${Region}:${Account}:user/${Resource_id}`	aws:ResourceTag/${TagKey} (p. 688)
addressbook	`arn:${Partition}:a4b:${Region}:${Account}:address-book/${Resource_id}`	
conferenceprovider	`arn:${Partition}:a4b:${Region}:${Account}:conference-provider/${Resource_id}`	
contact	`arn:${Partition}:a4b:${Region}:${Account}:contact/${Resource_id}`	

리소스 유형	ARN	조건 키
schedule	`arn:${Partition}:a4b:${Region}:${Account}:schedule/${Resource_id}`	
networkprofile	`arn:${Partition}:a4b:${Region}:${Account}:network-profile/${Resource_id}`	

Alexa for Business의 조건 키

Alexa for Business는 `Condition` 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
a4b:amazonId	요청의 Amazon ID를 기준으로 작업을 필터링합니다.	문자열
a4b:filters_deviceType	요청의 디바이스 유형을 기준으로 작업을 필터링합니다.	문자열
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Amplify에 사용되는 작업, 리소스 및 조건 키

AWS Amplify(서비스 접두사: `amplify`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Amplify에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateApp	새 Amplify 앱을 생성합니다.	쓰기	apps* (p. 692)		
				aws:RequestTag/${TagKey} (p. 692) aws:TagKeys (p. 692)	
CreateBackendEnvironment	Amplify App을 위한 새로운 백엔드 환경을 생성합니다.	쓰기	apps* (p. 692)		
CreateBranch	Amplify 앱의 새 브랜치를 생성합니다.	쓰기	apps* (p. 692)		
				aws:RequestTag/${TagKey} (p. 692) aws:TagKeys (p. 692)	
CreateDeployment	수동 배포 앱을 위한 배포를 생성합니다. (앱은 리포지토리에 연결되지 않음)	쓰기	branches* (p. 692)		
CreateDomainAssociation	앱에서 새 DomainAssociation을 생성합니다.	쓰기	apps* (p. 692)		
				aws:RequestTag/${TagKey} (p. 692) aws:TagKeys (p. 692)	
CreateWebHook	앱에서 새로운 웹후크를 생성합니다.	쓰기	branches* (p. 692)		
DeleteApp	appId를 기준으로 기존 Amplify 앱을 삭제합니다.	쓰기	apps* (p. 692)		
DeleteBackendEnvironment	Amplify 앱의 브랜치를 삭제합니다.	쓰기	apps* (p. 692)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteBranch	Amplify 앱의 브랜치를 삭제합니다.	쓰기	branches* (p. 692)		
DeleteDomainAssociation	DomainAssociation을 삭제합니다.	쓰기	domains* (p. 692)		
DeleteJob	Amplify 브랜치(Amplify App의 일부)에 대한 작업을 삭제합니다.	쓰기	jobs* (p. 692)		
DeleteWebHook	ID를 기준을 웹후크를 삭제합니다.	쓰기	apps* (p. 692)		
GenerateAccessLogs	미리 서명된 URL을 통해 특정 시간 범위에 대한 웹 사이트 액세스 로그를 생성합니다.	쓰기	apps* (p. 692)		
GetApp	appId를 기준으로 기존 Amplify 앱을 검색합니다.	Read	apps* (p. 692)		
GetArtifactUrl	아티팩트 ID에 해당하는 아티팩트 정보를 검색합니다.	Read	apps* (p. 692)		
GetBackendEnvironment	Amplify App을 위한 백엔드 환경을 검색합니다.	Read	apps* (p. 692)		
GetBranch	Amplify 앱의 브랜치를 검색합니다.	Read	branches* (p. 692)		
GetDomainAssociation	appId 및 domainName과 일치하는 도메인 정보를 검색합니다.	Read	domains* (p. 692)		
GetJob	브랜치(Amplify 앱의 일부)에 대한 작업을 가져옵니다.	Read	jobs* (p. 692)		
GetWebHook	webhookId와 일치하는 웹후크 정보를 가져옵니다.	Read	apps* (p. 692)		
ListApps	기존 Amplify 앱을 삭제합니다.	List			
ListArtifacts	앱, 분기, 작업 및 아티팩트 유형을 이용해 아티팩트를 나열합니다.	List	apps* (p. 692)		
ListBackendEnvironments	Amplify App을 위한 백엔드 환경을 나열합니다.	List	apps* (p. 692)		
ListBranches	Amplify 앱의 브랜치를 나열합니다.	List	apps* (p. 692)		
ListDomainAssociations	앱이 있는 도메인을 나열합니다.	List	apps* (p. 692)		
ListJobs	브랜치(Amplify 앱의 일부)에 대한 작업을 나열합니다.	List	branches* (p. 692)		
ListWebHooks	앱에 대한 웹후크를 나열합니다.	List	apps* (p. 692)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartDeployment	수동 배포 앱을 위한 배포를 시작합니다. (앱은 리포지토리에 연결되지 않음)	쓰기	branches* (p. 692)		
StartJob	브랜치(Amplify 앱의 일부)에 대한 새 작업을 시작합니다.	쓰기	jobs* (p. 692)		
StopJob	Amplify 브랜치(Amplify 앱의 일부)에 대해 진행 중인 작업을 중지합니다.	쓰기	jobs* (p. 692)		
TagResource	AWS Amplify Console 리소스에 태그를 지정합니다.	태그 지정	apps (p. 692)		
			branches (p. 692)		
			jobs (p. 692)		
				aws:TagKeys (p. 692) aws:RequestTag/${TagKey} (p. 692)	
UntagResource	AWS Amplify Console 리소스에서 태그를 제거합니다.	태그 지정	apps (p. 692)		
			branches (p. 692)		
			jobs (p. 692)		
				aws:TagKeys (p. 692)	
UpdateApp	기존 Amplify 앱을 업데이트합니다.	쓰기	apps* (p. 692)		
UpdateBranch	Amplify 앱의 브랜치를 삭제합니다.	쓰기	branches* (p. 692)		
UpdateDomainAssociation	앱에 대한 DomainAssociation을 업데이트합니다.	쓰기	domains* (p. 692)		
UpdateWebHook	웹후크를 업데이트합니다.	쓰기	apps* (p. 692)		

AWS Amplify에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 688)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유

형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
apps	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey} (p. 692)
branches	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}`	aws:ResourceTag/${TagKey} (p. 692)
jobs	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}/jobs/${JobId}`	
domains	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/domains/${DomainName}`	aws:ResourceTag/${TagKey} (p. 692)

AWS Amplify에 사용되는 조건 키

AWS Amplify는 `Condition` 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}		문자열
aws:ResourceTag/${TagKey}		문자열
aws:TagKeys		문자열

Amazon API Gateway에 사용되는 작업, 리소스 및 조건 키

Amazon API Gateway(서비스 접두사: `execute-api`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon API Gateway에서 정의한 작업 (p. 693)

Amazon API Gateway에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
InvalidateCache	클라이언트 요청에 따라 API 캐시를 무효화하는 데 사용됩니다.	쓰기	execute-api-general* (p. 693)		
Invoke	클라이언트 요청에 따라 API를 호출하는 데 사용됩니다.	쓰기	execute-api-general* (p. 693)		
ManageConnections	ManageConnections는 @connections API에 대한 액세스를 제어합니다.	쓰기	execute-api-general* (p. 693)		

Amazon API Gateway에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 693)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
execute-api-general	`arn:${Partition}:execute-api:${Region}:${Account}:${ApiId}/${Stage}/${Method}/${ApiSpecificResourcePath}`	

Amazon API Gateway의 조건 키

ExecuteAPI에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS App Mesh에 사용되는 작업, 리소스 및 조건 키

AWS App Mesh(서비스 접두사: `appmesh`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS App Mesh에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateMesh	메시를 생성합니다.	쓰기	mesh* (p. 698)		
				aws:TagKeys (p. 698) aws:RequestTag/${TagKey} (p. 698)	
CreateRoute	가상 라우터와 연결되는 라우팅을 생성합니다.	쓰기	route* (p. 698)		
			virtualNode (p. 698)		
				aws:TagKeys (p. 698)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 698)	
CreateVirtualNode	서비스 메시 내에 가상 노드를 생성합니다.	쓰기	virtualNode* (p. 698)		
			virtualService (p. 698)		
				aws:TagKeys (p. 698) aws:RequestTag/${TagKey} (p. 698)	
CreateVirtualRouter	서비스 메시 내에 가상 라우터를 생성합니다.	쓰기	virtualRouter* (p. 698)		
				aws:TagKeys (p. 698) aws:RequestTag/${TagKey} (p. 698)	
CreateVirtualService	서비스 메시 내에 가상 서비스를 생성합니다.	쓰기	virtualService* (p. 698)		
			virtualNode (p. 698)		
			virtualRouter (p. 698)		
				aws:TagKeys (p. 698) aws:RequestTag/${TagKey} (p. 698)	
DeleteMesh	기존 서비스 메시를 삭제합니다.	쓰기	mesh* (p. 698)		
DeleteRoute	기존 라우팅을 삭제합니다.	쓰기	route* (p. 698)		
DeleteVirtualNode	기존 가상 노드를 삭제합니다.	쓰기	virtualNode* (p. 698)		
DeleteVirtualRouter	기존 가상 라우터를 삭제합니다.	쓰기	virtualRouter* (p. 698)		
DeleteVirtualService	기존 가상 서비스를 삭제합니다.	쓰기	virtualService* (p. 698)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeMesh	기존 서비스 메시를 설명합니다.	Read	mesh* (p. 698)		
DescribeRoute	기존 라우팅을 설명합니다.	Read	route* (p. 698)		
DescribeVirtualNode	기존 가상 노드를 설명합니다.	Read	virtualNode* (p. 698)		
DescribeVirtualRouter	기존 가상 라우터를 설명합니다.	Read	virtualRouter* (p. 698)		
DescribeVirtualService	기존 가상 서비스를 설명합니다.	Read	virtualService* (p. 698)		
ListMeshes	기존 서비스 메시의 목록을 반환합니다.	List			
ListRoutes	서비스 메시의 기존 라우팅의 목록을 반환합니다.	List	virtualRouter* (p. 698)		
ListTagsForResource	App Mesh 리소스에 대한 태그를 나열합니다.	List	mesh (p. 698)		
			route (p. 698)		
			virtualNode (p. 698)		
			virtualRouter (p. 698)		
			virtualService (p. 698)		
ListVirtualNodes	기존 가상 노드의 목록을 반환합니다.	List	mesh* (p. 698)		
ListVirtualRouters	서비스 메시의 기존 가상 라우터의 목록을 반환합니다.	List	virtualRouter* (p. 698)		
ListVirtualServices	서비스 메시의 기존 가상 서비스의 목록을 반환합니다.	List	virtualService* (p. 698)		
StreamAggregatedResources	Envoy 프록시가 VirtualNode에 대한 스트리밍된 리소스를 수신하도록 허용합니다.	Read	virtualNode* (p. 698)		
TagResource	리소스에 지정된 태그를 지정된 resourceArn과 연결합니다.	쓰기	mesh (p. 698)		
			route (p. 698)		
			virtualNode (p. 698)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			virtualRouter (p. 698)		
			virtualService (p. 698)		
				aws:TagKeys (p. 698) aws:RequestTag/${TagKey} (p. 698)	
UntagResource	리소스에서 지정된 태그를 삭제합니다.	쓰기	mesh (p. 698)		
			route (p. 698)		
			virtualNode (p. 698)		
			virtualRouter (p. 698)		
			virtualService (p. 698)		
				aws:TagKeys (p. 698)	
UpdateMesh	기존 서비스 메시를 업데이트합니다.	쓰기	mesh* (p. 698)		
UpdateRoute	지정된 서비스 메시 및 가상 라우터에 대한 기존 라우팅을 업데이트합니다.	쓰기	route* (p. 698)		
			virtualNode (p. 698)		
UpdateVirtualNode	지정된 서비스 메시에서 기존 가상 노드를 업데이트합니다.	쓰기	virtualNode* (p. 698)		
UpdateVirtualRouter	지정된 서비스 메시에서 기존 가상 라우터를 업데이트합니다.	쓰기	virtualRouter* (p. 698)		
UpdateVirtualService	지정된 서비스 메시에서 기존 가상 서비스를 업데이트합니다.	쓰기	mesh* (p. 698)		
			virtualNode (p. 698)		
			virtualRouter (p. 698)		

AWS App Mesh에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 694)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
mesh	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}`	aws:ResourceTag/${TagKey} (p. 698)
virtualService	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	aws:ResourceTag/${TagKey} (p. 698)
virtualNode	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}`	aws:ResourceTag/${TagKey} (p. 698)
virtualRouter	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}`	aws:ResourceTag/${TagKey} (p. 698)
route	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}`	aws:ResourceTag/${TagKey} (p. 698)

AWS App Mesh에 사용되는 조건 키

AWS App Mesh는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS App Mesh 미리 보기에 사용되는 작업, 리소스 및 조건 키

AWS App Mesh 미리 보기(서비스 접두사: `appmesh-preview`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS App Mesh 미리 보기에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateMesh	메시를 생성합니다.	쓰기	mesh* (p. 701)		
CreateRoute	가상 라우터와 연결되는 라우팅을 생성합니다.	쓰기	route* (p. 701)		
			virtualNode (p. 701)		
CreateVirtualNode	서비스 메시 내에 가상 노드를 생성합니다.	쓰기	virtualNode* (p. 701)		
			virtualService (p. 701)		
CreateVirtualRouter	서비스 메시 내에 가상 라우터를 생성합니다.	쓰기	virtualRouter* (p. 701)		
CreateVirtualService	서비스 메시 내에 가상 서비스를 생성합니다.	쓰기	virtualService* (p. 701)		
			virtualNode (p. 701)		
			virtualRouter (p. 701)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteMesh	기존 서비스 메시를 삭제합니다.	쓰기	mesh* (p. 701)		
DeleteRoute	기존 라우팅을 삭제합니다.	쓰기	route* (p. 701)		
DeleteVirtualNode	기존 가상 노드를 삭제합니다.	쓰기	virtualNode* (p. 701)		
DeleteVirtualRouter	기존 가상 라우터를 삭제합니다.	쓰기	virtualRouter* (p. 701)		
DeleteVirtualService	기존 가상 서비스를 삭제합니다.	쓰기	virtualService* (p. 701)		
DescribeMesh	기존 서비스 메시를 설명합니다.	Read	mesh* (p. 701)		
DescribeRoute	기존 라우팅을 설명합니다.	Read	route* (p. 701)		
DescribeVirtualNode	기존 가상 노드를 설명합니다.	Read	virtualNode* (p. 701)		
DescribeVirtualRouter	기존 가상 라우터를 설명합니다.	Read	virtualRouter* (p. 701)		
DescribeVirtualService	기존 가상 서비스를 설명합니다.	Read	virtualService* (p. 701)		
ListMeshes	기존 서비스 메시의 목록을 반환합니다.	List			
ListRoutes	서비스 메시의 기존 라우팅의 목록을 반환합니다.	List	virtualRouter* (p. 701)		
ListVirtualNodes	기존 가상 노드의 목록을 반환합니다.	List	mesh* (p. 701)		
ListVirtualRouters	서비스 메시의 기존 가상 라우터의 목록을 반환합니다.	List	virtualRouter* (p. 701)		
ListVirtualServices	서비스 메시의 기존 가상 서비스의 목록을 반환합니다.	List	virtualService* (p. 701)		
StreamAggregatedResources	Envoy 프록시가 VirtualNode에 대한 스트리밍된 리소스를 수신하도록 허용합니다.	Read	virtualNode* (p. 701)		
UpdateMesh	기존 서비스 메시를 업데이트합니다.	쓰기	mesh* (p. 701)		
UpdateRoute	지정된 서비스 메시 및 가상 라우터에 대한 기존 라우팅을 업데이트합니다.	쓰기	route* (p. 701)		
			virtualNode (p. 701)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateVirtualNode	지정된 서비스 메시에서 기존 가상 노드를 업데이트합니다.	쓰기	virtualNode* (p. 701)		
UpdateVirtualRouter	지정된 서비스 메시에서 기존 가상 라우터를 업데이트합니다.	쓰기	virtualRouter* (p. 701)		
UpdateVirtualService	지정된 서비스 메시에서 기존 가상 서비스를 업데이트합니다.	쓰기	mesh* (p. 701)		
			virtualNode (p. 701)		
			virtualRouter (p. 701)		

AWS App Mesh Preview에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 699)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
mesh	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}`	
virtualService	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	
virtualNode	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}`	
virtualRouter	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}`	
route	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}`	

AWS App Mesh 미리 보기에 사용되는 조건 키

App Mesh 미리 보기에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS AppConfig에 사용할 수 있는 작업, 리소스 및 조건 키

AWS AppConfig(서비스 접두사: `appconfig`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에서 사용할 수 있는 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS AppConfig에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateApplication	애플리케이션을 생성할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
				aws:RequestTag/${TagKey} (p. 708) aws:TagKeys (p. 708)	
CreateConfigurationProfile	구성 프로필을 생성할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			configurationprofile* (p. 707)		
				aws:RequestTag/${TagKey} (p. 708) aws:TagKeys (p. 708)	
CreateDeploymentStrategy	배포 전략을 생성할 수 있는 권한을 부여합니다.	쓰기	deploymentstrategy* (p. 707)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 708) aws:TagKeys (p. 708)	
CreateEnvironment	환경을 생성할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			environment* (p. 707)		
				aws:RequestTag/${TagKey} (p. 708) aws:TagKeys (p. 708)	
DeleteApplication	애플리케이션을 삭제할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
DeleteConfigurationProfile	구성 프로필을 삭제할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			configurationprofile* (p. 707)		
DeleteDeploymentStrategy	배포 전략을 삭제할 수 있는 권한을 부여합니다.	쓰기	deploymentstrategy* (p. 707)		
DeleteEnvironment	환경을 삭제할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			environment* (p. 707)		
GetApplication	애플리케이션에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	application* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
GetConfiguration	구성에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	application* (p. 707)		
			configurationprofile* (p. 707)		
			environment* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetConfigurationProfile	구성 프로필에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	application* (p. 707)		
			configurationprofile* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
GetDeployment	배포에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	application* (p. 707)		
			deployment* (p. 707)		
			environment* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
GetDeploymentStrategy	배포 전략에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	deploymentstrategy* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
GetEnvironment	환경에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	application* (p. 707)		
			environment* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
ListApplications	계정에서 애플리케이션을 나열할 수 있는 권한을 부여합니다.	List			
ListConfigurationProfiles	애플리케이션의 구성 프로파일을 나열할 수 있는 권한을 부여합니다.	List	application* (p. 707)		
ListDeploymentStrategies	계정에 대한 배포 전략을 나열할 수 있는 권한을 부여합니다.	List			
ListDeployments	환경에 대한 배포를 나열할 수 있는 권한을 부여합니다.	List	application* (p. 707)		
			environment* (p. 707)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListEnvironments	애플리케이션의 환경을 나열할 수 있는 권한을 부여합니다.	List	application* (p. 707)		
ListTagsForResource	지정된 리소스에 대한 리소스 태그 목록을 볼 수 있는 권한을 부여합니다.	Read	application (p. 707)		
			configurationprofile (p. 707)		
			deployment (p. 707)		
			deploymentstrategy (p. 707)		
			environment (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
StartDeployment	배포를 시작할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			configurationprofile* (p. 707)		
			deployment* (p. 707)		
			deploymentstrategy* (p. 707)		
			environment* (p. 707)		
StopDeployment	배포를 중지할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			deployment* (p. 707)		
			environment* (p. 707)		
TagResource	appconfig 리소스에 태그를 지정할 수 있는 권한을 부여합니다.	태그 지정	application (p. 707)		
			configurationprofile (p. 707)		
			deployment (p. 707)		
			deploymentstrategy (p. 707)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			environment (p. 707)		
				aws:TagKeys (p. 708) aws:RequestTag/${TagKey} (p. 708) aws:ResourceTag/${TagKey} (p. 708)	
UntagResource	appconfig 리소스의 태그를 해제할 수 있는 권한을 부여합니다.	태그 지정	application (p. 707)		
			configurationprofile (p. 707)		
			deployment (p. 707)		
			deploymentstrategy (p. 707)		
			environment (p. 707)		
				aws:TagKeys (p. 708)	
UpdateApplication	애플리케이션을 수정할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
UpdateConfigurationProfile	구성 프로필을 수정할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			configurationprofile* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
UpdateDeploymentStrategy	배포 전략을 수정할 수 있는 권한을 부여합니다.	쓰기	deploymentstrategy* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateEnvironment	환경을 수정할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			environment* (p. 707)		
				aws:ResourceTag/${TagKey} (p. 708)	
ValidateConfiguration	구성을 검증할 수 있는 권한을 부여합니다.	쓰기	application* (p. 707)		
			configurationprofile* (p. 707)		

AWS AppConfig에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 702)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
application	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey} (p. 708)
environment	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}`	aws:ResourceTag/${TagKey} (p. 708)
configurationprofile	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}`	aws:ResourceTag/${TagKey} (p. 708)
deploymentstrategy	`arn:${Partition}:appconfig:${Region}:${Account}:deploymentstrategy/${DeploymentStrategyId}`	aws:ResourceTag/${TagKey} (p. 708)
deployment	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/deployment/${DeploymentNumber}`	aws:ResourceTag/${TagKey} (p. 708)

AWS AppConfig의 조건 키

AWS AppConfig는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	지정된 태그에 허용되는 값 세트를 기준으로 '생성' 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	AWS 리소스에 할당된 태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	필수 태그가 요청에 포함되는지 여부를 기준으로 '생성' 요청을 필터링합니다.	문자열

Application Auto Scaling에 사용되는 작업, 리소스 및 조건 키

Application Auto Scaling(서비스 접두사: `application-autoscaling`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Application Auto Scaling에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteScalingPolicy	이전에 생성된 Application Auto Scaling 조정 정책을 삭제합니다.	쓰기			
DeleteScheduledAction	이전에 생성된 Application Auto Scaling 예약 작업을 삭제합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeregisterScalableTarget	이전에 등록된 확장 가능 대상을 등록 취소합니다.	쓰기			
DescribeScalableTargets	지정된 서비스 네임스페이스를 사용하여 확장 가능 대상에 대한 설명이 포함된 정보를 제공합니다.	Read			
DescribeScalingActivities	지정된 서비스 네임스페이스를 사용하여 이전 6주 동안의 조정 활동에 대한 설명이 포함된 정보를 제공합니다.	Read			
DescribeScalingPolicies	지정된 서비스 네임스페이스를 사용하여 조정 정책에 대한 설명이 포함된 정보를 제공합니다.	Read			
DescribeScheduledActions	지정된 서비스 네임스페이스를 사용하여 예약된 작업에 대한 설명이 포함된 정보를 제공합니다.	Read			
PutScalingPolicy	기존 Application Auto Scaling 확장 가능 대상에 대한 정책을 생성 또는 업데이트합니다.	쓰기			
PutScheduledAction	기존 Application Auto Scaling 확장 가능 대상에 대해 예약된 작업을 생성 또는 업데이트합니다.	쓰기			
RegisterScalableTarget	확장 가능 대상을 등록 또는 업데이트합니다. 확장 가능 대상은 Application Auto Scaling을 사용하여 확장하거나 축소할 수 있는 리소스입니다.	쓰기			

Application Auto Scaling에서 정의한 리소스 유형

Application Auto Scaling은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Application Auto Scaling에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Application Auto Scaling의 조건 키

Application Auto Scaling에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Application Discovery에 사용되는 작업, 리소스 및 조건 키

Application Discovery(서비스 접두사: `discovery`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Application Discovery에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateConfigurationItemsToApplication	하나 이상의 구성 항목을 애플리케이션과 연결합니다	쓰기			
BatchDeleteImportData	각각 가져오기 ID로 식별된 하나 이상의 Migration Hub 가져오기 작업을 삭제합니다. 각 가져오기 작업에는 서버 또는 애플리케이션이 식별할 수 있는 여러 레코드가 있습니다.	쓰기			
CreateApplication	주어진 이름과 설명으로 애플리케이션을 생성합니다.	쓰기			
CreateTags	구성 항목에 대해 하나 이상의 태그를 만듭니다. 태그는 IT 자산 분류에 도움을 주는 메타데이터입니다. 이 API는 여러 구성 항목의 목록을 허용합니다.	태그 지정			
DeleteApplications	애플리케이션의 목록 및 구성 항목과의 연결을 삭제합니다.	쓰기			
DeleteTags	구성 항목과 하나 이상의 태그 간 연결을 삭제합니다. 이 API는 여러 구성 항목의 목록을 허용합니다.	태그 지정			
DescribeAgents	ID별로 에이전트 또는 커넥터를 나열하거나 ID를 지정하지 않은 경우 사용자 계정과 연결된 모든 에이전트/커넥터를 나열합니다.	Read			
DescribeConfigurations	구성 항목 ID의 목록에 대한 속성을 가져옵니다. 제공된 ID가 모두	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	동일한 자산 유형(서버, 애플리케이션, 프로세스 또는 연결)이어야 합니다. 출력 필드는 선택된 자산 유형에 고유해야 합니다. 예를 들어, 서버 구성 항목에 대한 출력은 호스트 이름, 운영 체제 및 네트워크 카드 수 등 서버에 대한 속성 목록을 포함합니다.				
DescribeContinuousExports	ID로 지정된 내보내기를 나열합니다. DescribeContinuousExports를 호출하면 사용자 계정과 연결된 연속 내보내기를 모두 나열할 수 있습니다(이 작업은 어떤 파라미터도 전달하지 않기 때문).	Read			
DescribeExportConfigurations	지정된 내보내기 프로세스의 상태를 가져옵니다. 최대 100개의 프로세스에서 상태를 가져올 수 있습니다.	Read			
DescribeExportTasks	하나 이상의 내보내기 작업의 상태를 검색합니다. 최대 100개 내보내기 작업의 상태를 검색할 수 있습니다.	Read			
DescribeImportTasks	계정에 대한 내보내기 작업의 배열을 반환합니다(상태 정보, 시간, ID, 내보내기 파일의 Amazon S3 객체 URL 등).	List			
DescribeTags	특정 태그로 지정된 구성 항목의 목록을 가져옵니다. 또는 특정 구성 항목에 할당된 모든 태그의 목록을 가져옵니다.	Read			
DisassociateConfigurationItemsFromApplication	애플리케이션에서 하나 이상의 구성 항목의 연결을 해제합니다.	쓰기			
ExportConfigurations	모든 발견된 구성 데이터를 보고 평가할 수 있는 Amazon S3 버킷 또는 애플리케이션으로 내보냅니다. 데이터는 태그과 태그 연결, 프로세스, 연결, 서버 및 시스템 성능을 포함합니다.	쓰기			
GetDiscoverySummary	발견된 자산에 대한 간단한 설명을 가져옵니다.	Read			
ListConfigurations	필터에 지정하는 기준에 따라 구성 항목의 목록을 가져옵니다. 필터 기준은 관계 요구 사항을 식별합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListServerNeighbors	지정된 서버로부터 멀리 떨어진 하나의 네트워크 홉인 서버의 목록을 가져옵니다.	List			
StartContinuousExport	에이전트가 검색한 데이터의 Amazon Athena로의 연속 흐름을 시작합니다.	쓰기			
StartDataCollectionByAgentIds	지정된 에이전트 또는 커넥터가 데이터 수집을 시작하도록 지시합니다.	쓰기			
StartExportTask	발견된 구성 항목 및 관계에 대한 구성 데이터를 지정된 형식의 S3 버킷으로 내보냅니다.	쓰기			
StartImportTask	가져오기 작업을 시작합니다. Migration Hub 가져오기 기능은 온프레미스 환경의 세부 정보를 Discovery Connector 또는 Discovery Agent 같은 Application Discovery Service(ADS) 도구를 사용하지 않고 AWS로 직접 가져올 수 있게 해줍니다. 그러면 디바이스를 애플리케이션으로 그룹화하고 해당 마이그레이션 상태를 추적하는 등 가져온 데이터에서 직접 마이그레이션 평가 및 계획을 수행할 수 있습니다.	쓰기			
StopContinuousExport	에이전트가 검색한 데이터의 Amazon Athena로의 연속 흐름을 중지합니다.	쓰기			
StopDataCollectionByAgentIds	지정된 에이전트 또는 커넥터가 데이터 수집을 중지하도록 지시합니다.	쓰기			
UpdateApplication	애플리케이션에 대한 메타데이터를 업데이트합니다.	쓰기			

Application Discovery에서 정의한 리소스 유형

Application Discovery는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Application Discovery에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Application Discovery에 사용되는 조건 키

Application Discovery에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Application Discovery Arsenal에 사용되는 작업, 리소스 및 조건 키

Application Discovery Arsenal(서비스 접두사: `arsenal`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Application Discovery Arsenal에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RegisterOnPremisesAgent [권한만 해당]	AWS에서 제공하는 데이터 수집기를 Application Discovery Arsenal에 등록할 수 있는 권한을 부여합니다.	쓰기			

Application Discovery Arsenal에서 정의한 리소스 유형

Application Discovery Arsenal는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Application Discovery Arsenal에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Application Discovery Arsenal의 조건 키

Application Discovery Arsenal에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon AppStream 2.0에 사용되는 작업, 리소스 및 조건 키

Amazon AppStream 2.0(서비스 접두사: `appstream`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon AppStream 2.0에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateFleet	지정된 플릿을 지정된 스택과 연결할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 721)		
			stack* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
BatchAssociateUserStack	지정된 사용자를 지정된 스택과 연결할 수 있는 권한을 부여합니다. 플릿이 Active Directory 도메인에 병합되는 스택에는 사용자 풀 사용자를 할당할 수 없습니다.	쓰기	stack* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
BatchDisassociateUserStack	지정된 스택에서 지정된 사용자를 연결 해제할 수 있는 권한을 부여합니다.	쓰기	stack* (p. 721)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:ResourceTag/${TagKey} (p. 722)	
CopyImage	지정된 이미지를 동일한 리전 안에서 복사하거나 동일한 AWS 계정 안의 새 리전으로 복사할 수 있는 권한을 부여합니다.	쓰기	image* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
CreateDirectoryConfig	AppStream 2.0에서 디렉터리 구성 객체를 생성할 수 있는 권한을 부여합니다. 이 객체는 플릿 및 이미지 빌더를 Microsoft Active Directory 도메인에 조인하는 데 필요한 구성 정보를 포함하고 있습니다.	쓰기			
CreateFleet	플릿을 생성할 수 있는 권한을 부여합니다. 플릿은 애플리케이션이 실행되고 사용자로 스트리밍되는 스트리밍 인스턴스 그룹입니다.	쓰기	fleet* (p. 721)		
			image* (p. 721)		
				aws:RequestTag/${TagKey} (p. 722) aws:TagKeys (p. 722)	
CreateImageBuilder	이미지 빌더를 생성할 수 있는 권한을 부여합니다. 이미지 빌더는 이미지를 생성하는 데 사용하는 가상 머신입니다.	쓰기	image* (p. 721)		
			image-builder* (p. 721)		
				aws:RequestTag/${TagKey} (p. 722) aws:TagKeys (p. 722)	
CreateImageBuilderStreamingURL	이미지 빌더 스트리밍 세션을 시작할 URL을 생성할 수 있는 권한을 부여합니다.	쓰기	image-builder* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateStack	사용자에게 애플리케이션 스트리밍을 시작할 스택을 생성할 수 있는 권한을 부여합니다. 스택은 연결된 플릿, 사용자 액세스 정책 및 스토리지 구성으로 구성되어 있습니다.	쓰기	stack* (p. 721)		
				aws:RequestTag/${TagKey} (p. 722) aws:TagKeys (p. 722)	
CreateStreamingURL	지정된 사용자에 대한 AppStream 2.0 스트리밍 세션을 시작할 임시 URL을 생성할 수 있는 권한을 부여합니다. 스트리밍 URL은 사용자 설정 없이 애플리케이션 스트리밍을 테스트할 수 있게 해줍니다.	쓰기	fleet* (p. 721)		
			stack* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
CreateUsageReportSubscription	사용 보고서 구독을 생성할 수 있는 권한을 부여합니다. 사용 보고서는 매일 생성됩니다.	쓰기			
CreateUser	사용자 풀에서 새 사용자를 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteDirectoryConfig	AppStream 2.0에서 지정된 디렉터리 구성 객체를 삭제할 수 있는 권한을 부여합니다. 이 객체는 플릿 및 이미지 빌더를 Microsoft Active Directory 도메인에 조인하는 데 필요한 구성 정보를 포함하고 있습니다.	쓰기			
DeleteFleet	지정된 플릿을 삭제할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
DeleteImage	지정된 이미지를 삭제할 수 있는 권한을 부여합니다. 사용 중인 이미지는 삭제할 수 없습니다.	쓰기	image* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
DeleteImageBuilder	지정된 이미지 빌더를 삭제하여 용량을 해제할 수 있는 권한을 부여합니다.	쓰기	image-builder* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteImagePermissions	지정된 프라이빗 이미지에 대한 권한을 삭제할 수 있는 권한을 부여합니다.	쓰기	image* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
DeleteStack	지정된 스택을 삭제할 수 있는 권한을 부여합니다. 스택이 삭제되면 사용자가 해당 스택에 의해 제공되는 애플리케이션 스트리밍 환경을 더 이상 이용할 수 없습니다. 또한 해당 스택의 애플리케이션 스트리밍 세션에 대한 예약도 모두 해제됩니다.	쓰기	stack* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
DeleteUsageReportSubscription	사용 보고서 생성을 비활성화할 수 있는 권한을 부여합니다.	쓰기			
DeleteUser	사용자 풀에서 사용자를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DescribeDirectoryConfigs	객체 이름이 제공될 경우, AppStream 2.0에 사용되는 하나 이상의 지정된 디렉터리 구성 객체를 설명하는 목록을 검색할 수 있는 권한을 부여합니다. 그렇지 않을 경우, 계정의 모든 디렉터리 구성 객체가 설명됩니다. 이 객체는 플릿 및 이미지 빌더를 Microsoft Active Directory 도메인에 조인하는 데 필요한 구성 정보를 포함하고 있습니다.	Read			
DescribeFleets	플릿 이름이 제공될 경우, 하나 이상의 지정된 플릿을 설명하는 목록을 검색할 수 있는 권한을 부여합니다. 그렇지 않을 경우, 계정의 모든 플릿이 설명됩니다.	Read	fleet (p. 721)		
DescribeImageBuilders	이미지 빌더 이름이 제공될 경우, 하나 이상의 지정된 이미지 빌더를 설명하는 목록을 검색할 수 있는 권한을 부여합니다. 그렇지 않을 경우, 계정의 모든 이미지 빌더가 설명됩니다.	Read	image-builder (p. 721)		
DescribeImagePermissions	사용자가 소유하는 프라이빗 이미지와 공유된 AWS 계정 ID에 대한 권한을 설명하는 목록을 검색할 수 있는 권한을 부여합니다.	Read	image* (p. 721)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeImages	이미지 이름 또는 이미지 ARN이 제공되는 경우, 하나 이상의 지정된 이미지를 설명하는 목록을 검색할 수 있는 권한을 부여합니다. 그렇지 않을 경우, 계정의 모든 이미지가 설명됩니다.	Read	image (p. 721)		
DescribeSessions	지정된 스택 및 플릿의 스트리밍 세션을 설명하는 목록을 검색할 수 있는 권한을 부여합니다. 스택 및 플랫의 사용자 ID가 제공되는 경우, 해당 사용자의 스트리밍 세션만 설명됩니다.	Read	fleet* (p. 721)		
			stack* (p. 721)		
DescribeStacks	스택 이름이 제공될 경우, 하나 이상의 지정된 스택을 설명하는 목록을 검색할 수 있는 권한을 부여합니다. 그렇지 않을 경우, 계정의 모든 스택이 설명됩니다.	Read	stack (p. 721)		
DescribeUsageReportSubscriptions	하나 이상의 사용 보고서 구독을 설명하는 목록을 검색할 수 있는 권한을 부여합니다.	Read			
DescribeUserStackAssociations	UserStackAssociation 객체를 설명하는 목록을 검색할 수 있는 권한을 부여합니다.	Read	stack (p. 721)		
DescribeUsers	사용자 풀의 사용자를 설명하는 목록을 검색할 수 있는 권한을 부여합니다.	Read			
DisableUser	사용자 풀에서 지정된 사용자를 비활성화할 수 있는 권한을 부여합니다. 이 작업은 사용자를 삭제하지 않습니다.	쓰기			
DisassociateFleet	지정된 스택에서 지정된 플릿을 연결 해제할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 721)		
			stack* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
EnableUser	사용자 풀에서 사용자를 활성화할 수 있는 권한을 부여합니다.	쓰기			
ExpireSession	지정된 스트리밍 세션을 즉시 중지할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetImageBuilders [권한만 해당]	이미지 빌더 이름이 제공될 경우, 하나 이상의 지정된 이미지 빌더를 설명하는 목록을 검색할 수 있는 권한을 부여합니다. 그렇지 않을 경우, 계정의 모든 이미지 빌더가 설명됩니다.	Read			
GetParametersForImageUpload [권한만 해당]	테마 자산을 업로드할 수 있는 권한을 부여합니다.	쓰기			
ListAssociatedFleets	지정된 스택과 연결된 플릿의 이름을 검색할 수 있는 권한을 부여합니다.	Read	stack* (p. 721)		
ListAssociatedStacks	지정된 플릿과 연결된 스택의 이름을 검색할 수 있는 권한을 부여합니다.	Read	fleet* (p. 721)		
ListTagsForResource	지정된 AppStream 2.0 리소스에 대한 모든 태그의 목록을 검색할 수 있는 권한을 부여합니다. 다음 리소스에 태그를 지정할 수 있습니다. 이미지 빌더, 이미지, 플릿 및 스택	Read			
StartFleet	지정된 플릿을 시작할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
StartImageBuilder	지정된 이미지 빌더를 시작할 수 있는 권한을 부여합니다.	쓰기	image-builder* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
StopFleet	지정된 플릿을 중지할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
StopImageBuilder	지정된 이미지 빌더를 중지할 수 있는 권한을 부여합니다.	쓰기	image-builder* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Stream	연합된 사용자에게 지정된 스택의 기존 자격 증명 및 스트림 애플리케이션을 사용하여 로그인할 수 있는 권한을 부여합니다.	쓰기	stack* (p. 721)		
				appstream:userId (p. 722)	
TagResource	지정된 AppStream 2.0 리소스에 대해 하나 이상의 태그를 추가 또는 덮어쓰기할 수 있는 권한을 부여합니다. 다음 리소스에 태그를 지정할 수 있습니다. 이미지 빌더, 이미지, 플릿 및 스택	태그 지정	fleet (p. 721)		
			image (p. 721)		
			image-builder (p. 721)		
			stack (p. 721)		
				aws:RequestTag/${TagKey} (p. 722) aws:TagKeys (p. 722) aws:ResourceTag/${TagKey} (p. 722)	
UntagResource	지정된 AppStream 2.0 리소스에서 하나 이상의 태그를 연결 해제할 수 있는 권한을 부여합니다.	태그 지정	fleet (p. 721)		
			image (p. 721)		
			image-builder (p. 721)		
			stack (p. 721)		
				aws:TagKeys (p. 722)	
UpdateDirectoryConfig	AppStream 2.0에서 지정된 디렉터리 구성 객체를 업데이트할 수 있는 권한을 부여합니다. 이 객체는 플릿 및 이미지 빌더를 Microsoft Active Directory 도메인에 조인하는 데 필요한 구성 정보를 포함하고 있습니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateFleet	지정된 플릿을 업데이트할 수 있는 권한을 부여합니다. 플릿이 STOPPED 상태에 있을 때 플릿 이름을 제외한 모든 속성을 업데이트할 수 있습니다.	쓰기	fleet* (p. 721)		
			image (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
UpdateImagePermissions	지정된 프라이빗 이미지에 대한 권한을 추가 또는 업데이트할 수 있는 권한을 부여합니다.	쓰기	image* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	
UpdateStack	지정된 스택에 대한 지정된 필드를 업데이트할 수 있는 권한을 부여합니다.	쓰기	stack* (p. 721)		
				aws:ResourceTag/${TagKey} (p. 722)	

Amazon AppStream 2.0에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 714)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
fleet	`arn:${Partition}:appstream:${Region}:${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey} (p. 722)
image	`arn:${Partition}:appstream:${Region}:${Account}:image/${ImageName}`	aws:ResourceTag/${TagKey} (p. 722)
image-builder	`arn:${Partition}:appstream:${Region}:${Account}:image-builder/${ImageBuilderName}`	aws:ResourceTag/${TagKey} (p. 722)
stack	`arn:${Partition}:appstream:${Region}:${Account}:stack/${StackName}`	aws:ResourceTag/${TagKey} (p. 722)

Amazon AppStream 2.0에 사용되는 조건 키

Amazon AppStream 2.0은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
appstream:userId	AppStream 2.0 사용자의 ID를 기준으로 액세스를 필터링합니다.	문자열
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS AppSync에 사용되는 작업, 리소스 및 조건 키

AWS AppSync(서비스 접두사: `appsync`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS AppSync에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateApiKey	API를 실행하는 클라이언트에 배포할 수 있는 고유 키를 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateDataSource	DataSource 객체를 생성합니다.	쓰기			
CreateFunction	새 Function 객체를 생성합니다.	쓰기			
CreateGraphqlApi	최상위 AppSync 리소스인 GraphqlApi 객체를 생성합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 726) aws:TagKeys (p. 726)	
CreateResolver	Resolver 객체를 생성합니다. 해석기는 수신 요청을 데이터 원본이 이해할 수 있는 형식으로 변환하고 데이터 원본의 응답을 GraphQL로 변환합니다.	쓰기			
CreateType	Type 객체를 생성합니다.	쓰기			
DeleteApiKey	API 키를 삭제합니다.	쓰기			
DeleteDataSource	DataSource 객체를 삭제합니다.	쓰기			
DeleteFunction	Function 객체를 삭제합니다.	쓰기			
DeleteGraphqlApi	GraphqlApi 객체를 삭제합니다. 이렇게 하면 해당 API 아래의 모든 AppSync 리소스도 정리됩니다.	쓰기	graphqlapi* (p. 725)		
				aws:ResourceTag/${TagKey} (p. 726)	
DeleteResolver	Resolver 객체를 삭제합니다.	쓰기			
DeleteType	Type 객체를 삭제합니다.	쓰기			
GetDataSource	DataSource 객체를 검색합니다.	Read			
GetFunction	Function 객체를 검색합니다.	Read			
GetGraphqlApi	GraphqlApi 객체를 검색합니다.	Read	graphqlapi* (p. 725)		
				aws:ResourceTag/${TagKey} (p. 726)	
GetIntrospectionSchema	GraphQL API에 대한 내부 검사 스키마를 검색합니다.	Read			
GetResolver	Resolver 객체를 검색합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetSchemaCreationStatus	스키마 생성 작업의 현재 상태를 검색합니다.	Read			
GetType	Type 객체를 검색합니다.	Read			
GraphQL	GraphQL 쿼리를 GraphQL API로 전송합니다.	쓰기	field* (p. 726)		
			graphqlapi* (p. 725)		
ListApiKeys	지정된 API에 대한 API 키를 나열합니다.	List			
ListDataSources	지정된 API에 대한 데이터 원본을 나열합니다.	List			
ListFunctions	지정된 API에 대한 함수를 나열합니다.	List			
ListGraphqlApis	GraphQL API를 나열합니다.	List			
ListResolvers	지정된 API 및 유형에 대한 해석기를 나열합니다.	List			
ListResolversByFunction	특정 함수와 연결된 해석기를 나열합니다.	List			
ListTagsForResource	리소스에 대한 태그를 나열합니다.	Read	graphqlapi (p. 725)		
				aws:ResourceTag/${TagKey} (p. 726)	
ListTypes	지정된 API에 대한 유형을 나열합니다.	List			
StartSchemaCreation	새 스키마를 GraphQL API에 추가합니다. 이 작업은 비동기식입니다. 작업이 완료되면 GetSchemaCreationStatus가 표시될 수 있습니다.	쓰기			
TagResource	리소스에 태그를 지정합니다.	태그 지정	graphqlapi (p. 725)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 726) aws:ResourceTag/${TagKey} (p. 726) aws:TagKeys (p. 726)	
UntagResource	리소스에서 태그를 제거합니다.	태그 지정	graphqlapi (p. 725)		
				aws:TagKeys (p. 726)	
UpdateApiKey	지정된 API에 대한 API 키를 업데이트합니다.	쓰기			
UpdateDataSource	DataSource 객체를 업데이트합니다.	쓰기			
UpdateFunction	기존 Function 객체를 업데이트합니다.	쓰기			
UpdateGraphqlApi	GraphqlApi 객체를 업데이트합니다.	쓰기	graphqlapi* (p. 725)		
				aws:ResourceTag/${TagKey} (p. 726)	
UpdateResolver	Resolver 객체를 업데이트합니다.	쓰기			
UpdateType	Type 객체를 업데이트합니다.	쓰기			

AWS AppSync에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 722)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
datasource	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/datasources/${DatasourceName}`	
graphqlapi	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}`	aws:ResourceTag/${TagKey} (p. 726)

리소스 유형	ARN	조건 키
field	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}/fields/${FieldName}`	
type	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}`	
function	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/functions/${FunctionId}`	

AWS AppSync의 조건 키

AWS AppSync는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Artifact에 사용되는 작업, 리소스 및 조건 키

AWS Artifact(서비스 접두사: `artifact`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Artifact에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptAgreement	고객 계정에서 아직 수락하지 않은 AWS 계약서를 수락할 수 있는 권한을 부여합니다.	쓰기	agreement* (p. 727)		
DownloadAgreement	고객 계정에서 아직 수락하지 않은 AWS 계약서 또는 수락한 고객 계약서를 다운로드할 수 있는 권한을 부여합니다.	Read	agreement (p. 727)		
			customer-agreement (p. 727)		
Get	AWS 규정 준수 패키지를 다운로드할 수 있는 권한을 부여합니다.	Read	report-package* (p. 727)		
TerminateAgreement	고객 계정에서 이전에 수락한 고객 계약서를 종료할 수 있는 권한을 부여합니다.	쓰기	customer-agreement* (p. 727)		

AWS Artifact에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 727)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
report-package	`arn:${Partition}:artifact:::report-package/*`	
customer-agreement	`arn:${Partition}:artifact::${Account}:customer-agreement/*`	
agreement	`arn:${Partition}:artifact:::agreement/*`	

AWS Artifact의 조건 키

Artifact에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Athena에 사용되는 작업, 리소스 및 조건 키

Amazon Athena(서비스 접두사: `athena`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Athena에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchGetNamedQuery	하나 이상의 명명된 쿼리에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	workgroup* (p. 731)		
BatchGetQueryExecution	하나 이상의 쿼리 실행에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	workgroup* (p. 731)		
CancelQueryExecution	사용되지 않음. 1.1.0 이전의 Athena JDBC 드라이버를 사용하는 AWS 서비스 및 보안 주체에만 적용합니다. 그렇지 않을 경우 StopQueryExecution을 사용합니다.	쓰기	workgroup* (p. 731)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateNamedQuery	명명된 쿼리를 생성할 수 있는 권한을 부여합니다.	쓰기	workgroup* (p. 731)		
CreateWorkGroup	작업 그룹을 생성할 수 있는 권한을 부여합니다.	태그 지정	workgroup* (p. 731)		
				aws:RequestTag/${TagKey} (p. 732) aws:TagKeys (p. 732)	
DeleteNamedQuery	지정된 명명된 쿼리를 삭제할 수 있는 권한을 부여합니다.	쓰기	workgroup* (p. 731)		
DeleteWorkGroup	작업 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	workgroup* (p. 731)		
GetCatalogs	Athena JDBC 드라이버 버전 1.1.0을 사용하는 AWS 관리형 정책 및 보안 주체에만 적용됩니다. 데이터베이스 및 테이블에 대한 액세스를 활성화할 수 있는 권한을 부여합니다.	Read			
GetExecutionEngine	Athena JDBC 드라이버 버전 1.1.0을 사용하는 AWS 관리형 정책 및 보안 주체에만 적용됩니다. 지정된 데이터베이스 및 테이블에 대한 액세스를 활성화할 수 있는 권한을 부여합니다.	Read			
GetExecutionEngines	Athena JDBC 드라이버 버전 1.1.0을 사용하는 AWS 관리형 정책 및 보안 주체에만 적용됩니다. 데이터베이스 및 테이블에 대한 액세스를 활성화할 수 있는 권한을 부여합니다.	Read			
GetNamedQuery	지정된 명명된 쿼리에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	workgroup* (p. 731)		
GetNamespace	Athena JDBC 드라이버 버전 1.1.0을 사용하는 AWS 관리형 정책 및 보안 주체에만 적용됩니다. 지정된 데이터베이스 및 테이블에 대한 액세스를 활성화할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetNamespaces	Athena JDBC 드라이버 버전 1.1.0을 사용하는 AWS 관리형 정책 및 보안 주체에만 적용됩니다. 데이터베이스 및 테이블에 대한 액세스를 활성화할 수 있는 권한을 부여합니다.	Read			
GetQueryExecution	지정된 쿼리 실행에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	workgroup* (p. 731)		
GetQueryExecutions	사용되지 않음. 1.1.0 이전의 Athena JDBC 드라이버를 사용하는 AWS 서비스 및 보안 주체에만 적용합니다. 그렇지 않을 경우 ListQueryExecutions를 사용합니다.	Read			
GetQueryResults	쿼리 결과를 가져올 수 있는 권한을 부여합니다.	Read	workgroup* (p. 731)		
GetQueryResultsStream	쿼리 결과 스트림을 가져올 수 있는 권한을 부여합니다.	Read	workgroup* (p. 731)		
GetTable	Athena JDBC 드라이버 버전 1.1.0을 사용하는 AWS 관리형 정책 및 보안 주체에만 적용됩니다. 지정된 테이블에 대한 액세스를 활성화할 수 있는 권한을 부여합니다.	Read			
GetTables	Athena JDBC 드라이버 버전 1.1.0을 사용하는 AWS 관리형 정책 및 보안 주체에만 적용됩니다. 테이블에 대한 액세스를 활성화할 수 있는 권한을 부여합니다.	Read			
GetWorkGroup	작업 그룹을 가져올 수 있는 권한을 부여합니다.	Read	workgroup* (p. 731)		
ListNamedQueries	지정된 AWS 구성에 대한 Amazon Athena의 명명된 쿼리 목록을 반환할 수 있는 권한을 부여합니다.	List	workgroup* (p. 731)		
ListQueryExecutions	지정된 AWS 구성에 대한 쿼리 실행 목록을 반환할 수 있는 권한을 부여합니다.	List	workgroup* (p. 731)		
ListTagsForResource	작업 그룹에 대한 태그 목록을 반환할 수 있는 권한을 부여합니다.	Read	workgroup* (p. 731)		
ListWorkGroups	지정된 AWS 계정에 대한 작업 그룹 목록을 반환할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RunQuery	사용되지 않음. 1.1.0 이전의 Athena JDBC 드라이버를 사용하는 AWS 서비스 및 보안 주체에만 적용합니다. 그렇지 않을 경우 StartQueryExecution을 사용합니다.	쓰기			
StartQueryExecution	문자열로 제공된 SQL 쿼리를 사용하여 쿼리 실행을 시작할 수 있는 권한을 부여합니다.	쓰기	workgroup* (p. 731)		
StopQueryExecution	지정된 쿼리 실행을 중지할 수 있는 권한을 부여합니다.	쓰기	workgroup* (p. 731)		
TagResource	작업 그룹에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	workgroup* (p. 731)		
				aws:RequestTag/${TagKey} (p. 732) aws:TagKeys (p. 732)	
UntagResource	작업 그룹에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	workgroup* (p. 731)		
				aws:TagKeys (p. 732)	
UpdateWorkGroup	작업 그룹을 업데이트할 수 있는 권한을 부여합니다.	쓰기	workgroup* (p. 731)		

Amazon Athena에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 728)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
workgroup	`arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}`	aws:ResourceTag/${TagKey} (p. 732)

Amazon Athena에 사용되는 조건 키

Amazon SES는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Auto Scaling에 사용되는 작업, 리소스 및 조건 키

AWS Auto Scaling(서비스 접두사: `autoscaling-plans`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Auto Scaling에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateScalingPlan	조정 계획을 생성합니다.	쓰기			
DeleteScalingPlan	지정된 조정 계획을 삭제합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeScalingPlanResources	지정된 조정 계획에서 확장 가능한 리소스를 설명합니다.	Read			
DescribeScalingPlans	지정된 조정 계획 또는 모든 조정 계획을 설명합니다.	Read			
GetScalingPlanResourceForecastData	조정 가능한 리소스에 대한 예측 데이터를 검색합니다.	Read			
UpdateScalingPlan	조정 계획을 업데이트합니다.	쓰기			

AWS Auto Scaling에서 정의한 리소스 유형

AWS Auto Scaling은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Auto Scaling에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Auto Scaling에 사용되는 조건 키

Auto Scaling에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Backup에 사용되는 작업, 리소스 및 조건 키

AWS Backup(서비스 접두사: `backup`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Backup에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CopyIntoBackupVault [권한만 해당]	백업 볼트에 복사합니다.	쓰기			
CreateBackupPlan	새 백업 계획을 생성합니다.	쓰기	backupPlan* (p. 737)		
				aws:RequestTag/${TagKey} (p. 737) aws:TagKeys (p. 737)	
CreateBackupSelection	백업 계획에 새 리소스 할당을 생성합니다.	쓰기	backupPlan* (p. 737)		iam:PassRole
CreateBackupVault	새 백업 볼트를 생성합니다.	쓰기	backupVault* (p. 737)		
				aws:RequestTag/${TagKey} (p. 737) aws:TagKeys (p. 737)	
DeleteBackupPlan	백업 계획을 삭제합니다.	쓰기	backupPlan* (p. 737)		
DeleteBackupSelection	백업 계획에서 리소스 할당을 삭제합니다.	쓰기	backupPlan* (p. 737)		
DeleteBackupVault	백업 볼트를 삭제합니다.	쓰기	backupVault* (p. 737)		
DeleteBackupVaultAccessPolicy	백업 볼트 액세스 정책을 삭제합니다.	쓰기	backupVault* (p. 737)		
DeleteBackupVaultNotifications	백업 볼트에서 알림을 제거합니다.	쓰기	backupVault* (p. 737)		
DeleteRecoveryPoint	백업 볼트에서 복구 시점을 삭제합니다.	쓰기	recoveryPoint* (p. 737)		
DescribeBackupJob	백업 작업을 설명합니다.	Read			
DescribeBackupVault	지정된 이름으로 새 백업 볼트를 생성합니다.	Read	backupVault* (p. 737)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeCopyJob	복사 작업을 설명합니다.	Read		aws:RequestTag/${TagKey} (p. 737) aws:TagKeys (p. 737)	
DescribeProtectedResource	보호되는 리소스를 설명합니다.	Read			
DescribeRecoveryPoint	복구 시점을 설명합니다.	Read	recoveryPoint* (p. 737)		
DescribeRestoreJob	복원 자업을 설명합니다.	Read			
ExportBackupPlanTemplate	백업 계획을 JSON으로 내보냅니다.	Read			
GetBackupPlan	백업 계획을 가져옵니다.	Read	backupPlan* (p. 737)		
GetBackupPlanFromJSON	JSON을 백업 계획으로 변환합니다.	Read			
GetBackupPlanFromTemplate	템플릿을 백업 계획으로 변환합니다.	Read			
GetBackupSelection	백업 계획 리소스 할당을 가져옵니다.	Read	backupPlan* (p. 737)		
GetBackupVaultAccessPolicy	백업 볼트 액세스 정책을 가져옵니다.	Read	backupVault* (p. 737)		
GetBackupVaultNotifications	백업 볼트 알림을 가져옵니다.	Read	backupVault* (p. 737)		
GetRecoveryPointRestoreMetadata	복구 시점 복원 메타데이터를 가져옵니다.	Read	recoveryPoint* (p. 737)		
GetSupportedResourceTypes	지원되는 리소스 유형을 가져옵니다.	Read			
ListBackupJobs	백업 작업을 나열합니다.	List			
ListBackupPlanTemplates	AWS Backup이 제공하는 백업 계획 템플릿을 나열합니다.	List			
ListBackupPlanVersions	백업 계획 버전을 나열합니다.	List	backupPlan* (p. 737)		
ListBackupPlans	백업 계획을 나열합니다.	List			
ListBackupSelections	특정 백업 계획의 리소스 할당을 나열합니다.	List	backupPlan* (p. 737)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListBackupVaults	백업 볼트를 나열합니다.	List			
ListCopyJobs	복사 작업을 나열합니다.	List			
ListProtectedResources	AWS Backup에 의해 보호되는 리소스를 나열합니다.	List			
ListRecoveryPointsByBackupVault	백업 볼트 내부의 복구 시점을 나열합니다.	List	backupVault* (p. 737)		
ListRecoveryPointsByResource	리소스의 복구 시점을 나열합니다.	List			
ListRestoreJobs	복원 작업을 나열합니다.	List			
ListTags	리소스에 대한 태그를 나열합니다.	List			
PutBackupVaultAccessPolicy	백업 볼트에 액세스 정책을 추가합니다.	쓰기	backupVault* (p. 737)		
PutBackupVaultNotifications	백업 볼트에 SNS 주제를 추가합니다.	쓰기	backupVault* (p. 737)		
StartBackupJob	새 백업 작업을 시작합니다.	쓰기	backupVault* (p. 737)		iam:PassRole
StartCopyJob	소스 리전에서 대상 리전으로 백업을 복사합니다.	쓰기	recoveryPoint* (p. 737)		iam:PassRole
				aws:RequestTag/${TagKey} (p. 737) aws:TagKeys (p. 737)	
StartRestoreJob	새 복원 작업을 시작합니다.	쓰기	recoveryPoint* (p. 737)		iam:PassRole
StopBackupJob	백업 작업을 중지합니다.	쓰기			
TagResource	리소스에 태그를 지정합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 737) aws:TagKeys (p. 737)	
UntagResource	리소스에서 태그를 제거합니다.	태그 지정		aws:TagKeys (p. 737)	
UpdateBackupPlan	백업 계획을 업데이트합니다.	쓰기	backupPlan* (p. 737)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateRecoveryPointLifecycle	복구 시점의 수명 주기를 업데이트합니다	쓰기	recoveryPoint* (p. 737)		

AWS Backup에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 733)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
backupVault	`arn:${Partition}:backup:${Region}:${Account}:backup-vault:${BackupVaultName}`	
backupPlan	`arn:${Partition}:backup:${Region}:${Account}:backup-plan:${BackupPlanId}`	
recoveryPoint	`arn:${Partition}:${Vendor}:${Region}:*:${ResourceType}:${RecoveryPointId}`	

AWS Backup에 사용되는 조건 키

AWS Backup은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Backup 스토리지에 사용되는 작업, 리소스 및 조건 키

AWS Backup 스토리지(서비스 접두사: `backup-storage`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Backup 스토리지에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
MountCapsule [권한만 해당]	KMS 키를 백업 볼트에 연결합니다.	쓰기			

AWS Backup 스토리지에서 정의한 리소스 유형

AWS Backup 스토리지는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Backup 스토리지에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Backup 스토리지에 사용되는 조건 키

Backup 스토리지에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Batch에 사용되는 작업, 리소스 및 조건 키

AWS Batch(서비스 접두사: `batch`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Batch에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelJob	AWS Batch 작업 대기열에서 작업을 취소합니다.	쓰기			
CreateComputeEnvironment	AWS Batch 컴퓨팅 환경을 생성합니다.	쓰기			
CreateJobQueue	AWS Batch 작업 대기열을 생성합니다.	쓰기			
DeleteComputeEnvironment	AWS Batch 컴퓨팅 환경을 삭제합니다.	쓰기			
DeleteJobQueue	지정된 작업 대기열을 삭제합니다.	쓰기			
DeregisterJobDefinition	AWS Batch 작업 정의를 등록 취소합니다.	쓰기	job-definition* (p. 740)		
DescribeComputeEnvironments	하나 이상의 컴퓨팅 환경을 설명합니다.	Read			
DescribeJobDefinitions	작업 정의 목록을 설명합니다.	Read			
DescribeJobQueues	하나 이상의 작업 대기열을 설명합니다.	Read			
DescribeJobs	AWS Batch 작업 목록을 설명합니다.	Read			
ListJobs	지정된 작업 대기열에 대한 작업 목록을 반환합니다.	List			
RegisterJobDefinition	AWS Batch 작업 정의를 등록합니다.	쓰기	job-definition* (p. 740)		
				batch:User (p. 741)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				batch:Privileged (p. 741) batch:Image (p. 740)	
SubmitJob	작업 정의의 AWS Batch 작업을 제출합니다.	쓰기	job-definition* (p. 740)		
			job-queue* (p. 740)		
TerminateJob	작업 대기열에서 작업을 종료합니다.	쓰기			
UpdateComputeEnvironment	AWS Batch 컴퓨팅 환경을 업데이트합니다.	쓰기			
UpdateJobQueue	작업 대기열을 업데이트합니다.	쓰기			

AWS Batch에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 739)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
job-queue	`arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}`	
job-definition	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}:${Revision}`	

AWS Batch에 사용되는 조건 키

AWS Batch는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
batch:Image	컨테이너를 시작하는 데 사용되는 이미지입니다.	문자열

조건 키	설명	유형
batch:Privileged	이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).	부울
batch:User	컨테이너 내부에서 사용할 사용자 이름 또는 숫자 uid입니다.	문자열

AWS Billing에 사용되는 작업, 리소스 및 조건 키

AWS Billing(서비스 접두사: `aws-portal`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Billing에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyAccount	IAM 사용자가 Account Settings를 수정할 수 있도록 허용하거나 거부합니다.	쓰기			
ModifyBilling	결제(billing) 설정을 수정할 수 있는 IAM 사용자 권한을 허용하거나 거부합니다.	쓰기			
ModifyPaymentMethods	지불 방법을 수정할 수 있는 IAM 사용자 권한을 허용하거나 거부합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ViewAccount	계정 설정을 볼 수 있는 IAM 사용자 권한을 허용하거나 거부합니다.	Read			
ViewBilling	콘솔에서 결제(billing) 페이지를 볼 수 있는 IAM 사용자 권한을 허용하거나 거부합니다.	Read			
ViewPaymentMethods	지불 방법을 볼 수 있는 IAM 사용자 권한을 허용하거나 거부합니다	Read			
ViewUsage	AWS 사용 보고서를 볼 수 있는 IAM 사용자 권한을 허용하거나 거부합니다.	Read			

AWS Billing에서 정의한 리소스 유형

AWS Billing은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Billing에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Billing에 사용되는 조건 키

Billing에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Budget Service에 사용되는 작업, 리소스 및 조건 키

AWS Budget Service(서비스 접두사: `budgets`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Budget Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시

됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Note

이 테이블에서의 작업은 API가 아니라, 예산에 액세스하는 AWS Billing and Cost Management API에 대한 액세스를 부여하는 권한입니다.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyBudget	예산 및 예산 세부 정보를 수정합니다.	쓰기	budget* (p. 743)		
ViewBudget	예산 및 예산 세부 정보를 봅니다.	Read	budget* (p. 743)		

AWS Budget Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 742)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
budget	`arn:${Partition}:budgets::${Account}:budget/${BudgetName}`	

AWS Budget Service에 사용되는 조건 키

Budget에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Certificate Manager에 사용되는 작업, 리소스 및 조건 키

AWS Certificate Manager(서비스 접두사: `acm`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS Certificate Manager에서 정의한 작업 (p. 744)
- AWS Certificate Manager에서 정의한 리소스 유형 (p. 745)
- AWS Certificate Manager의 조건 키 (p. 745)

AWS Certificate Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTagsToCertificate	하나 이상의 태그를 인증서에 추가합니다.	태그 지정	certificate* (p. 745)		
				aws:RequestTag/${TagKey} (p. 745) aws:TagKeys (p. 746)	
DeleteCertificate	인증서 및 연결된 프라이빗 키를 삭제합니다.	쓰기	certificate* (p. 745)		
DescribeCertificate	지정된 인증서에 포함된 필드의 목록을 반환합니다.	Read	certificate* (p. 745)		
ExportCertificate	사설 인증 기관(CA)에서 발급한 사설 인증서를 어디서든 사용할 수 있도록 내보냅니다.	Read	certificate* (p. 745)		
GetCertificate	인증서 및 ARN으로 지정된 인증서에 대한 인증서 체인을 검색합니다.	Read	certificate* (p. 745)		
ImportCertificate	타사 SSL/TLS 인증서를 AWS Certificate Manager(ACM)로 가져옵니다.	쓰기	certificate* (p. 745)		
				aws:RequestTag/${TagKey} (p. 745) aws:TagKeys (p. 746)	
ListCertificates	인증서 ARN의 목록 및 각 ARN의 도메인 이름을 검색합니다.	List			
ListTagsForCertificate	인증서에 적용된 태그를 나열합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RemoveTagsFromCertificate	인증서에서 하나 이상의 태그를 제거합니다. 태그는 키-값 쌍으로 이루어져 있습니다	태그 지정	certificate* (p. 745)		
				aws:RequestTag/${TagKey} (p. 745) aws:TagKeys (p. 746)	
RenewCertificate	자격이 있는 사설 인증서를 갱신합니다.	쓰기	certificate* (p. 745)		
RequestCertificate	공인 또는 사설 인증서를 요청합니다.	쓰기		aws:RequestTag/${TagKey} (p. 745) aws:TagKeys (p. 746)	
ResendValidationEmail	도메인 소유권 확인을 요청하는 이메일을 재발송합니다.	쓰기	certificate* (p. 745)		
UpdateCertificateOptions	인증서를 업데이트합니다. 인증성 투명성 로깅 옵트인 또는 옵트아웃 여부를 지정하는 데 사용합니다.	쓰기	certificate* (p. 745)		

AWS Certificate Manager에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 744)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
certificate	`arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}`	aws:ResourceTag/${TagKey} (p. 746)

AWS Certificate Manager의 조건 키

AWS Certificate Manager는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Certificate Manager Private Certificate Authority에 사용되는 작업, 리소스 및 조건 키

AWS Certificate Manager Private Certificate Authority(서비스 접두사: `acm-pca`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Certificate Manager Private Certificate Authority에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCertificateAuthority	ACM 사설 CA와 연결된 프라이빗 키 및 구성을 생성합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 749) aws:TagKeys (p. 749)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCertificateAuthorityAuditReport	ACM 프라이빗 CA에 대한 감사 보고서를 생성합니다.	쓰기	certificate-authority* (p. 748)		
CreatePermission	ACM 사설 CA에 대한 권한을 생성합니다.	권한 관리	certificate-authority* (p. 748)		
DeleteCertificateAuthority	ACM 사설 CA와 연결된 프라이빗 키 및 구성을 삭제합니다.	쓰기	certificate-authority* (p. 748)		
DeletePermission	ACM 사설 CA에 대한 권한을 삭제합니다.	권한 관리	certificate-authority* (p. 748)		
DescribeCertificateAuthority	지정된 ACM 사설 CA에 포함된 구성 및 상태 필드의 목록을 반환합니다.	Read	certificate-authority* (p. 748)		
DescribeCertificateAuthorityAuditReport	ACM 사설 CA 감사 보고서에 대한 상태 및 정보를 반환합니다.	Read	certificate-authority* (p. 748)		
GetCertificate	ARN에 의해 지정된 인증 기관을 위한 ACM 사설 CA 인증서와 인증서 체인을 검색합니다.	Read	certificate-authority* (p. 748)		
GetCertificateAuthorityCertificate	ARN에 의해 지정된 인증 기관을 위한 ACM 사설 CA 인증서와 인증서 체인을 검색합니다.	Read	certificate-authority* (p. 748)		
GetCertificateAuthorityCsr	ARN에 의해 지정된 인증 기관을 위한 ACM 사설 CA 인증서 서명 요청(CSR)을 검색합니다.	Read	certificate-authority* (p. 748)		
ImportCertificateAuthorityCertificate	ACM 사설 CA의 CA 인증서로 사용하기 위해 SSL/TLS 인증서를 ACM 사설 CA로 가져옵니다.	쓰기	certificate-authority* (p. 748)		
IssueCertificate	ACM 사설 CA 인증서를 발급합니다.	쓰기	certificate-authority* (p. 748)		
				acm-pca:TemplateArn (p. 749)	
ListCertificateAuthorities	ACM 사설 CA 인증 기관 ARN의 목록 및 호출 계정의 각 CA 상태에 대한 요약을 가져옵니다.	List			
ListPermissions	ACM 사설 CA 인증 기관에 적용된 권한을 나열합니다.	Read	certificate-authority* (p. 748)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTags	ACM 사설 CA 인증 기관에 적용된 태그를 나열합니다.	Read	certificate-authority* (p. 748)		
RestoreCertificateAuthority	ACM 사설 CA를 삭제됨 상태에서 삭제 당시의 상태로 복원합니다.	쓰기	certificate-authority* (p. 748)		
RevokeCertificate	ACM 사설 CA에 의해 발급된 인증서를 취소합니다.	쓰기	certificate-authority* (p. 748)		
TagCertificateAuthority	ACM 사설 CA에 하나 이상의 태그를 추가합니다.	태그 지정	certificate-authority* (p. 748)		
				aws:TagKeys (p. 749) aws:RequestTag/${TagKey} (p. 749)	
UntagCertificateAuthority	ACM 사설 CA에서 하나 이상의 태그를 제거합니다.	태그 지정	certificate-authority* (p. 748)		
				aws:TagKeys (p. 749)	
UpdateCertificateAuthority	ACM 사설 CA의 구성을 업데이트합니다.	쓰기	certificate-authority* (p. 748)		

AWS Certificate Manager Private Certificate Authority에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 746)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
certificate-authority	`arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}`	aws:ResourceTag/${TagKey} (p. 749)

AWS Certificate Manager Private Certificate Authority에 사용되는 조건 키

AWS Certificate Manager Private Certificate Authority는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음의 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
acm-pca:TemplateArn	요청에 TemplateArn이 있는지 여부를 기준으로 인증서 발급 요청을 필터링합니다.	문자열
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열

AWS Chatbot에 사용되는 작업, 리소스 및 조건 키

AWS Chatbot(서비스 접두사: `chatbot`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

주제

- AWS Chatbot에서 정의한 작업 (p. 749)
- AWS Chatbot에서 정의한 리소스 유형 (p. 750)
- AWS Chatbot의 조건 키 (p. 750)

AWS Chatbot에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateChimeWebhookConfiguration	AWS Chatbot Chime 웹후크 구성을 생성합니다	쓰기			
CreateSlackChannelConfiguration	AWS Chatbot Slack 채널 구성을 생성합니다	쓰기			
DeleteChimeWebhookConfiguration	AWS Chatbot Chime 웹후크 구성을 삭제합니다	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteSlackChannelConfiguration	AWS Chatbot Slack 채널 구성을 삭제합니다.	쓰기			
DescribeChimeWebhookConfigurations	AWS 계정에서 모든 AWS Chatbot Chime 웹후크 구성을 나열합니다.	Read			
DescribeSlackChannelConfigurations	AWS 계정에서 모든 AWS Chatbot Slack 채널 구성을 나열합니다.	Read			
DescribeSlackChannels	AWS Chatbot 서비스로 등록된 AWS 계정에 연결되어 있는 Slack 작업 영역에서 퍼블릭 Slack 채널을 모두 나열합니다.	Read			
DescribeSlackWorkspaces	AWS Chatbot 서비스로 등록된 AWS 계정에 연결되어 권한이 부여된 Slack 작업 영역을 모두 나열합니다.	Read			
GetSlackOauthParameters	AWS Chatbot 서비스에서 Slack OAuth 코드를 사용하도록 요청하는 OAuth 파라미터를 생성합니다.	Read			
RedeemSlackOauthCode	AWS Chatbot 서비스에서 사용할 OAuth 토큰을 얻기 위해 Slack API를 사용해 이전에 생성된 파라미터를 다시 찾습니다.	쓰기			
UpdateChimeWebhookConfiguration	AWS Chatbot Chime 웹후크 구성을 업데이트합니다.	쓰기			
UpdateSlackChannelConfiguration	AWS Chatbot Slack 채널 구성을 업데이트합니다.	쓰기			

AWS Chatbot에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 749)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
ChatbotConfiguration	`arn:${Partition}:chatbot::${account}:${resourceType}/${resourceName}`	

AWS Chatbot의 조건 키

Chatbot에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Chime에 사용되는 작업, 리소스 및 조건 키

Amazon Chime(서비스 접두사: `chime`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Chime에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptDelegate	AWS 계정 관리를 다른 Amazon Chime 계정과 공유하기 위한 위임 초대를 수락할 수 있는 권한을 부여합니다.	쓰기			
ActivateUsers	Amazon Chime 엔터프라이즈 계정에서 사용자를 활성화할 수 있는 권한을 부여합니다.	쓰기			
AddDomain	Amazon Chime 계정에 도메인을 추가할 수 있는 권한을 부여합니다.	쓰기			
AddOrUpdateGroups	Amazon Chime 엔터프라이즈 계정과 연결된 Active Directory 또는 Okta 사용자 그룹을 새로 추가하거나 업데이트할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociatePhoneNumberWithUser	전화 번호를 Amazon Chime 사용자와 연결할 수 있는 권한을 부여합니다.	쓰기			
AssociatePhoneNumbersWithVoiceConnector	여러 전화 번호를 Amazon Chime Voice Connector와 연결할 수 있는 권한을 부여합니다.	쓰기			
AssociatePhoneNumbersWithVoiceConnectorGroup	여러 전화 번호를 Amazon Chime Voice Connector 그룹과 연결할 수 있는 권한을 부여합니다.	쓰기			
AssociateSigninDelegateGroupsWithAccount	지정된 로그인 위임 그룹을 지정된 Amazon Chime 계정과 연결할 수 있는 권한을 부여합니다.	쓰기			
AuthorizeDirectory	Amazon Chime 엔터프라이즈 계정에 대해 Active Directory를 승인할 수 있는 권한을 부여합니다.	쓰기			
BatchCreateAttendee	활성 Amazon Chime SDK 회의를 위해 새 참석자를 생성할 수 있는 권한을 부여합니다.	쓰기			
BatchCreateRoomMembership	회의실 구성원을 일괄 추가할 수 있는 권한을 부여합니다.	쓰기			
BatchDeletePhoneNumber	최대 50개의 전화 번호를 삭제 대기열로 이동할 수 있는 권한을 부여합니다.	쓰기			
BatchSuspendUser	팀 또는 엔터프라이즈 LWA Amazon Chime 계정에서 최대 50명의 사용자를 정지할 수 있는 권한을 부여합니다.	쓰기			
BatchUnsuspendUser	지정된 Amazon Chime 엔터프라이즈 LWA 계정에서 이전에 정지된 최대 50명의 사용자로부터 정지를 제거할 수 있는 권한을 부여합니다.	쓰기			
BatchUpdatePhoneNumber	최대 50개의 전화 번호에 대한 UpdatePhoneNumberRequestItem 객체 내에서 전화 번호 세부 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
BatchUpdateUser	지정된 Amazon Chime 계정에서 최대 20명의 사용자에 대해 UpdateUserRequestItem 객체 내에서 사용자 세부 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ConnectDirectory	Amazon Chime 엔터프라이즈 계정에 Active Directory를 연결할 수 있는 권한을 부여합니다.	쓰기			ds:ConnectDirectory
CreateAccount	관리자의 AWS 계정 아래에 Amazon Chime 계정을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateApiKey	Amazon Chime 계정 및 Okta 구성에 대한 새 SCIM 액세스 키를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateAttendee	활성 Amazon Chime SDK 회의를 위해 새 참석자를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateBot	Amazon Chime 엔터프라이즈 계정에 대한 봇을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateBotMembership	Amazon Chime 엔터프라이즈 계정의 채팅룸에 봇을 추가할 수 있는 권한을 부여합니다.	쓰기			
CreateCDRBucket	새 Call Detail Record S3 버킷을 생성할 수 있는 권한을 부여합니다.	쓰기			s3:CreateBucket s3:ListAllMyBuckets
CreateMeeting	초기 참석자 없이 지정된 미디어 리전에서 새 Amazon Chime SDK 회의를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreatePhoneNumberOrder	통신 사업자에 전화 번호 주문을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateProxySession	지정된 Amazon Chime Voice Connector에 대한 프록시 세션을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateRoom	회의실을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateRoomMembership	회의실 구성원을 추가할 수 있는 권한을 부여합니다.	쓰기			
CreateUser	지정된 Amazon Chime 계정으로 사용자를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateVoiceConnector	관리자의 AWS 계정으로 Amazon Chime Voice Connector를 생성할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateVoiceConnectorGroup	관리자의 AWS 계정으로 Amazon Chime Voice Connector 그룹을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteAccount	지정된 Amazon Chime 계정을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteAccountOpenIdConfig	Amazon Chime 계정에서 OpenIdConfig 속성을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteApiKey	Amazon Chime 계정 및 Okta 구성과 연결되어 있는 지정된 SCIM 액세스 키를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteAttendee	Amazon Chime SDK 회의에서 지정된 참석자를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteCDRBucket	Amazon Chime 계정에서 Call Detail Record S3 버킷을 삭제할 수 있는 권한을 부여합니다.	쓰기			s3:DeleteBucket
DeleteDelegate	Amazon Chime 계정에서 위임된 AWS 계정 관리를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteDomain	Amazon Chime 계정에서 도메인을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteEventsConfiguration	봇이 발신 이벤트를 수신하는 이벤트 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteGroups	Amazon Chime 엔터프라이즈 계정에서 Active Directory 또는 Okta 사용자 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteMeeting	지정된 Amazon Chime SDK 회의를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeletePhoneNumber	한 전화 번호를 삭제 대기열로 이동할 수 있는 권한을 부여합니다.	쓰기			
DeleteProxySession	지정된 Amazon Chime Voice Connector에 대한 프록시 세션을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteRoom	회의실을 삭제할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteRoomMembership	회의실 구성원을 제거할 수 있는 권한을 부여합니다.	쓰기			
DeleteVoiceConnector	지정된 Amazon Chime Voice Connector를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVoiceConnectorGroup	지정된 Amazon Chime Voice Connector 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVoiceConnectorOrigination	지정된 Amazon Chime Voice Connector에 대한 발생 설정을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVoiceConnectorProxy	지정된 Amazon Chime Voice Connector에 대한 프록시 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVoiceConnectorStreamingConfiguration	지정된 Amazon Chime Voice Connector에 대한 스트리밍 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVoiceConnectorTermination	지정된 Amazon Chime Voice Connector에 대한 종료 설정을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVoiceConnectorTerminationCredentials	지정된 Amazon Chime Voice Connector에 대한 SIP 종료 자격 증명을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DisassociatePhoneNumberFromUser	지정된 Amazon Chime 사용자로부터 기본 프로비저닝된 번호를 연결 해제할 수 있는 권한을 부여합니다.	쓰기			
DisassociatePhoneNumbersFromVoiceConnector	지정된 Amazon Chime Voice Connector에서 여러 전화 번호를 연결 해제할 수 있는 권한을 부여합니다.	쓰기			
DisassociatePhoneNumbersFromVoiceConnectorGroup	지정된 Amazon Chime Voice Connector 그룹에서 여러 전화 번호를 연결 해제할 수 있는 권한을 부여합니다.	쓰기			
DisassociateSigninDelegateGroupsFromAccount	지정된 Amazon Chime 계정에서 지정된 로그인 위임 그룹의 연결을 해제할 권한을 부여합니다.	쓰기			
DisconnectDirectory	Amazon Chime 엔터프라이즈 계정에서 Active Directory를 연결 해제할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetAccount	지정된 Amazon Chime 계정의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetAccountResource	Amazon Chime 계정과 연결된 계정 리소스의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetAccountSettings	지정된 Amazon Chime 계정 ID에 대한 계정 설정을 가져올 수 있는 권한을 부여합니다.	Read			
GetAccountWithOpenIdConfig	Amazon Chime 계정에 대한 계정 세부 정보 및 OpenIdConfig 속성을 가져올 수 있는 권한을 부여합니다.	Read			
GetAttendee	지정된 회의 ID 및 참석자 ID에 대한 참석자 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetBot	지정된 봇의 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read			
GetCDRBucket	Amazon Chime 계정과 연결된 Call Detail Record S3 버킷의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			s3:GetBucketAcl s3:GetBucketLocation s3:GetBucketLogging s3:GetBucketVersioning s3:GetBucketWebsite
GetDomain	Amazon Chime 계정과 연결된 도메인에 대한 도메인 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetEventsConfiguration	봇이 발신 이벤트를 수신하는 이벤트 구성의 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read			
GetGlobalSettings	AWS 계정의 Amazon Chime과 관련된 전역적 설정을 가져올 수 있는 권한을 부여합니다.	Read			
GetMeeting	지정된 회의 ID에 대한 회의 레코드를 가져올 수 있는 권한을 부여합니다.	Read			
GetMeetingDetail	참석자, 연결 및 기타 회의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetPhoneNumber	지정된 전화 번호의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetPhoneNumberOrder	지정된 전화 번호 주문의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetPhoneNumberSettings	AWS 계정의 Amazon Chime과 관련된 전화 번호 설정을 가져올 수 있는 권한을 부여합니다.	Read			
GetProxySession	지정된 Amazon Chime Voice Connector에 대한 지정된 프록시 세션의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetRoom	회의실을 검색할 수 있는 권한을 부여합니다.	Read			
GetTelephonyLimits	AWS 계정에 대한 텔레포니 제한을 가져올 수 있는 권한을 부여합니다.	Read			
GetUser	지정된 사용자 ID의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetUserActivityReportData	사용자 세부 정보 페이지에 사용자 활동 요약을 가져올 수 있는 권한을 부여합니다.	Read			
GetUserByEmail	Amazon Chime 엔터프라이즈 또는 팀 계정의 이메일 주소를 기반으로 Amazon Chime 사용자에 대한 사용자 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetUserSettings	지정된 Amazon Chime 사용자와 관련된 사용자 설정을 가올 수 있는 권한을 부여합니다.	Read			
GetVoiceConnector	지정된 Amazon Chime Voice Connector의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetVoiceConnectorGroup	지정된 Amazon Chime Voice Connector 그룹에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetVoiceConnectorLoggingConfiguration	지정된 Amazon Chime Voice Connector에 대한 로깅 구성의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetVoiceConnectorOrigination	지정된 Amazon Chime Voice Connector에 대한 발생 설정의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetVoiceConnectorProxy	지정된 Amazon Chime Voice Connector에 대한 프록시 구성의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetVoiceConnectorStreamingConfiguration	지정된 Amazon Chime Voice Connector에 대한 스트리밍 구성의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetVoiceConnectorTermination	지정된 Amazon Chime Voice Connector에 대한 종료 설정의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetVoiceConnectorTerminationHealth	지정된 Amazon Chime Voice Connector에 대한 종료 상태의 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
InviteDelegate	Amazon Chime 계정에 대한 AWS 계정 위임 요청을 수락하는 초대를 전송할 수 있는 권한을 부여합니다.	쓰기			
InviteUsers	지정된 Amazon Chime 계정으로 최대 50명의 사용자를 초대할 수 있는 권한을 부여합니다.	쓰기			
InviteUsersFromProvider	제3의 공급자의 사용자를 Amazon Chime 계정으로 초대할 수 있는 권한을 부여합니다.	쓰기			
ListAccountUsageReportData	Amazon Chime 계정 사용 보고 데이터를 나열할 수 있는 권한을 부여합니다.	List			
ListAccounts	관리자의 AWS 계정에 속하는 Amazon Chime 계정을 나열할 수 있는 권한을 부여합니다.	List			
ListApiKeys	Amazon Chime 계정 및 Okta 구성에 대해 정의된 SCIM 액세스 키를 나열할 수 있는 권한을 부여합니다.	List			
ListAttendeeTags	Amazon Chime SDK 참석자 리소스에 적용된 태그를 나열할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListAttendees	지정된 Amazon Chime SDK 회의에 대해 최대 100명의 참석자를 나열할 수 있는 권한을 부여합니다.	Read			
ListBots	관리자의 Amazon Chime 엔터프라이즈 계정과 연결된 봇을 나열할 수 있는 권한을 부여합니다.	List			
ListCDRBucket	Call Detail Record S3 버킷을 나열할 수 있는 권한을 부여합니다.	List			s3:ListAllMyBuckets s3:ListBucket
ListCallingRegions	관리자의 AWS 계정에 사용 가능한 호출 리전을 나열할 수 있는 권한을 부여합니다.	List			
ListDelegates	Amazon Chime 계정과 연결된 계정 위임 정보를 나열할 수 있는 권한을 부여합니다.	List			
ListDirectories	AWS 계정의 Directory Service에 호스팅된 활성 Active Directory를 나열할 수 있는 권한을 부여합니다.	List			
ListDomains	Amazon Chime 계정과 연결된 도메인을 나열할 수 있는 권한을 부여합니다.	List			
ListGroups	Amazon Chime 엔터프라이즈 계정과 연결된 Active Directory 또는 Okta 사용자 그룹을 나열할 수 있는 권한을 부여합니다.	List			
ListMeetingEvents	지정된 회의에서 발생한 모든 이벤트를 나열할 수 있는 권한을 부여합니다.	List			
ListMeetingTags	Amazon Chime SDK 모임 리소스에 적용된 태그를 나열할 수 있는 권한을 부여합니다.	Read			
ListMeetings	활성 Amazon Chime SDK 회의를 최대 100개까지 나열할 수 있는 권한을 부여합니다.	Read			
ListMeetingsReportData	지정된 날짜 범위 중에 종료된 회의를 나열할 수 있는 권한을 부여합니다.	List			
ListPhoneNumberOrders	관리자의 AWS 계정 아래의 전화번호 주문을 나열할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListPhoneNumbers	관리자의 AWS 계정 아래의 전화번호를 나열할 수 있는 권한을 부여합니다.	List			
ListProxySessions	지정된 Amazon Chime Voice Connector에 대한 프록시 세션을 나열할 수 있는 권한을 부여합니다.	List			
ListRoomMemberships	모든 회의실 구성원을 나열할 수 있는 권한을 부여합니다.	Read			
ListRooms	회의실을 나열할 수 있는 권한을 부여합니다.	Read			
ListTagsForResource	Amazon Chime SDK 모임 리소스에 적용된 태그를 나열할 수 있는 권한을 부여합니다.	Read			
ListUsers	지정된 Amazon Chime 계정에 속한 사용자를 나열할 수 있는 권한을 부여합니다.	List			
ListVoiceConnectorGroups	관리자의 AWS 계정으로 Amazon Chime Voice Connector 그룹을 나열할 수 있는 권한을 부여합니다.	List			
ListVoiceConnectorTerminationCredentials	지정된 Amazon Chime Voice Connector에 대한 SIP 종료 자격 증명을 나열할 수 있는 권한을 부여합니다.	List			
ListVoiceConnectors	관리자의 AWS 계정으로 Amazon Chime Voice Connector를 나열할 수 있는 권한을 부여합니다.	List			
LogoutUser	지정된 사용자를 현재 로그인된 모든 디바이스에서 로그아웃할 수 있는 권한을 부여합니다.	쓰기			
PutEventsConfiguration	봇이 발신 이벤트를 수신하는 이벤트 구성의 세부 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
PutVoiceConnectorLoggingConfiguration	지정된 Amazon Chime Voice Connector에 대한 로깅 구성을 추가할 수 있는 권한을 부여합니다.	쓰기			logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:GetLogDelivery logs:ListLogDeliveries

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutVoiceConnectorOrigination	지정된 Amazon Chime Voice Connector에 대한 발생 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
PutVoiceConnectorProxy	지정된 Amazon Chime Voice Connector에 대한 프록시 구성을 추가할 수 있는 권한을 부여합니다.	쓰기			
PutVoiceConnectorStreamingConfiguration	지정된 Amazon Chime Voice Connector에 대한 스트리밍 구성을 추가할 수 있는 권한을 부여합니다.	쓰기			
PutVoiceConnectorTermination	지정된 Amazon Chime Voice Connector에 대한 종료 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
PutVoiceConnectorTerminationCredentials	지정된 Amazon Chime Voice Connector에 대한 SIP 종료 자격 증명을 추가할 수 있는 권한을 부여합니다.	쓰기			
RegenerateSecurityToken	지정된 봇에 대한 보안 토큰을 재생성할 수 있는 권한을 부여합니다.	쓰기			
RenameAccount	Amazon Chime 엔터프라이즈 또는 팀 계정의 계정 이름을 수정할 수 있는 권한을 부여합니다.	쓰기			
RenewDelegate	Amazon Chime 계정과 연결된 위임 요청을 갱신할 수 있는 권한을 부여합니다.	쓰기			
ResetAccountResource	Amazon Chime 계정에서 계정 리소스를 재설정할 수 있는 권한을 부여합니다.	쓰기			
ResetPersonalPIN	Amazon Chime 계정에서 지정된 사용자의 개인 회의 PIN을 재설정할 수 있는 권한을 부여합니다.	쓰기			
RestorePhoneNumber	지정된 전화 번호를 삭제 대기열에서 다시 전화 번호 인벤토리로 복원할 수 있는 권한을 부여합니다.	쓰기			
RetrieveDataExports	"첨부 파일 요청" 작업의 일부로 반환된 모든 사용자 첨부 파일에 대한 링크가 포함된 파일을 다운로드할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SearchAvailablePhoneNumbers	통신 사업자에게 주문할 수 있는 전화 번호를 검색할 수 있는 권한을 부여합니다.	Read			
StartDataExport	"첨부 파일 요청" 요청을 제출할 수 있는 권한을 부여합니다.	쓰기			
SubmitSupportRequest	고객 서비스 지원 요청을 제출할 수 있는 권한을 부여합니다.	쓰기			
SuspendUsers	Amazon Chime 엔터프라이즈 계정에서 사용자를 정지할 수 있는 권한을 부여합니다.	쓰기			
TagAttendee	지정된 Amazon Chime SDK 참석자에게 지정된 태그를 적용할 수 있는 권한을 부여합니다.	태그 지정			
TagMeeting	지정된 Amazon Chime SDK 모임에 지정된 태그를 적용할 권한을 부여합니다.	태그 지정			
TagResource	지정된 Amazon Chime SDK 모임 리소스에 지정된 태그를 적용할 권한을 부여합니다.	태그 지정			
UnauthorizeDirectory	Amazon Chime 엔터프라이즈 계정에서 Active Directory를 승인 취소할 수 있는 권한을 부여합니다.	쓰기			
UntagAttendee	지정된 Amazon Chime SDK 참석자로부터 지정된 태그를 해제할 수 있는 권한을 부여합니다.	태그 지정			
UntagMeeting	지정된 Amazon Chime SDK 모임에서 지정된 태그를 해제할 권한을 부여합니다.	태그 지정			
UntagResource	지정된 Amazon Chime SDK 모임 리소스에서 지정된 태그를 해제할 권한을 부여합니다.	태그 지정			
UpdateAccount	지정된 Amazon Chime 계정의 계정 세부 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateAccountOpenIdConfig	Amazon Chime 계정에서 OpenIdConfig 속성을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateAccountResource	Amazon Chime 계정에서 계정 리소스를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateAccountSettings	지정된 Amazon Chime 계정에 대한 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateBot	지정된 봇의 상태를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateCDRSettings	Call Detail Record S3 버킷을 업데이트할 수 있는 권한을 부여합니다.	쓰기			s3:CreateBucket s3:DeleteBucket s3:ListAllMyBuckets
UpdateGlobalSettings	AWS 계정의 Amazon Chime과 관련된 전역적 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdatePhoneNumber	지정된 전화 번호에 대한 전화 번호 세부 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdatePhoneNumberSettings	AWS 계정의 Amazon Chime과 관련된 전화 번호 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateProxySession	지정된 Amazon Chime Voice Connector에 대한 프록시 세션을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateRoom	회의실을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateRoomMembership	회의실 멤버십 역할을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateSupportedLicenses	Amazon Chime 계정의 사용자가 사용할 수 있는 지원되는 라이선스 티어를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateUser	지정된 사용자 ID의 사용자 세부 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateUserLicenses	Amazon Chime 사용자의 라이선스를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateUserSettings	지정된 Amazon Chime 사용자와 관련된 사용자 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateVoiceConnector	지정된 Amazon Chime Voice Connector에 대한 Amazon Chime Voice Connector 세부 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateVoiceConnectorGroup	지정된 Amazon Chime Voice Connector 그룹에 대한 Amazon Chime Voice Connector 그룹 세부 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
ValidateAccountResource	Amazon Chime 계정에서 계정 리소스를 검증할 수 있는 권한을 부여합니다.	Read			

Amazon Chime에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 751)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
meeting	`arn:${Partition}:chime::${AccountId}:meeting/${MeetingId}`	

Amazon Chime의 조건 키

Chime에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Cloud Directory에 사용되는 작업, 리소스 및 조건 키

Amazon Cloud Directory(서비스 접두사: `clouddirectory`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Cloud Directory에서 정의한 작업 (p. 764)
- Amazon Cloud Directory에서 정의한 리소스 유형 (p. 769)
- Amazon Cloud Directory의 조건 키 (p. 770)

Amazon Cloud Directory에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddFacetToObject	새 패싯을 객체에 추가합니다.	쓰기	directory* (p. 770)		
ApplySchema	입력이 게시된 스키마를 게시된 스키마의 디렉터리와 동일한 이름 및 버전의 디렉터리에 복사합니다.	쓰기	directory* (p. 770)		
			publishedSchema* (p. 770)		
AttachObject	기존 객체를 다른 기존 객체에 연결합니다.	쓰기	directory* (p. 770)		
AttachPolicy	정책 객체를 다른 객체에 연결합니다.	쓰기	directory* (p. 770)		
AttachToIndex	지정된 객체를 지정된 인덱스에 연결합니다.	쓰기	directory* (p. 770)		
AttachTypedLink	소스 및 대상 객체 참조 간에 형식 링크를 연결합니다.	쓰기	directory* (p. 770)		
BatchRead	모든 읽기 작업을 일괄적으로 수행합니다. BatchRead 내의 개별 작업마다 명시적으로 권한을 부여해야 합니다.	Read	directory* (p. 770)		
BatchWrite	모든 쓰기 작업을 일괄적으로 수행합니다. BatchWrite 내의 개별 작업마다 명시적으로 권한을 부여해야 합니다.	쓰기	directory* (p. 770)		
CreateDirectory	게시된 스키마를 디렉터리에 복사하여 디렉터리를 생성합니다.	쓰기	publishedSchema* (p. 770)		
CreateFacet	스키마에 새 패싯을 생성합니다.	쓰기	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
CreateIndex	인덱스 객체를 생성합니다.	쓰기	directory* (p. 770)		
CreateObject	디렉터리에 객체를 생성합니다.	쓰기	directory* (p. 770)		
CreateSchema	새 스키마를 개발 상태로 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateTypedLinkFacet	스키마에 새 형식 링크 패싯을 생성합니다.	쓰기	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
DeleteDirectory	디렉터리를 삭제합니다. 비활성화된 디렉터리만 삭제할 수 있습니다.	쓰기	directory* (p. 770)		
DeleteFacet	지정된 패싯을 삭제합니다. 패싯과 연결된 모든 속성 및 규칙이 삭제됩니다.	쓰기	developmentSchema* (p. 770)		
DeleteObject	객체 및 연결된 속성을 삭제합니다.	쓰기	directory* (p. 770)		
DeleteSchema	지정된 스키마를 삭제합니다.	쓰기	developmentSchema* (p. 770)		
			publishedSchema* (p. 770)		
DeleteTypedLinkFacet	지정된 TypedLink 패싯을 삭제합니다. 패싯과 연결된 모든 속성 및 규칙이 삭제됩니다.	쓰기	developmentSchema* (p. 770)		
DetachFromIndex	지정된 인덱스에서 지정된 객체를 분리합니다.	쓰기	directory* (p. 770)		
DetachObject	상위 객체에서 지정된 객체를 분리합니다.	쓰기	directory* (p. 770)		
DetachPolicy	객체에서 정책을 분리합니다.	쓰기	directory* (p. 770)		
DetachTypedLink	지정된 소스 및 대상 객체 참조 간의 지정된 형식 링크를 분리합니다.	쓰기	directory* (p. 770)		
DisableDirectory	지정된 디렉터리를 비활성화합니다.	쓰기	directory* (p. 770)		
EnableDirectory	지정된 디렉터리를 활성화합니다.	쓰기	directory* (p. 770)		
GetDirectory	디렉터리에 대한 메타데이터를 검색합니다.	Read	directory* (p. 770)		
GetFacet	패싯 이름, 속성, 규칙 또는 ObjectType과 같은 패싯의 세부 정보를 가져옵니다.	Read	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
			publishedSchema* (p. 770)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetLinkAttributes	형식 링크와 연결된 속성을 검색합니다.	Read	directory* (p. 770)		
GetObjectAttributes	객체와 연결된 패싯 내의 속성을 검색합니다.	Read	directory* (p. 770)		
GetObjectInformation	객체에 대한 메타데이터를 검색합니다.	Read	directory* (p. 770)		
GetSchemaAsJson	스키마의 JSON 표현을 검색합니다.	Read	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
			publishedSchema* (p. 770)		
GetTypedLinkFacetInformation	지정된 형식 링크 패싯과 연결된 자격 증명 속성 주문 정보를 반환합니다.	Read	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
			publishedSchema* (p. 770)		
ListAppliedSchemaArns	디렉터리에 적용된 스키마를 나열합니다.	List	directory* (p. 770)		
ListAttachedIndices	객체에 연결된 인덱스를 나열합니다.	Read	directory* (p. 770)		
ListDevelopmentSchemaArns	개발 상태의 스키마 ARN을 검색합니다.	List			
ListDirectories	계정 내에 생성된 디렉터리를 나열합니다.	List			
ListFacetAttributes	패싯에 연결된 속성을 검색합니다.	Read	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
			publishedSchema* (p. 770)		
ListFacetNames	스키마에 있는 패싯의 이름을 검색합니다.	Read	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
			publishedSchema* (p. 770)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListIncomingTypedLinks	지정된 객체에 대한 모든 수신 TypedLinks의 페이지 매김 목록을 반환합니다.	Read	directory* (p. 770)		
ListIndex	지정된 인덱스에 연결된 객체를 나열합니다.	Read	directory* (p. 770)		
ListObjectAttributes	객체와 연결된 모든 속성을 나열합니다.	Read	directory* (p. 770)		
ListObjectChildren	지정된 객체와 연결된 하위 객체의 페이지 매김 목록을 반환합니다.	Read	directory* (p. 770)		
ListObjectParentPaths	노드, 리프 노드, 정책 노드, 인덱스 노드 객체 등의 모든 객체 유형에서 사용 가능한 모든 상위 경로를 검색합니다.	Read	directory* (p. 770)		
ListObjectParents	지정된 객체와 연결된 상위 객체를 페이지 매김 방식으로 나열합니다.	Read	directory* (p. 770)		
ListObjectPolicies	객체에 연결된 정책을 페이지 매김 방식으로 반환합니다.	Read	directory* (p. 770)		
ListOutgoingTypedLinks	지정된 객체에 대한 모든 발신 TypedLinks의 페이지 매김 목록을 반환합니다.	Read	directory* (p. 770)		
ListPolicyAttachments	지정된 정책이 연결된 모든 ObjectIdentifier를 반환합니다.	Read	directory* (p. 770)		
ListPublishedSchemaArns	게시된 스키마 ARN을 검색합니다.	List			
ListTagsForResource	리소스에 대한 태그를 반환합니다.	Read	directory* (p. 770)		
ListTypedLinkFacetAttributes	형식 링크 패싯과 연결된 속성의 페이지 매김 목록을 반환합니다.	Read	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
			publishedSchema* (p. 770)		
ListTypedLinkFacetNames	스키마에 있는 형식 링크 패싯 이름의 페이지 매김 목록을 반환합니다.	Read	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
			publishedSchema* (p. 770)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
LookupPolicy	디렉터리의 루트에서 지정된 객체에 대한 모든 정책을 나열합니다.	Read	directory* (p. 770)		
PublishSchema	버전이 있는 개발 스키마를 게시합니다.	쓰기	developmentSchema* (p. 770)		
PutSchemaFromJson	JSON 업로드를 사용하여 스키마를 업데이트할 수 있습니다. 개발 스키마에서만 사용할 수 있습니다.	쓰기			
RemoveFacetFromObject	지정된 객체에서 지정된 패싯을 제거합니다.	쓰기	directory* (p. 770)		
TagResource	태그를 리소스에 추가합니다.	태그 지정	directory* (p. 770)		
UntagResource	리소스에서 태그를 제거합니다.	태그 지정	directory* (p. 770)		
UpdateFacet	패싯의 기존 속성, 규칙 또는 ObjectType을 추가/업데이트/삭제합니다.	쓰기	appliedSchema* (p. 769)		
			developmentSchema* (p. 770)		
UpdateLinkAttributes	지정된 형식 링크의 속성을 업데이트합니다. 업데이트할 속성은 IdentityAttributeOrder로 정의되는 형식 링크 자격 증명에 기여하지 않아야 합니다.	쓰기	directory* (p. 770)		
UpdateObjectAttributes	지정된 객체의 속성을 업데이트합니다.	쓰기	directory* (p. 770)		
UpdateSchema	스미카 이름을 새 이름으로 업데이트합니다.	쓰기	developmentSchema* (p. 770)		
UpdateTypedLinkFacet	TypedLink 패싯의 기존 속성, 규칙, 자격 증명 속성 주문을 추가/업데이트/삭제합니다.	쓰기	developmentSchema* (p. 770)		

Amazon Cloud Directory에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 764)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
appliedSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}/schema/${SchemaName}/${Version}`	

리소스 유형	ARN	조건 키
developmentSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/development/${SchemaName}`	
directory	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}`	
publishedSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/published/${SchemaName}/${Version}`	

Amazon Cloud Directory의 조건 키

Cloud Directory에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Cloud Map에 사용되는 작업, 리소스 및 조건 키

AWS Cloud Map(서비스 접두사: `servicediscovery`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Cloud Map에 정의된 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateHttpNamespace	HTTP 네임스페이스를 생성합니다.	쓰기			
CreatePrivateDnsNamespace	지정된 Amazon VPC 내에서만 볼 수 있는 DNS에 기반한 프라이빗 네임스페이스를 만듭니다.	쓰기			
CreatePublicDnsNamespace	인터넷에서 볼 수 있는 DNS에 기반한 퍼블릭 네임스페이스를 만듭니다.	쓰기			
CreateService	서비스를 생성합니다.	쓰기		servicediscovery:NamespaceArn (p. 772)	
DeleteNamespace	지정된 네임스페이스를 삭제합니다.	쓰기	namespace* (p. 772)		
DeleteService	지정된 서비스를 삭제합니다.	쓰기	service* (p. 772)		
DeregisterInstance	Amazon Route 53이 지정된 인스턴스에 대해 생성한 레코드 및 상태 확인(있는 경우)을 삭제합니다.	쓰기		servicediscovery:ServiceArn (p. 772)	
DiscoverInstances	지정된 네임스페이스 및 서비스에 대해 등록된 인스턴스를 검색합니다.	Read		servicediscovery:NamespaceName (p. 772) servicediscovery:ServiceName (p. 772)	
GetInstance	지정된 인스턴스에 대한 정보를 가져옵니다.	Read		servicediscovery:ServiceArn (p. 772)	
GetInstancesHealthStatus	하나 이상의 인스턴스에 대한 현재 상태(정상, 비정상 또는 알 수 없음)를 가져옵니다.	Read		servicediscovery:ServiceArn (p. 772)	
GetNamespace	네임스페이스에 대한 정보를 가져옵니다.	Read	namespace* (p. 772)		
GetOperation	지정된 인스턴스에 대한 정보를 가져옵니다.	Read			
GetService	지정된 서비스에 대한 설정을 가져옵니다.	Read	service* (p. 772)		
ListInstances	지정된 서비스에 등록된 인스턴스에 대한 요약 정보를 가져옵니다.	List		servicediscovery:ServiceArn (p. 772)	
ListNamespaces	네임스페이스에 대한 정보를 가져옵니다.	List			
ListOperations	지정한 기준과 일치하는 작업을 나열합니다.	List			
ListServices	지정된 필터와 일치하는 모든 서비스에 대한 설정을 가져옵니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RegisterInstance	지정된 서비스의 설정을 기준으로 인스턴스를 등록합니다.	쓰기		servicediscovery:ServiceArn (p. 772)	
UpdateInstanceCustomHealthStatus	사용자 지정 상태 확인이 있는 인스턴스의 현재 상태를 업데이트합니다.	쓰기		servicediscovery:ServiceArn (p. 772)	
UpdateService	지정된 서비스의 설정을 업데이트합니다.	쓰기	service* (p. 772)		

AWS Cloud Map에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 770)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
namespace	`arn:${Partition}:servicediscovery:${Region}:${Account}:namespace/${NamespaceId}`	
service	`arn:${Partition}:servicediscovery:${Region}:${Account}:service/${ServiceId}`	

AWS Cloud Map에 사용되는 조건 키

AWS Cloud Map은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
servicediscovery:NamespaceArn	관련 네임스페이스에 대해 Amazon 리소스 이름(ARN)을 지정하여 객체를 가져올 수 있는 필터입니다.	문자열
servicediscovery:NamespaceName	관련 네임스페이스의 이름을 지정하여 객체를 가져올 수 있는 필터입니다.	문자열
servicediscovery:ServiceArn	관련 서비스에 대해 Amazon 리소스 이름(ARN)을 지정하여 객체를 가져올 수 있는 필터입니다.	문자열
servicediscovery:ServiceName	관련 서비스의 이름을 지정하여 객체를 가져올 수 있는 필터입니다.	문자열

AWS Cloud9에 사용되는 작업, 리소스 및 조건 키

AWS Cloud9(서비스 접두사: `cloud9`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Cloud9에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateEnvironmentEC2	AWS Cloud9 개발 환경을 생성하고 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 시작한 다음 인스턴스에서 환경을 호스팅할 수 있는 권한을 부여합니다.	쓰기		cloud9:EnvironmentName (p. 776) cloud9:InstanceType (p. 776) cloud9:SubnetId (p. 776) cloud9:UserArn (p. 776)	ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedI
CreateEnvironmentMembership	환경 멤버를 AWS Cloud9 개발 환경에 추가할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 775)		
				cloud9:UserArn (p. 776) cloud9:EnvironmentId (p. 775) cloud9:Permissions (p. 776)	
DeleteEnvironment	AWS Cloud9 개발 환경을 삭제할 수 있는 권한을 부여합니다. 환	쓰기	environment* (p. 775)		iam:CreateServiceLinkedI

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	경이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 호스팅된 경우 인스턴스도 종료합니다.				
DeleteEnvironmentMembership	AWS Cloud9 개발 환경에서 환경 멤버를 삭제할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 775)		
DescribeEnvironmentMemberships	AWS Cloud9 개발 환경의 환경 멤버에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	environment* (p. 775)		
				cloud9:UserArn (p. 776) cloud9:EnvironmentId (p. 775)	
DescribeEnvironmentStatus	AWS Cloud9 개발 환경에 대한 상태 정보를 가져올 수 있는 권한을 부여합니다.	Read	environment* (p. 775)		
DescribeEnvironments	AWS Cloud9 개발 환경에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	environment* (p. 775)		
GetUserSettings [권한만 해당]	AWS Cloud9 사용자의 IDE별 설정을 가져올 수 있는 권한을 부여합니다.	Read			
ListEnvironments	AWS Cloud9 개발 환경 식별자의 목록을 가져올 수 있는 권한을 부여합니다.	Read			
ListTagsForResource	cloud9 환경에 대한 태그 나열	Read	environment* (p. 775)		
TagResource	cloud9 환경에 태그 추가	쓰기	environment* (p. 775)		
				aws:RequestTag/${TagKey} (p. 775) aws:TagKeys (p. 775)	
UntagResource	cloud9 환경에서 태그 제거	쓰기	environment* (p. 775)		
				aws:TagKeys (p. 775)	
UpdateEnvironment	기존 AWS Cloud9 개발 환경의 설정을 변경할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 775)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateEnvironmentMembership	AWS Cloud9 개발 환경에 대한 기존 환경 멤버의 설정을 변경할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 775)		
				cloud9:UserArn (p. 776) cloud9:EnvironmentId (p. 775) cloud9:Permissions (p. 776)	
UpdateUserSettings [권한만 해당]	AWS Cloud9 사용자의 IDE별 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			

AWS Cloud9에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 773)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
environment	`arn:${Partition}:cloud9:${Region}:${Account}:environment:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 775)

AWS Cloud9의 조건 키

AWS Cloud9은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
cloud9:EnvironmentId	AWS Cloud9 환경 ID를 기준으로 액세스를 필터링합니다.	문자열

조건 키	설명	유형
cloud9:EnvironmentName	AWS Cloud9 환경 이름을 기준으로 액세스를 필터링합니다.	문자열
cloud9:InstanceType	AWS Cloud9 환경의 Amazon EC2 인스턴스를 기준으로 액세스를 필터링합니다.	문자열
cloud9:Permissions	AWS Cloud9 권한의 유형을 기준으로 액세스를 필터링합니다.	문자열
cloud9:SubnetId	AWS Cloud9 환경이 생성될 서브넷 ID를 기준으로 액세스를 필터링합니다.	문자열
cloud9:UserArn	지정된 사용자 ARN을 기준으로 액세스를 필터링합니다.	ARN

AWS CloudFormation에 사용되는 작업, 리소스 및 조건 키

AWS CloudFormation(서비스 접두사: `cloudformation`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CloudFormation에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelUpdateStack	지정된 스택에 대한 업데이트를 취소합니다.	쓰기	stack* (p. 782)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ContinueUpdateRollback	UPDATE_ROLLBACK_FAILED 상태에 있는 지정된 스택의 경우 UPDATE_ROLLBACK_COMPLETE 상태로 롤백을 계속합니다.	쓰기	stack* (p. 782)		
				cloudformation:RoleArn (p. 782)	
CreateChangeSet	스택에 대한 변경 사항 목록을 생성합니다.	쓰기	stack* (p. 782)		
				cloudformation:ChangeSetName (p. 782) cloudformation:ResourceTypes (p. 782) cloudformation:ImportResourceTypes (p. 782) cloudformation:RoleArn (p. 782) cloudformation:StackPolicyUrl (p. 782) cloudformation:TemplateUrl (p. 783) aws:RequestTag/${TagKey} (p. 782) aws:TagKeys (p. 782)	
CreateStack	템플릿에 지정된 대로 스택을 생성합니다.	쓰기	stack* (p. 782)		
				cloudformation:ResourceTypes (p. 782) cloudformation:RoleArn (p. 782) cloudformation:StackPolicyUrl (p. 782) cloudformation:TemplateUrl (p. 783) aws:RequestTag/${TagKey} (p. 782) aws:TagKeys (p. 782)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateStackInstances	지정된 리전 내에서 지정된 계정에 대한 스택 인스턴스를 생성합니다.	쓰기	stackset* (p. 782)		
CreateStackSet	템플릿에 지정된 대로 스택 세트를 생성합니다.	쓰기		cloudformation:RoleArn (p. 782) cloudformation:TemplateUrl (p. 783) aws:RequestTag/${TagKey} (p. 782) aws:TagKeys (p. 782)	
CreateUploadBucket [권한만 해당]		쓰기			
DeleteChangeSet	지정된 변경 세트를 삭제합니다. 변경 세트를 삭제하면 아무도 잘못된 변경 세트를 실행할 수 없습니다.	쓰기	stack* (p. 782)		
				cloudformation:ChangeSetName (p. 782)	
DeleteStack	지정된 스택을 삭제합니다.	쓰기	stack* (p. 782)		
				cloudformation:RoleArn (p. 782)	
DeleteStackInstances	지정된 리전에서 지정된 계정에 대한 스택 인스턴스를 삭제합니다.	쓰기	stackset* (p. 782)		
DeleteStackSet	지정된 스택 세트를 삭제합니다.	쓰기	stackset* (p. 782)		
DescribeAccountLimits	계정의 AWS CloudFormation 제한을 검색합니다.	Read			
DescribeChangeSet	지정된 변경 세트에 대한 설명을 반환합니다.	Read	stack* (p. 782)		
				cloudformation:ChangeSetName (p. 782)	
DescribeStackDriftDetectionStatus	스택 드리프트 감지 작업에 대한 정보를 반환합니다.	Read			
DescribeStackEvents	지정된 스택에 대한 모든 스택 관련 이벤트를 반환합니다.	Read	stack* (p. 782)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeStackInstance	지정된 스택 세트, AWS 계정 및 리전과 연결된 스택 인스턴스를 반환합니다.	Read	stackset* (p. 782)		
DescribeStackResource	지정된 스택에서 지정된 리소스의 설명을 반환합니다.	Read	stack* (p. 782)		
DescribeStackResourceDrifts	지정된 스택에서 드리프트 여부가 확인된 리소스에 대한 드리프트 정보를 반환합니다.	Read	stack* (p. 782)		
DescribeStackResources	실행 중인 스택과 삭제된 스택에 대한 AWS 리소스 설명을 반환합니다.	Read	stack* (p. 782)		
DescribeStackSet	지정된 스택 세트에 대한 설명을 반환합니다.	Read	stackset* (p. 782)		
DescribeStackSetOperation	지정된 스택 세트 작업에 대한 설명을 반환합니다.	Read	stackset* (p. 782)		
DescribeStacks	지정된 스택에 대한 설명을 반환합니다.	List	stack* (p. 782)		
DetectStackDrift	스택의 실제 구성이 스택 템플릿 내 정의 및 템플릿 파라미터로 지정된 값에 따라 예상된 구성과 다른지 또는 드리프트되었는지 여부를 감지합니다.	Read	stack* (p. 782)		
DetectStackResourceDrift	리소스의 실제 구성이 스택 템플릿 내 정의 및 템플릿 파라미터로 지정된 값에 따라 예상된 구성과 다른지 또는 드리프트되었는지 여부에 대한 정보를 반환합니다.	Read	stack* (p. 782)		
DetectStackSetDrift	사용자가 스택 세트와 해당 스택 세트에 속한 스택 인스턴스에서 드리프트를 감지할 수 있도록 합니다.	Read	stackset* (p. 782)		
EstimateTemplateCost	템플릿의 월별 추정 비용을 반환합니다.	Read			
ExecuteChangeSet	지정된 변경 세트가 생성되었을 때 제공된 입력 정보를 사용하여 스택을 업데이트합니다.	쓰기	stack* (p. 782)		
				cloudformation:ChangeSetName (p. 782)	
GetStackPolicy	지정된 스택에 대한 스택 정책을 반환합니다.	Read	stack* (p. 782)		
GetTemplate	지정된 스택에 대한 템플릿 본문을 반환합니다.	Read	stack* (p. 782)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetTemplateSummary	새 템플릿이나 기존 템플릿에 대한 정보를 반환합니다.	Read	stack (p. 782)		
			stackset (p. 782)		
ListChangeSets	스택에 대한 각 활성 변경 세트의 ID 및 상태를 반환합니다. 예를 들어 AWS CloudFormation은 CREATE_IN_PROGRESS 또는 CREATE_PENDING 상태에 있는 변경 세트를 나열합니다.	List	stack* (p. 782)		
ListExports	이 작업을 호출한 계정 및 리전의 모든 내보낸 출력 값을 나열합니다.	List			
ListImports	내보낸 출력 값을 가져오는 모든 스택을 나열합니다.	List			
ListStackInstances	지정된 스택 세트와 연결된 스택 인스턴스에 대한 요약 정보를 반환합니다.	List	stackset* (p. 782)		
ListStackResources	지정된 스택의 모든 리소스에 대한 설명을 반환합니다.	List	stack* (p. 782)		
ListStackSetOperationResults	스택 세트 작업의 결과에 대한 요약 정보를 반환합니다.	List	stackset* (p. 782)		
ListStackSetOperations	스택 세트에서 수행된 작업에 대한 요약 정보를 반환합니다.	List	stackset* (p. 782)		
ListStackSets	사용자와 연결된 스택 세트에 대한 요약 정보를 반환합니다.	List	stackset* (p. 782)		
ListStacks	상태가 지정된 StackStatusFilter와 일치하는 스택에 대한 요약 정보를 반환합니다.	List			
SetStackPolicy	지정된 스택에 대한 스택 정책을 설정합니다.	권한 관리	stack* (p. 782)		
				cloudformation:StackPolicyUrl (p. 782)	
SignalResource	지정된 리소스에 성공 또는 실패 상태로 신호를 보냅니다.	쓰기	stack* (p. 782)		
StopStackSetOperation	스택 세트 및 연결된 스택 인스턴스에서 진행 중인 작업을 중지합니다.	쓰기	stackset* (p. 782)		
TagResource	CloudFormation 리소스에 태그를 지정합니다.	태그 지정	stack (p. 782)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			stackset (p. 782)		
UntagResource	CloudFormation 리소스의 태그 지정을 해제합니다.	태그 지정	stack (p. 782)		
			stackset (p. 782)		
UpdateStack	템플릿에 지정된 대로 스택을 업데이트합니다.	쓰기	stack* (p. 782)		
				cloudformation:ResourceTypes (p. 782) cloudformation:RoleArn (p. 782) cloudformation:StackPolicyUrl (p. 782) cloudformation:TemplateUrl (p. 783) aws:RequestTag/${TagKey} (p. 782) aws:TagKeys (p. 782)	
UpdateStackInstances	지정된 리전 내에서 지정된 계정에 대한 스택 인스턴스의 파라미터 값을 업데이트합니다.	쓰기	stackset* (p. 782)		
UpdateStackSet	템플릿에 지정된 대로 스택 세트를 업데이트합니다.	쓰기	stackset* (p. 782)		
				cloudformation:RoleArn (p. 782) cloudformation:TemplateUrl (p. 783) aws:RequestTag/${TagKey} (p. 782) aws:TagKeys (p. 782)	
UpdateTerminationProtection	지정된 스택에 대한 종료 방지 기능을 업데이트합니다.	쓰기	stack* (p. 782)		
ValidateTemplate	지정된 템플릿을 확인합니다.	쓰기			

AWS CloudFormation에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 776)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
stack	`arn:${Partition}:cloudformation:${Region}:${Account}:stack/${StackName}/${Id}`	aws:ResourceTag/${TagKey} (p. 782)
stackset	`arn:${Partition}:cloudformation:${Region}:${Account}:stackset/${StackSetName}:${Id}`	aws:ResourceTag/${TagKey} (p. 782)
changeset	`arn:${Partition}:cloudformation:${Region}:${Account}:changeSet/${ChangeSetName}:${Id}`	

AWS CloudFormation의 조건 키

AWS CloudFormation은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}		문자열
aws:ResourceTag/${TagKey}		문자열
aws:TagKeys		문자열
cloudformation:ChangeSetName	AWS CloudFormation 변경 세트 이름입니다. IAM 사용자가 실행하거나 삭제할 수 있는 변경 세트를 제어하는 데 사용합니다.	문자열
cloudformation:ImportResourceTypes	템플릿 리소스 유형(예: <code>AWS::EC2::Instance</code>) 입니다. IAM 사용자가 리소스를 스택으로 가져올 때 작업할 수 있는 리소스 유형을 제어하는 데 사용합니다.	문자열
cloudformation:ResourceTypes	템플릿 리소스 유형(예: <code>AWS::EC2::Instance</code>) 입니다. IAM 사용자가 스택을 생성하거나 업데이트할 때 작업할 수 있는 리소스 유형을 제어하는 데 사용합니다.	문자열
cloudformation:RoleArn	IAM 서비스 역할의 ARN입니다. IAM 사용자가 스택 또는 변경 세트로 작업할 때 사용할 수 있는 서비스 역할을 제어하는 데 사용합니다.	ARN
cloudformation:StackPolicyUrl	Amazon S3 스택 정책 URL입니다. IAM 사용자가 스택 생성 또는 업데이트 작업 중에 스택과 연결할 수 있는 스택 정책을 제어하는 데 사용합니다.	문자열

조건 키	설명	유형
cloudformation:TemplateURL	Amazon S3 템플릿 URL입니다. IAM 사용자가 스택을 생성하거나 업데이트할 때 사용할 수 있는 템플릿을 제어하는 데 사용합니다.	문자열

Amazon CloudFront에 사용되는 작업, 리소스 및 조건 키

Amazon CloudFront(서비스 접두사: `cloudfront`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon CloudFront에서 정의한 작업 (p. 783)
- Amazon CloudFront에서 정의한 리소스 유형 (p. 788)
- Amazon CloudFront의 조건 키 (p. 788)

Amazon CloudFront에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCloudFrontOriginAccessIdentity	이 작업에서는 새 CloudFront 원본 액세스 ID를 생성합니다(POST /2019-03-26/origin-access-identity/cloudfront).	쓰기	origin-access-identity* (p. 788)		
CreateDistribution	이 작업에서는 새 웹 배포를 생성합니다(POST /2019-03-26/distribution).	쓰기	distribution* (p. 788)		
CreateDistributionWithTags	이 작업에서는 태그가 있는 새 웹 배포를 생성합니다(POST /2019-03-26/distribution?WithTags).	태그 지정	distribution* (p. 788)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 789) aws:TagKeys (p. 789)	
CreateFieldLevelEncryptionConfig	이 작업은 새로운 필드 레벨 암호화 구성을 생성합니다. (POST /2019-03-26/field-level-encryption).	쓰기			
CreateFieldLevelEncryptionProfile	이 작업은 필드 레벨 암호화 프로파일을 생성합니다. (POST /2019-03-26/field-level-encryption-profile).	쓰기			
CreateInvalidation	이 작업은 새 무효화 배치 요청을 생성합니다 (POST /2019-03-26/distribution/<DISTRIBUTION_ID>/invalidation).	쓰기	distribution* (p. 788)		
CreatePublicKey	이 작업은 CloudFront에 새 퍼블릭 키를 추가합니다. (POST /2019-03-26/public-key).	쓰기			
CreateStreamingDistribution	이 작업은 새 RTMP 배포를 생성합니다(POST /2019-03-26/streaming-distribution).	쓰기	streaming-distribution* (p. 788)		
CreateStreamingDistributionWithTags	이 작업은 태그가 있는 새 RTMP 배포를 생성합니다 (POST /2019-03-26/streaming-distribution?WithTags).	태그 지정	streaming-distribution* (p. 788)		
				aws:RequestTag/${TagKey} (p. 789) aws:TagKeys (p. 789)	
DeleteCloudFrontOriginAccessIdentity	이 작업은 CloudFront 원본 액세스 ID를 삭제합니다 (DELETE /2019-03-26/origin-access-identity/cloudfront/<OAI_ID>).	쓰기	origin-access-identity* (p. 788)		
DeleteDistribution	작업은 웹 배포를 삭제합니다(DELETE /2019-03-26/distribution/<DISTRIBUTION_ID>).	쓰기	distribution* (p. 788)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteFieldLevelEncryptionConfig	이 작업은 필드 레벨 암호화 구성을 삭제합니다. (DELETE /2019-03-26/field-level-encryption/Id/<Id>).	쓰기			
DeleteFieldLevelEncryptionProfile	이 작업은 필드 레벨 암호화 프로파일을 삭제합니다. (DELETE /2019-03-26/field-level-encryption-profile/<Id>).	쓰기			
DeletePublicKey	이 작업은 CloudFront에서 퍼블릭 키를 삭제합니다. (DELETE /2019-03-26/public-key/<Id>).	쓰기			
DeleteStreamingDistribution	이 작업은 RTMP 배포를 삭제합니다(DELETE /2019-03-26/streaming-distribution/<DISTRIBUTION_ID>).	쓰기	streaming-distribution* (p. 788)		
GetCloudFrontOriginAccessIdentity	CloudFront 원본 액세스 ID에 대한 정보를 가져옵니다 (GET /2019-03-26/origin-access-identity/cloudfront/<OAI_ID>).	Read	origin-access-identity* (p. 788)		
GetCloudFrontOriginAccessIdentityConfig	CloudFront 원본 액세스 ID에 대한 구성 정보를 가져옵니다 (GET /2019-03-26/origin-access-identity/cloudfront/<OAI_ID>/config).	Read	origin-access-identity* (p. 788)		
GetDistribution	웹 배포에 대한 정보를 가져옵니다(GET /2019-03-26/distribution/<DISTRIBUTION_ID>).	Read	distribution* (p. 788)		
GetDistributionConfig	배포에 대한 구성 정보를 가져옵니다 (GET /2019-03-26/distribution/<DISTRIBUTION_ID>/config).	Read	distribution* (p. 788)		
GetFieldLevelEncryption	필드 레벨 암호화 구성 정보를 가져옵니다. (GET /2019-03-26/field-level-encryption/<Id>).	Read			
GetFieldLevelEncryptionConfig	필드 레벨 암호화 구성 정보를 가져옵니다(GET /2019-03-26/field-level-encryption/<Id>/config).	Read			
GetFieldLevelEncryptionProfile	필드 레벨 암호화 구성 정보를 가져옵니다(GET /2019-03-26/field-level-encryption/<Id>/config).	Read			
GetFieldLevelEncryptionProfileConfig	필드 레벨 암호화 프로파일 구성 정보를 가져옵니다 (GET /2019-03-26/field-level-encryption-profile/<Id>/config).	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetInvalidation	무효화에 대한 정보를 가져옵니다(GET /2019-03-26/distribution/<DISTRIBUTION_ID>/invalidation/<INVALIDATION_ID>).	Read	distribution* (p. 788)		
GetPublicKey	퍼블릭 키 정보를 가져옵니다(GET /2019-03-26/public-key/<Id>).	Read			
GetPublicKeyConfig	퍼블릭 키 구성 정보를 가져옵니다(GET /2019-03-26/public-key/<Id>/config).	Read			
GetStreamingDistribution	RTMP 배포에 대한 정보를 가져옵니다(GET /2019-03-26/streaming-distribution/<DISTRIBUTION_ID>).	Read	streaming-distribution* (p. 788)		
GetStreamingDistributionConfig	스트리밍 배포에 대한 구성 정보를 가져옵니다(GET /2019-03-26/streaming-distribution/<DISTRIBUTION_ID>/config).	Read	streaming-distribution* (p. 788)		
ListCloudFrontOriginAccessIdentities	CloudFront 원본 액세스 ID를 나열합니다(GET /2019-03-26/origin-access-identity/cloudfront?Marker=<MARKER>&MaxItems=<MAX_ITEMS>).	List			
ListDistributions	AWS 계정과 연결된 배포를 나열합니다(GET /2019-03-26/distribution?Marker=<MARKER>&MaxItems=<MAX_ITEMS>).	List			
ListDistributionsByWebACLId	지정된 AWS WAF 웹 ACL을 사용하여 AWS 계정과 연결된 배포를 나열합니다(GET /2019-03-26/distributionsByWebACLId/<WEB_ACL_ID>?Marker=<MARKER>&MaxItems=<MAX_ITEMS>).	List			
ListFieldLevelEncryptionConfigs	이 계정에 대해 CloudFront에서 생성된 모든 필드 레벨 암호화 구성을 나열합니다(GET /2019-03-26/field-level-encryption?Marker=<MARKER>&MaxItems=<MAX_ITEMS>).	List			
ListFieldLevelEncryptionProfiles	이 계정에 대해 CloudFront에서 생성된 모든 필드 레벨 암호화 프로파일을 나열합니다. (GET /2019-03-26/field-level-encryption-profile?Marker=<MARKER>&MaxItems=<MAX_ITEMS>).	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListInvalidations	무효화 배치를 나열합니다(GET /2019-03-26/distribution/<DISTRIBUTION_ID>/invalidation?Marker=<MARKER>&MaxItems=<MAX_ITEMS>).	List	distribution* (p. 788)		
ListPublicKeys	이 계정에 대해 CloudFront에 추가된 모든 퍼블릭 키를 나열합니다. (GET /2019-03-26/public-key?Marker=<MARKER>&MaxItems=<MAX_ITEMS>).	List			
ListStreamingDistributions	RTMP 배포를 나열합니다(GET /2019-03-26/streaming-distribution?Marker=<MARKER>&MaxItems=<MAX_ITEMS>).	List			
ListTagsForResource	CloudFront 리소스에 대한 태그를 나열합니다(GET /2019-03-26/tagging?Resource=<RESOURCE>).	Read	distribution (p. 788)		
			streaming-distribution (p. 788)		
TagResource	CloudFront 리소스에 태그를 추가합니다(POST /2019-03-26/tagging?Operation=Tag?Resource=<RESOURCE>).	태그 지정	distribution (p. 788)		
			streaming-distribution (p. 788)		
				aws:RequestTag/${TagKey} (p. 789) aws:TagKeys (p. 789)	
UntagResource	CloudFront 리소스에서 태그를 제거합니다(POST /2019-03-26/tagging?Operation=Untag?Resource=<RESOURCE>).	태그 지정	distribution (p. 788)		
			streaming-distribution (p. 788)		
				aws:TagKeys (p. 789)	
UpdateCloudFrontOriginAccessIdentity	이 작업에서는 CloudFront 원본 액세스 ID에 대한 구성을 설정합니다(PUT /2019-03-26/origin-access-identity/cloudfront/<OAI_ID>/config).	쓰기	origin-access-identity* (p. 788)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateDistribution	이 작업에서는 웹 배포에 대한 구성을 업데이트합니다 (PUT /2019-03-26/distribution/<DISTRIBUTION_ID>/config).	쓰기	distribution* (p. 788)		
UpdateFieldLevelEncryptionConfig	이 작업은 필드 레벨 암호화 구성을 업데이트합니다. (PUT /2019-03-26/field-level-encryption/<Id>/config).	쓰기			
UpdateFieldLevelEncryptionProfile	이 작업은 필드 레벨 암호화 프로파일을 업데이트합니다. (PUT /2019-03-26/field-level-encryption-profile/<Id>/config).	쓰기			
UpdatePublicKey	이 작업은 퍼블릭 키 정보를 업데이트합니다. (PUT /2019-03-26/public-key/<Id>/config).	쓰기			
UpdateStreamingDistribution	이 작업에서는 RTMP 배포에 대한 구성을 업데이트 합니다(PUT /2019-03-26/streaming-distribution/<DISTRIBUTION_ID>/config).	쓰기	streaming-distribution* (p. 788)		

Amazon CloudFront에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 783)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
distribution	`arn:${Partition}:cloudfront::${Account}:distribution/${DistributionId}`	aws:ResourceTag/${TagKey} (p. 789)
streaming-distribution	`arn:${Partition}:cloudfront::${Account}:streaming-distribution/${DistributionId}`	aws:ResourceTag/${TagKey} (p. 789)
origin-access-identity	`arn:${Partition}:cloudfront::${Account}:origin-access-identity/${Id}`	

Amazon CloudFront의 조건 키

Amazon CloudFront는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS CloudHSM에 사용되는 작업, 리소스 및 조건 키

AWS CloudHSM(서비스 접두사: `cloudhsm`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CloudHSM에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTagsToResource	지정된 AWS CloudHSM 리소스에 대한 하나 이상의 태그를 추가하거나 덮어씁니다.	태그 지정			
CopyBackupToRegion	지정된 리전에 백업의 복사본을 생성합니다.	쓰기	backup* (p. 792)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 792) aws:TagKeys (p. 792)	
CreateCluster	새 AWS CloudHSM 클러스터를 생성합니다.	쓰기	backup (p. 792)		
				aws:RequestTag/${TagKey} (p. 792) aws:TagKeys (p. 792)	
CreateHapg	고가용성 파티션 그룹을 생성합니다.	쓰기			
CreateHsm	지정된 AWS CloudHSM 클러스터에 새 하드웨어 보안 모듈(HSM)을 생성합니다.	쓰기	cluster* (p. 792)		
CreateLunaClient	HSM 클라이언트를 생성합니다	쓰기			
DeleteBackup	지정된 CloudHSM 백업을 삭제합니다.	쓰기	backup* (p. 792)		
DeleteCluster	지정된 AWS CloudHSM 클러스터를 삭제합니다.	쓰기	cluster* (p. 792)		
DeleteHapg	고가용성 파티션 그룹을 삭제합니다.	쓰기			
DeleteHsm	지정된 HSM을 삭제합니다.	쓰기			
DeleteLunaClient	클라이언트를 삭제합니다.	쓰기			
DescribeBackups	AWS CloudHSM 클러스터의 백업에 대한 정보를 가져옵니다.	Read			
DescribeClusters	AWS CloudHSM 클러스터에 대한 정보를 가져옵니다.	Read			
DescribeHapg	고가용성 파티션 그룹에 대한 정보를 검색합니다.	Read			
DescribeHsm	HSM에 대한 정보를 검색합니다. HSM은 ARN 또는 일련 번호로 식별할 수 있습니다.	Read			
DescribeLunaClient	HSM 클라이언트에 대한 정보를 검색합니다	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetConfig	클라이언트가 연결된 모든 고가용성 파티션 그룹에 연결하는 데 필요한 구성 파일을 가져옵니다.	Read			
InitializeCluster	AWS CloudHSM 클러스터를 클레임합니다.	쓰기	cluster* (p. 792)		
ListAvailableZones	사용 가능한 AWS CloudHSM 용량이 있는 가용 영역을 나열합니다.	List			
ListHapgs	계정에 대한 고가용성 파티션 그룹을 나열합니다.	List			
ListHsms	현재 고객에 대해 프로비저닝된 모든 HSM의 식별자를 검색합니다	List			
ListLunaClients	모든 클라이언트를 나열합니다.	List			
ListTags	지정된 AWS CloudHSM 클러스터에 대한 태그 목록을 가져옵니다.	Read	backup (p. 792)		
			cluster (p. 792)		
ListTagsForResource	지정된 AWS CloudHSM 리소스에 대한 모든 태그 목록을 반환합니다.	Read			
ModifyHapg	기존 고가용성 파티션 그룹을 수정합니다.	쓰기			
ModifyHsm	HSM을 수정합니다.	쓰기			
ModifyLunaClient	클라이언트에서 사용되는 인증서를 수정합니다.	쓰기			
RemoveTagsFromResource	지정된 AWS CloudHSM 리소스에서 하나 이상의 태그를 제거합니다.	태그 지정			
RestoreBackup	지정된 CloudHSM 백업을 복원합니다.	쓰기	backup* (p. 792)		
TagResource	지정된 AWS CloudHSM 클러스터에 대한 하나 이상의 태그를 추가하거나 덮어씁니다.	태그 지정	backup (p. 792)		
			cluster (p. 792)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 792) aws:TagKeys (p. 792)	
UntagResource	지정된 AWS CloudHSM 클러스터에서 지정된 태그를 제거합니다.	태그 지정	backup (p. 792)		
			cluster (p. 792)		
				aws:TagKeys (p. 792)	

AWS CloudHSM에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 789)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
backup	`arn:${Partition}:cloudhsm:${Region}:${Account}:backup/${CloudHsmBackupInstanceName}`	aws:ResourceTag/${TagKey} (p. 792)
cluster	`arn:${Partition}:cloudhsm:${Region}:${Account}:cluster/${CloudHsmClusterInstanceName}`	aws:ResourceTag/${TagKey} (p. 792)

AWS CloudHSM의 조건 키

AWS CloudHSM은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon CloudSearch에 사용되는 작업, 리소스 및 조건 키

Amazon CloudSearch(서비스 접두사: `cloudsearch`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon CloudSearch에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTags	Amazon CloudSearch 도메인에 리소스 태그를 연결합니다.	태그 지정	domain* (p. 795)		
BuildSuggesters	검색 권장 사항에 인덱스를 설정합니다.	쓰기	domain* (p. 795)		
CreateDomain	새로운 검색 도메인을 만듭니다.	쓰기	domain* (p. 795)		
DefineAnalysisScheme	언어별 텍스트 처리 옵션을 정의하기 위해 텍스트 또는 텍스트 배열에 적용할 수 있는 분석 체계를 구성합니다.	쓰기	domain* (p. 795)		
DefineExpression	검색 도메인에 대한 표현식을 구성합니다.	쓰기	domain* (p. 795)		
DefineIndexField	검색 도메인에 대한 IndexField를 구성합니다.	쓰기	domain* (p. 795)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DefineSuggester	도메인에 대한 제안자를 구성합니다.	쓰기	domain* (p. 795)		
DeleteAnalysisScheme	분석 체계를 삭제합니다.	쓰기	domain* (p. 795)		
DeleteDomain	검색 도메인과 모든 포함된 데이터를 영구적으로 삭제합니다.	쓰기	domain* (p. 795)		
DeleteExpression	검색 도메인에서 표현식을 제거합니다.	쓰기	domain* (p. 795)		
DeleteIndexField	검색 도메인에서 IndexField를 제거합니다.	쓰기	domain* (p. 795)		
DeleteSuggester	제안자를 삭제합니다.	쓰기	domain* (p. 795)		
DescribeAnalysisSchemes	도메인에 대해 구성된 분석 체계를 가져옵니다.	Read	domain* (p. 795)		
DescribeAvailabilityOptions	도메인에 대해 구성된 가용성 옵션을 가져옵니다.	Read	domain* (p. 795)		
DescribeDomainEndpointOptions	도메인에 대해 구성된 도메인 엔드포인트 옵션을 가져옵니다.	Read	domain* (p. 795)		
DescribeDomains	이 계정이 소유한 검색 도메인에 대한 정보를 가져옵니다.	List	domain* (p. 795)		
DescribeExpressions	검색 도메인에 대해 구성된 표현식을 가져옵니다.	Read	domain* (p. 795)		
DescribeIndexFields	검색 도메인에 대해 구성된 인덱스 필드에 대한 정보를 가져옵니다.	Read	domain* (p. 795)		
DescribeScalingParameters	도메인에 대해 구성된 조정 파라미터를 가져옵니다.	Read	domain* (p. 795)		
DescribeServiceAccessPolicies	도메인의 문서 및 검색 엔드포인트에 대한 액세스를 제어하는 액세스 정책에 대한 정보를 가져옵니다.	Read	domain* (p. 795)		
DescribeSuggesters	도메인에 대해 구성된 제안을 가져옵니다.	Read	domain* (p. 795)		
IndexDocuments	최근 인덱싱 옵션을 사용하여 해당 문서의 인덱싱을 시작하도록 검색 도메인에 알려줍니다.	쓰기	domain* (p. 795)		
ListDomainNames	계정이 소유한 모든 검색 도메인을 나열합니다.	List	domain* (p. 795)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTags	Amazon CloudSearch 도메인에 대한 리소스 태그를 모두 표시합니다.	Read	domain* (p. 795)		
RemoveTags	Amazon ES 도메인에서 지정된 리소스 태그를 제거합니다.	태그 지정	domain* (p. 795)		
UpdateAvailabilityOptions	도메인에 대한 가용성 옵션을 구성합니다.	쓰기	domain* (p. 795)		
UpdateDomainEndpointOptions	도메인에 대한 도메인 엔드포인트 옵션을 구성합니다.	쓰기	domain* (p. 795)		
UpdateScalingParameters	도메인에 대한 조정 파라미터를 구성합니다.	쓰기	domain* (p. 795)		
UpdateServiceAccessPolicies	도메인의 문서 및 검색 엔드포인트에 대한 액세스를 제어하는 액세스 규칙을 구성합니다.	권한 관리	domain* (p. 795)		
document [권한만 해당]	문서 서비스 작업에 대한 액세스를 허용합니다.	쓰기	domain (p. 795)		
search [권한만 해당]	검색 작업에 대한 액세스를 허용합니다.	Read	domain (p. 795)		
suggest [권한만 해당]	제안 작업에 대한 액세스를 허용합니다.	Read	domain (p. 795)		

Amazon CloudSearch에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 793)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

> **Note**
>
> IAM 정책에서 Amazon CloudSearch 리소스 ARN 사용에 대한 자세한 내용은 Amazon CloudSearch 개발자 안내서의 Amazon CloudSearch ARN을 참조하십시오.

리소스 유형	ARN	조건 키
domain	`arn:${Partition}:cloudsearch:${Region}:${Account}:domain/${DomainName}`	

Amazon CloudSearch의 조건 키

CloudSearch에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS CloudTrail에 사용되는 작업, 리소스 및 조건 키

AWS CloudTrail(서비스 접두사: `cloudtrail`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CloudTrail에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTags	추적에 하나 이상의 태그를 추가할 수 있는 권한을 부여합니다(최대 10개까지).	태그 지정	trail* (p. 798)		
CreateTrail	Amazon S3 버킷에 로그 데이터를 전달하기 위한 설정을 지정하는 추적을 생성할 수 있는 권한을 부여합니다.	쓰기	trail* (p. 798)		s3:PutObject
DeleteTrail	추적을 삭제할 수 있는 권한을 부여합니다.	쓰기	trail* (p. 798)		
DescribeTrails	계정의 현재 리전과 연결된 추적에 대한 설정을 나열할 수 있는 권한을 부여합니다.	Read			
GetEventSelectors	추적에 구성된 이벤트 선택기에 대한 설정을 나열할 수 있는 권한을 부여합니다.	Read	trail* (p. 798)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetInsightSelectors	추적에 대해 구성된 CloudTrail Insights 선택기를 나열할 수 있는 권한을 부여합니다.	Read	trail* (p. 798)		
GetTrail	추적 설정을 나열할 수 있는 권한을 부여합니다.	Read			
GetTrailStatus	지정된 추적에 대한 정보의 JSON 형식 목록을 검색할 수 있는 권한을 부여합니다.	Read	trail* (p. 798)		
ListPublicKeys	지정된 시간 범위에서 추적 다이제스트 파일을 서명하는 데 프라이빗 키가 사용된 퍼블릭 키를 나열할 수 있는 권한을 부여합니다.	Read			
ListTags	현재 리전의 추적에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	trail* (p. 798)		
ListTrails	계정의 현재 리전과 연결된 추적을 나열할 수 있는 권한을 부여합니다.	List			
LookupEvents	CloudTrail에서 캡처한 API 활동 이벤트(계정의 리소스를 생성, 업데이트 또는 삭제)를 검색할 수 있는 권한을 부여합니다.	Read			
PutEventSelectors	추적에 대한 이벤트 선택기를 생성 및 업데이트할 수 있는 권한을 부여합니다.	쓰기	trail* (p. 798)		
PutInsightSelectors	추적에 대한 CloudTrail Insights 선택기를 생성 및 업데이트할 수 있는 권한을 부여합니다.	쓰기	trail* (p. 798)		
RemoveTags	추적에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	trail* (p. 798)		
StartLogging	AWS API 호출 기록 및 추적에 대한 로그 파일 전달을 시작할 수 있는 권한을 부여합니다.	쓰기	trail* (p. 798)		
StopLogging	AWS API 호출 기록 및 추적에 대한 로그 파일 전달을 중지할 수 있는 권한을 부여합니다.	쓰기	trail* (p. 798)		
UpdateTrail	로그 파일 전달을 지정하는 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기	trail* (p. 798)		

AWS CloudTrail에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 796)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

> **Note**
>
> CloudTrail 작업에 대한 액세스를 제어하는 정책의 경우 Resource 요소가 항상 "*"로 설정됩니다. IAM 정책에서 리소스 ARN 사용에 대한 자세한 내용은 AWS CloudTrail User Guide의 사용자 지정 권한 부여를 참조하십시오.

리소스 유형	ARN	조건 키
trail	`arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}`	

AWS CloudTrail의 조건 키

CloudTrail에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon CloudWatch에 사용되는 작업, 리소스 및 조건 키

Amazon CloudWatch(서비스 접두사: `cloudwatch`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon CloudWatch에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteAlarms	지정된 경보를 모두 삭제합니다. 오류가 발생할 경우 경보가 삭제되지 않습니다	쓰기	alarm* (p. 801)		
DeleteAnomalyDetector	계정에서 지정된 이상 탐지 모델을 삭제합니다.	쓰기			
DeleteDashboards	지정한 CloudWatch 대시보드를 모두 삭제합니다	쓰기	dashboard* (p. 802)		
DeleteInsightRules	통찰력 규칙 모음을 삭제할 수 있는 권한을 부여합니다.	쓰기	insight-rule* (p. 802)		
DescribeAlarmHistory	지정된 경보의 내역을 검색합니다	Read	alarm* (p. 801)		
DescribeAlarms	지정된 이름을 가진 경보를 검색합니다	Read	alarm* (p. 801)		
DescribeAlarmsForMetric	단일 지표에 대한 모든 경보를 검색합니다	Read			
DescribeAnomalyDetectors	계정에서 생성한 이상 탐지 모델을 나열합니다.	Read			
DescribeInsightRules	사용자 계정이 현재 소유한 모든 통찰력 규칙을 설명할 수 있는 권한을 부여합니다.	Read			
DisableAlarmActions	지정된 경보에 대한 작업을 비활성화합니다	쓰기	alarm* (p. 801)		
DisableInsightRules	통찰력 규칙 모음을 비활성화할 수 있는 권한을 부여합니다.	쓰기	insight-rule* (p. 802)		
EnableAlarmActions	지정된 경보에 대한 작업을 활성화합니다	쓰기	alarm* (p. 801)		
EnableInsightRules	통찰력 규칙 모음을 활성화할 수 있는 권한을 부여합니다.	쓰기	insight-rule* (p. 802)		
GetDashboard	지정한 CloudWatch 대시보드의 세부 정보를 표시합니다	Read	dashboard* (p. 802)		
GetInsightRuleReport	지정된 통찰력 규칙에 대해 특정 시간 범위 동안 고유 기여자의 상위 N개 보고서를 반환할 수 있는 권한을 부여합니다.	Read	insight-rule* (p. 802)		
GetMetricData	CloudWatch 지표 데이터의 배치 양을 검색하고 검색된 데이터의	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	지표 수식을 계산하는 데 필요합니다				
GetMetricStatistics	지정된 지표에 대한 통계를 얻습니다	Read			
GetMetricWidgetImage	지표 위젯의 스냅샷을 검색하는 데 필요합니다	Read			
ListDashboards	사용자 계정의 모든 CloudWatch 대시보드 목록을 반환합니다	List			
ListMetrics	AWS 계정 소유자에 대해 저장된 유효한 지표 목록을 반환합니다	List			
ListTagsForResource	이 작업은 Amazon CloudWatch 리소스에 대한 태그를 나열합니다.	List	alarm (p. 801)		
			insight-rule (p. 802)		
	시나리오: CloudWatch-Alarm		alarm* (p. 801)		
	시나리오: CloudWatch-InsightRule		insight-rule* (p. 802)		
PutAnomalyDetector	CloudWatch 지표에 대한 이상 탐지 모델을 생성하거나 업데이트합니다.	쓰기			
PutDashboard	CloudWatch 대시보드를 생성하거나 이미 존재하는 경우 기존 대시보드를 업데이트합니다	쓰기	dashboard* (p. 802)		
PutInsightRule	새 통찰력 규칙을 생성하거나 기존 통찰력 규칙을 대체할 수 있는 권한을 부여합니다.	쓰기	insight-rule* (p. 802)		
				aws:RequestTag/${TagKey} (p. 802) aws:TagKeys (p. 802)	
PutMetricAlarm	경보를 생성 또는 업데이트하고 이를 지정된 Amazon CloudWatch 지표와 연결합니다	쓰기	alarm* (p. 801)		
				aws:RequestTag/${TagKey} (p. 802) aws:TagKeys (p. 802)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutMetricData	Amazon CloudWatch에 지표 데이터 요소를 게시합니다	쓰기		cloudwatch:namespace (p. 802)	
SetAlarmState	테스트 용도로 경보 상태를 일시적으로 설정합니다	쓰기	alarm* (p. 801)		
TagResource	이 작업은 Amazon CloudWatch 리소스에 태그를 지정합니다.	태그 지정	alarm (p. 801)		
			insight-rule (p. 802)		
				aws:TagKeys (p. 802) aws:RequestTag/${TagKey} (p. 802)	
	시나리오: CloudWatch-Alarm		alarm* (p. 801)		
	시나리오: CloudWatch-InsightRule		insight-rule* (p. 802)		
UntagResource	이 작업은 Amazon CloudWatch 리소스에서 태그를 제거합니다.	태그 지정	alarm (p. 801)		
			insight-rule (p. 802)		
				aws:TagKeys (p. 802)	
	시나리오: CloudWatch-Alarm		alarm* (p. 801)		
	시나리오: CloudWatch-InsightRule		insight-rule* (p. 802)		

Amazon CloudWatch에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 798)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
alarm	`arn:${Partition}:cloudwatch:${Region}:${Account}:alarm:${AlarmName}`	aws:ResourceTag/${TagKey} (p. 802)

리소스 유형	ARN	조건 키
dashboard	`arn:${Partition}:cloudwatch::${Account}:dashboard/${DashboardName}`	
insight-rule	`arn:${Partition}:cloudwatch:${Region}:${Account}:insight-rule/${InsightRuleName}`	aws:ResourceTag/${TagKey} (p. 802)

Amazon CloudWatch의 조건 키

Amazon CloudWatch는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
cloudwatch:namespace	선택적 네임스페이스 값의 존재 여부에 따라 작업을 필터링합니다.	문자열

CloudWatch Application Insights에 사용되는 작업, 리소스 및 조건 키

CloudWatch Application Insights(서비스 접두사: `applicationinsights`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- CloudWatch Application Insights에서 정의한 작업 (p. 802)
- CloudWatch Application Insights에서 정의한 리소스 유형 (p. 804)
- CloudWatch Application Insights에 사용되는 조건 키 (p. 804)

CloudWatch Application Insights에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateApplication	리소스 그룹에서 애플리케이션을 생성합니다.	쓰기			
CreateComponent	리소스 그룹에서 구성 요소를 생성합니다.	쓰기			
DeleteApplication	애플리케이션을 삭제합니다.	쓰기			
DeleteComponent	구성 요소를 삭제합니다.	쓰기			
DescribeApplication	애플리케이션을 설명합니다.	Read			
DescribeComponent	구성 요소를 설명합니다.	Read			
DescribeComponentConfiguration	구성 요소 구성을 설명합니다.	Read			
DescribeComponentConfigurationRecommendation	권장 애플리케이션 구성 요소 구성을 설명합니다.	Read			
DescribeObservation	관측치를 설명합니다.	Read			
DescribeProblem	문제를 설명합니다.	Read			
DescribeProblemObservations	문제의 관측치를 설명합니다.	Read			
ListApplications	모든 애플리케이션을 나열합니다.	List			
ListComponents	애플리케이션의 구성 요소를 나열합니다.	List			
ListProblems	애플리케이션의 문제를 나열합니다.	List			
UpdateApplication	애플리케이션을 업데이트합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateComponent	구성 요소를 업데이트합니다.	쓰기			
UpdateComponentConfiguration	구성 요소 구성을 업데이트합니다.	쓰기			

CloudWatch Application Insights에서 정의한 리소스 유형

CloudWatch Application Insights는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. CloudWatch Application Insights에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

CloudWatch Application Insights에 사용되는 조건 키

CloudWatch Application Insights에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon CloudWatch Logs에 사용되는 작업, 리소스 및 조건 키

Amazon CloudWatch Logs(서비스 접두사: `logs`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon CloudWatch Logs에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateKmsKey	지정된 AWS Key Management Service(AWS KMS) 고객 마스터 키(CMK)를 지정된 로그 그룹에 연결합니다.	쓰기	log-group* (p. 808)		
CancelExportTask	PENDING 또는 RUNNING 상태에 있을 경우 내보내기 작업을 취소합니다	쓰기			
CreateExportTask	로그 그룹의 데이터를 Amazon S3 버킷으로 효율적으로 내보낼 수 있는 ExportTask를 생성합니다	쓰기	log-group* (p. 808)		
CreateLogDelivery [권한만 해당]	로그 전달을 생성합니다	쓰기			
CreateLogGroup	지정된 이름으로 새 로그 그룹을 생성합니다	쓰기			
CreateLogStream	지정된 이름으로 새 로그 스트림을 생성합니다	쓰기	log-group* (p. 808)		
DeleteDestination	지정된 이름을 가진 대상을 삭제하고 해당 대상에 게시한 모든 구독 필터를 최종적으로 비활성화합니다	쓰기			
DeleteLogDelivery [권한만 해당]	지정된 로그 전달의 로그 전달 정보를 삭제합니다	쓰기			
DeleteLogGroup	지정된 이름을 가진 로그 그룹을 삭제하고 해당 로그 그룹과 연결된 모든 아카이브된 로그 이벤트를 영구적으로 삭제합니다	쓰기	log-group* (p. 808)		
DeleteLogStream	로그 스트림을 삭제하고 해당 로그 스트림과 연결된 모든 아카이브된 로그 이벤트를 영구적으로 삭제합니다	쓰기	log-stream* (p. 808)		
DeleteMetricFilter	지정된 로그 그룹과 연결된 지표 필터를 삭제합니다	쓰기	log-group* (p. 808)		
DeleteResourcePolicy	이 계정에서 리소스 정책을 삭제합니다	쓰기			
DeleteRetentionPolicy	지정된 로그 그룹의 보존 정책을 삭제합니다	쓰기	log-group* (p. 808)		
DeleteSubscriptionFilter	지정된 로그 그룹과 연결된 구독 필터를 삭제합니다	쓰기	log-group* (p. 808)		
DescribeDestinations	AWS 요청 계정과 연결된 모든 대상을 반환합니다	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeExportTasks	AWS 요청 계정과 연결된 모든 내보내기 작업을 반환합니다	List			
DescribeLogGroups	AWS 요청 계정과 연결된 모든 로그 그룹을 반환합니다	List	log-group* (p. 808)		
DescribeLogStreams	지정된 로그 그룹과 연결된 모든 로그 스트림을 반환합니다	List	log-group* (p. 808)		
DescribeMetricFilters	지정된 로그 그룹과 연결된 모든 지표 필터를 반환합니다	List	log-group* (p. 808)		
DescribeQueries	이 계정에서 예약되었거나 실행 중이거나 최근에 실행된 CloudWatch Logs Insights 쿼리의 목록을 반환합니다. 모든 쿼리를 요청하거나, 특정 그룹에 대한 쿼리 또는 특정 상태를 갖는 쿼리로 제한할 수 있습니다.	List			
DescribeResourcePolicies	이 계정의 모든 리소스 정책을 반환합니다.	List			
DescribeSubscriptionFilters	지정된 로그 그룹과 연결된 모든 구독 필터를 반환합니다	List	log-group* (p. 808)		
DisassociateKmsKey	지정된 로그 그룹에서 연결된 AWS Key Management Service(AWS KMS) 고객 마스터 키(CMK)를 연결 해제합니다	쓰기	log-group* (p. 808)		
FilterLogEvents	지정된 로그 그룹에서 필터 패턴을 기준으로 필터링된 로그 이벤트를 검색합니다	Read	log-group* (p. 808)		
GetLogDelivery [권한만 해당]	지정된 로그 전달의 로그 전달 정보를 가져옵니다	Read			
GetLogEvents	지정된 로그 스트림에서 로그 이벤트를 검색합니다	Read	log-stream* (p. 808)		
GetLogGroupFields	지정된 로그 그룹의 로그 이벤트에 포함된 필드의 목록을 각 필드를 포함하는 로그 이벤트의 백분율과 함께 반환합니다. 이 검색은 사용자가 지정하는 기간으로 제한됩니다.	Read	log-group* (p. 808)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetLogRecord	단일 로그 이벤트의 모든 필드 및 값을 검색합니다. logRecordPointer를 생성한 원래 쿼리가 필드 하위 집합만 검색하더라도 모든 필드가 검색됩니다. 필드는 필드 이름/필드 값 페어로 반환됩니다.	Read			
GetQueryResults	지정된 쿼리의 결과를 반환합니다. 쿼리가 진행 중일 경우 현재 실행의 부분 결과가 반환됩니다. 쿼리에서 요청된 필드만 반환됩니다.	Read			
ListLogDeliveries [권한만 해당]	지정된 계정 및/또는 로그 소스에 대한 모든 로그 전달을 나열합니다	List			
ListTagsLogGroup	지정된 로그 그룹에 대한 태그를 나열합니다	List	log-group* (p. 808)		
PutDestination	대상을 생성 또는 업데이트합니다	쓰기			
PutDestinationPolicy	기존 대상과 연결된 액세스 정책을 생성 또는 업데이트합니다	쓰기			
PutLogEvents	지정된 로그 스트림에 로그 이벤트의 배치를 업로드합니다	쓰기	log-stream* (p. 808)		
PutMetricFilter	지표 필터를 생성 또는 업데이트하고 이를 지정된 로그 그룹과 연결합니다	쓰기	log-group* (p. 808)		
PutResourcePolicy	다른 AWS 서비스가 이 계정에 로그 이벤트를 적용할 수 있도록 하는 리소스 정책을 생성 또는 업데이트합니다	쓰기			
PutRetentionPolicy	지정된 로그 그룹의 보존을 설정합니다	쓰기	log-group* (p. 808)		
PutSubscriptionFilter	구독 필터를 생성 또는 업데이트하고 이를 지정된 로그 그룹과 연결합니다	쓰기	log-group* (p. 808)		
StartQuery	CloudWatch Logs Insights를 사용하여 로그 그룹 쿼리를 예약합니다. 사용자는 쿼리할 로그 그룹 및 시간 범위 그리고 사용할 쿼리 문자열을 지정합니다.	Read	log-group* (p. 808)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StopQuery	진행 중인 CloudWatch Logs Insights 쿼리를 중지합니다. 쿼리가 이미 완료된 경우 작업이 지정된 쿼리가 실행 중이지 않음을 나타내는 오류를 반환합니다.	Read			
TagLogGroup	지정된 로그 그룹에 지정된 태그를 추가 또는 업데이트합니다	쓰기	log-group* (p. 808)		
TestMetricFilter	로그 이벤트 메시지의 샘플을 기준으로 지표 필터의 필터 패턴을 테스트합니다	Read			
UntagLogGroup	지정된 로그 그룹에서 지정된 태그를 제거합니다	쓰기	log-group* (p. 808)		
UpdateLogDelivery [권한만 해당]	지정된 로그 전달의 로그 전달 정보를 업데이트합니다	쓰기			

Amazon CloudWatch Logs에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 804)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
log-group	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}`	
log-stream	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}:log-stream:${LogStreamName}`	

Amazon CloudWatch Logs의 조건 키

CloudWatch Logs에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon CloudWatch Synthetics에 사용되는 작업, 리소스 및 조건 키

Amazon CloudWatch Synthetics(서비스 접두사: `synthetics`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon CloudWatch Synthetics에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCanary	카나리아를 생성합니다.	쓰기			
DeleteCanary	카나리아를 삭제합니다. Amazon Synthetics에서는 Lambda 함수와 CloudWatch 경보를 생성한 경우 이를 제외한 모든 리소스를 삭제합니다.	쓰기	canary* (p. 810)		
DescribeCanaries	모든 카나리아 또는 하나의 카나리아에 대한 정보를 반환합니다.	Read	canary (p. 810)		
DescribeTestRuns	카나리아와 관련된 모든 테스트 실행에 대한 정보를 반환합니다.	Read	canary (p. 810)		
ListTagsForResource	카나리아와 관련된 모든 태그 및 값 목록을 반환합니다.	Read	canary (p. 810)		
StartCanary	Amazon Synthetics가 웹 사이트 모니터링을 시작하도록 카나리아를 시작합니다.	쓰기	canary* (p. 810)		
StopCanary	카나리아를 중지합니다.	쓰기	canary* (p. 810)		
TagResource	카나리아에 하나 이상의 태그를 추가합니다.	쓰기	canary (p. 810)		
UntagResource	카나리아에서 하나 이상의 태그를 제거합니다.	쓰기	canary (p. 810)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateCanary	카나리아를 업데이트합니다.	쓰기	canary* (p. 810)		

Amazon CloudWatch Synthetics에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 809)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
canary	`arn:${Partition}:synthetics::${Account}:canary:${CanaryName}`	

Amazon CloudWatch Synthetics의 조건 키

CloudWatch Synthetics에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Code Signing for Amazon FreeRTOS에 사용되는 작업, 리소스 및 조건 키

AWS Code Signing for Amazon FreeRTOS(서비스 접두사: `signer`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Code Signing for Amazon FreeRTOS에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있

으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelSigningProfile	서명 프로필을 취소합니다.	쓰기	signing-profile* (p. 812)		
DescribeSigningJob	서명 작업을 설명합니다.	Read	signing-job* (p. 812)		
GetSigningPlatform	서명 플랫폼을 검색합니다.	Read			
GetSigningProfile	서명 프로파일을 검색합니다.	Read	signing-profile* (p. 812)		
ListSigningJobs	서명 작업을 나열합니다.	List			
ListSigningPlatforms	모든 서명 플랫폼을 나열합니다.	List			
ListSigningProfiles	계정과 연결된 모든 서명 프로필을 나열합니다.	List			
ListTagsForResource	서명 프로파일 리소스와 연결된 태그를 나열합니다.	List	signing-profile* (p. 812)		
PutSigningProfile	서명 프로필이 없을 경우 새로 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 812) aws:TagKeys (p. 812)	
StartSigningJob	코드 서명 요청을 시작합니다.	쓰기	signing-profile* (p. 812)		
TagResource	서명 프로파일 리소스에 하나 이상의 태그를 추가합니다.	태그 지정	signing-profile* (p. 812)		
				aws:TagKeys (p. 812) aws:RequestTag/${TagKey} (p. 812)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UntagResource	서명 프로파일 리소스에서 하나 이상의 태그를 제거합니다.	태그 지정	signing-profile* (p. 812)		
				aws:TagKeys (p. 812) aws:RequestTag/${TagKey} (p. 812)	

AWS Code Signing for Amazon FreeRTOS에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 810)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
signing-profile	`arn:${Partition}:signer:${Region}::/signing-profiles/${profileName}`	aws:ResourceTag/${TagKey} (p. 812)
signing-job	`arn:${Partition}:signer:${Region}::/signing-jobs/${jobId}`	

AWS Code Signing for Amazon FreeRTOS의 조건 키

AWS Code Signing for Amazon FreeRTOS는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열

AWS CodeBuild에 사용되는 작업, 리소스 및 조건 키

AWS CodeBuild(서비스 접두사: `codebuild`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CodeBuild에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchDeleteBuilds	하나 이상의 빌드를 삭제합니다.	쓰기	project* (p. 817)		
BatchGetBuilds	하나 이상의 빌드에 대한 정보를 가져옵니다.	Read	project* (p. 817)		
BatchGetProjects	하나 이상의 빌드 프로젝트에 대한 정보를 가져옵니다.	Read	project* (p. 817)		
BatchGetReportGroups	입력 reportGroupArns 파라미터에서 지정한 ReportGroup 객체의 배열을 반환합니다.	Read	report-group* (p. 817)		
BatchGetReports	입력 reportArns 파라미터에서 지정한 보고서 객체의 배열을 반환합니다.	Read	report-group* (p. 817)		
BatchPutTestCases [권한만 해당]	보고서에 대한 정보를 추가하거나 업데이트합니다.	쓰기	report-group* (p. 817)		
CreateProject	빌드 프로젝트를 생성합니다.	쓰기	project* (p. 817)		
				aws:RequestTag/${TagKey} (p. 817)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 817)	
CreateReport [권한만 해당]	보고서를 생성합니다. 보고서 그룹에 대한 buildspec 파일에 지정된 테스트가 프로젝트를 빌드하는 동안 실행될 때 보고서가 생성됩니다.	쓰기	report-group* (p. 817)		
CreateReportGroup	보고서 그룹을 생성합니다.	쓰기	report-group* (p. 817)		
CreateWebhook	소스 코드가 GitHub 또는 Bitbucket 리포지토리에 저장된 기존 AWS CodeBuild 빌드 프로젝트의 경우, 코드 변경이 리포지토리에 푸시될 때마다 AWS CodeBuild가 소스 코드를 다시 빌드할 수 있습니다.	쓰기	project* (p. 817)		
DeleteOAuthToken [권한만 해당]	연결된 타사 OAuth 공급자의 OAuth 토큰을 삭제합니다. AWS CodeBuild 콘솔에서만 사용됩니다.	쓰기			
DeleteProject	빌드 프로젝트를 삭제합니다.	쓰기	project* (p. 817)		
DeleteReport	보고서를 삭제합니다.	쓰기	report-group* (p. 817)		
DeleteReportGroup	보고서 그룹을 삭제합니다.	쓰기	report-group* (p. 817)		
DeleteResourcePolicy	연결된 프로젝트 또는 보고서 그룹에 대한 리소스 정책을 삭제합니다.	권한 관리	project (p. 817)		
			report-group (p. 817)		
DeleteSourceCredentials	GitHub, GitHub Enterprise 또는 Bitbucket 소스 자격 증명 세트를 삭제합니다.	쓰기			
DeleteWebhook	소스 코드가 GitHub 또는 Bitbucket 리포지토리에 저장된 기존 AWS CodeBuild 빌드 프로젝트의 경우, 코드 변경이 리포지토리에 푸시될 때마다 AWS CodeBuild가 소스 코드를 다시 빌드할 수 없습니다.	쓰기	project* (p. 817)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeTestCases	TestCase 객체의 배열을 반환합니다.	Read	report-group* (p. 817)		
GetResourcePolicy	지정된 프로젝트 또는 보고서 그룹에 대한 리소스 정책을 반환합니다.	Read	project (p. 817)		
			report-group (p. 817)		
ImportSourceCredentials	GitHub, GitHub Enterprise 또는 Bitbucket 리포지토리에 소스 코드가 저장된 AWS CodeBuild 프로젝트의 소스 리포지토리 자격 증명을 가져옵니다.	쓰기			
InvalidateProjectCache	프로젝트의 캐시를 재설정합니다.	쓰기	project* (p. 817)		
ListBuilds	하나의 빌드를 나타내는 각 빌드 ID가 들어 있는 빌드 ID 목록을 가져옵니다.	List			
ListBuildsForProject	지정된 빌드 프로젝트에 대해 하나의 빌드를 나타내는 각 빌드 ID가 들어 있는 빌드 ID 목록을 가져옵니다.	List	project* (p. 817)		
ListConnectedOAuthAccounts [권한만 해당]	연결된 타사 OAuth 공급자를 나열합니다. AWS CodeBuild 콘솔에서만 사용됩니다.	List			
ListCuratedEnvironmentImages	AWS CodeBuild에서 관리하는 도커 이미지에 대한 정보를 가져옵니다.	List			
ListProjects	하나의 빌드 프로젝트를 나타내는 각 빌드 프로젝트 이름이 들어 있는 빌드 프로젝트 이름 목록을 가져옵니다.	List			
ListReportGroups	보고서 그룹 ARN의 목록을 반환합니다. 각 보고서 그룹 ARN은 하나의 보고서 그룹을 나타냅니다.	List			
ListReports	보고서 ARN의 목록을 반환합니다. 각 보고서 ARN은 하나의 보고서를 나타냅니다.	List			
ListReportsForReportGroup	지정된 보고서 그룹에 속하는 보고서 ARN의 목록을 반환합니다. 각 보고서 ARN은 하나의 보고서를 나타냅니다.	List	report-group* (p. 817)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListRepositories [권한만 해당]	연결된 타사 OAuth 공급자의 소스 코드 리포지토리를 나열합니다. AWS CodeBuild 콘솔에서만 사용됩니다.	List			
ListSharedProjects	요청자들과 공유한 프로젝트 ARN의 목록을 반환합니다. 각 프로젝트 ARN은 하나의 프로젝트를 나타냅니다.	List			
ListSharedReportGroups	요청자들과 공유한 보고서 그룹 ARN의 목록을 반환합니다. 각 보고서 그룹 ARN은 하나의 보고서 그룹을 나타냅니다.	List			
ListSourceCredentials	SourceCredentialsInfo 객체의 목록을 반환합니다.	List			
PersistOAuthToken [권한만 해당]	연결된 타사 OAuth 공급자의 OAuth 토큰을 저장합니다. AWS CodeBuild 콘솔에서만 사용됩니다.	쓰기			
PutResourcePolicy	연결된 프로젝트 또는 보고서 그룹에 대한 리소스 정책을 생성합니다.	권한 관리	project (p. 817)		
			report-group (p. 817)		
StartBuild	빌드 실행을 시작합니다.	쓰기	project* (p. 817)		
StopBuild	빌드 실행 중지를 시도합니다.	쓰기	project* (p. 817)		
UpdateProject	기존 빌드 프로젝트의 설정을 변경합니다.	쓰기	project* (p. 817)		
				aws:RequestTag/${TagKey} (p. 817) aws:TagKeys (p. 817)	
UpdateReport [권한만 해당]	보고서에 대한 정보를 업데이트합니다.	쓰기	report-group* (p. 817)		
UpdateReportGroup	기존 보고서 그룹의 설정을 변경합니다.	쓰기	report-group* (p. 817)		
UpdateWebhook	AWS CodeBuild 빌드 프로젝트와 연결된 웹후크를 업데이트합니다.	쓰기	project* (p. 817)		

AWS CodeBuild에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 813)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
build	`arn:${Partition}:codebuild:${Region}:${Account}:build/${BuildId}`	
project	`arn:${Partition}:codebuild:${Region}:${Account}:project/${ProjectName}`	aws:ResourceTag/${TagKey} (p. 817)
report-group	`arn:${Partition}:codebuild:${Region}:${Account}:report-group/${ReportGroupName}`	
report	`arn:${Partition}:codebuild:${Region}:${Account}:report/${ReportGroupName}:${ReportId}`	

AWS CodeBuild의 조건 키

AWS CodeBuild는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS CodeCommit에 사용되는 작업, 리소스 및 조건 키

AWS CodeCommit(서비스 접두사: `codecommit`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CodeCommit에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateApprovalRuleTemplateWithRepository	승인 규칙 템플릿을 리포지토리와 연결할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
BatchAssociateApprovalRuleTemplateWithRepositories	단일 작업으로 승인 규칙 템플릿을 여러 리포지토리와 연결할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
BatchDescribeMergeConflicts	3방향 병합 또는 스쿼시 병합 옵션을 사용하여 두 개의 커밋을 병합하려 할 때 여러 병합 충돌에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
BatchDisassociateApprovalRuleTemplateFromRepositories	단일 작업으로 승인 규칙 템플릿과 여러 리포지토리 간의 연결을 제거할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
BatchGetCommits	AWS CodeCommit 리포지토리에서 하나 이상의 커밋에 대한 반환 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
BatchGetPullRequests [권한만 해당]	AWS CodeCommit 리포지토리에서 하나 이상의 풀 요청에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
BatchGetRepositories	여러 리포지토리에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelUploadArchive [권한만 해당]	AWS CodePipeline의 파이프라인으로 아카이브 업로드를 취소할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
CreateApprovalRuleTemplate	템플릿에 정의된 조건과 일치하는 풀 요청에 승인 규칙을 자동으로 생성하는 승인 규칙 템플릿을 만들 수 있는 권한을 부여합니다. 개별 풀 요청에 대한 승인 규칙을 생성할 수 있는 권한은 부여하지 않습니다.	쓰기			
CreateBranch	이 API를 사용하여 AWS CodeCommit 리포지토리에서 브랜치를 생성할 수 있는 권한을 부여합니다. Git create branch 작업은 제어하지 않습니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
CreateCommit	AWS CodeCommit 리포지토리의 브랜치에서 하나 또는 여러 파일을 추가, 복사, 이동 또는 업데이트하고 지정된 브랜치에서 변경 사항에 대한 커밋을 생성할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
CreatePullRequest	지정된 리포지토리에서 풀 요청을 생성할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
CreatePullRequestApprovalRule	개별 풀 요청과 관련된 승인 규칙을 생성할 수 있는 권한을 부여합니다. 승인 규칙 템플릿을 생성할 수 있는 권한은 부여하지 않습니다.	쓰기	repository* (p. 826)		
CreateRepository	AWS CodeCommit 리포지토리를 생성할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				aws:RequestTag/${TagKey} (p. 826) aws:TagKeys (p. 826)	
CreateUnreferencedMergeCommit	3방향 또는 스쿼시 병합 옵션을 사용한 2개 커밋 병합의 결과를 포함하는 참조되지 않은 커밋을 생성할 수 있는 권한을 부여합니다. Git merge 작업은 제어하지 않습니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
DeleteApprovalRuleTemplate	승인 규칙 템플릿을 삭제할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteBranch	이 API를 사용하여 AWS CodeCommit 리포지토리에서 브랜치를 삭제할 수 있는 권한을 부여합니다. Git create branch 작업은 제어하지 않습니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
DeleteCommentContent	리포지토리에서 변경 사항, 파일 또는 커밋에 대한 설명의 내용을 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
DeleteFile	지정된 브랜치에서 지정된 파일을 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
DeletePullRequestApprovalRule	규칙이 승인 규칙 템플릿에 의해 생성되지 않은 경우 풀 요청에 대해 생성된 승인 규칙을 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
DeleteRepository	AWS CodeCommit 리포지토리를 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
DescribeMergeConflicts	3방향 또는 스쿼시 병합 옵션을 사용하여 두 개의 커밋을 병합하려 할 때 특정 병합 충돌에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
DescribePullRequestEvents	하나 이상의 풀 요청 이벤트에 관한 정보를 반환할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
DisassociateApprovalRuleTemplateFromRepository	승인 규칙 템플릿과 리포지토리 간의 연결을 제거할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
EvaluatePullRequestApprovalRules	현재 승인 상태 및 승인 규칙 요구 사항에 따라 풀 요청이 병합 가능한지 여부를 평가할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetApprovalRuleTemplate	승인 규칙 템플릿에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read			
GetBlob	AWS CodeCommit 콘솔에서 AWS CodeCommit 리포지토리 내 개별 파일의 인코딩된 콘텐츠를 볼 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetBranch	이 API를 사용하여 AWS CodeCommit 리포지토리 내 브랜치의 세부 정보를 가져올 수 있는 권한을 부여합니다. Git branch 작업은 제어하지 않습니다.	Read	repository* (p. 826)		
GetComment	리포지토리에서 변경 사항, 파일 또는 커밋에 대한 설명의 내용을 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetCommentsForComparedCommit	두 커밋 간의 비교에 대해 작성된 설명에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetCommentsForPullRequest	풀 요청에 대한 설명을 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetCommit	이 API를 사용하여 커밋에 대한 정보(커밋 메시지, 커미터 정보 등)를 반환할 수 있는 권한을 부여합니다. Git log 작업은 제어하지 않습니다.	Read	repository* (p. 826)		
GetCommitHistory [권한만 해당]	리포지토리의 커밋 이력에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetCommitsFromMergeBase [권한만 해당]	잠재적 병합 컨텍스트에서 커밋 간의 차이에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetDifferences	커밋 지정자(예: 브랜치, 태그, HEAD, 커밋 ID 또는 기타 정규화된 참조) 간의 차이에 관한 정보를 반환할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetFile	지정된 파일 및 그 메타데이터의 base-64 인코딩된 내용을 반환할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetFolder	리포지토리의 지정된 폴더의 내용을 반환할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetMergeCommit	병합 커밋을 생성하는 풀 요청의 병합 옵션 중 하나로 생성된 병합 커밋에 대한 정보를 가져올 수 있는 권한을 부여합니다. 모든 병합 옵션이 병합 커밋을 생성하는 것은 아닙니다. 이 권한은 Git merge 작업을 제어하지 않습니다.	Read	repository* (p. 826)		
				codecommit:References (p. 826)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetMergeConflicts	리포지토리의 풀 요청에 대한 커밋 전/후 ID 간의 병합 출돌에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetMergeOptions	두 개의 커밋을 병합하는 데 사용할 수 있는 풀 요청의 병합 옵션에 대한 정보를 가져올 수 있는 권한을 부여합니다. Git merge 작업은 제어하지 않습니다.	Read	repository* (p. 826)		
GetObjectIdentifier [권한만 해당]	BLOB, 트리 및 커밋을 해당 식별자로 확인할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetPullRequest	지정된 리포지토리의 풀 요청에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetPullRequestApprovalStates	입력된 풀 요청에 대한 현재 승인을 검색할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetPullRequestOverrideState	지정된 풀 요청의 현재 재정의 상태를 검색할 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetReferences [권한만 해당]	AWS CodeCommit 리포지토리의 참조에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다. Git reference 작업은 제어하지 않습니다.	Read	repository* (p. 826)		
GetRepository	AWS CodeCommit 리포지토리에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetRepositoryTriggers	리포지토리에 대해 구성된 트리거에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetTree [권한만 해당]	AWS CodeCommit 콘솔에서 AWS CodeCommit 리포지토리의 지정된 트리의 콘텐츠를 볼 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GetUploadArchiveStatus [권한만 해당]	AWS CodePipeline의 파이프라인으로 아카이브 업로드에 대한 상태 정보를 볼 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		
GitPull [권한만 해당]	AWS CodeCommit 리포지토리에서 로컬 리포지토리로 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 826)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GitPush [권한만 해당]	로컬 리포지토리에서 AWS CodeCommit 리포지토리로 정보를 내보낼 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
ListApprovalRuleTemplates	AWS 계정의 AWS 리전에 있는 모든 승인 규칙 템플릿을 나열할 수 있는 권한을 부여합니다.	List			
ListAssociatedApprovalRuleTemplatesForRepository	리포지토리와 연결된 승인 규칙 템플릿을 나열할 수 있는 권한을 부여합니다.	List	repository* (p. 826)		
ListBranches	이 API를 사용하여 AWS CodeCommit 리포지토리의 브랜치를 나열할 수 있는 권한을 부여합니다. Git branch 작업은 제어하지 않습니다.	List	repository* (p. 826)		
ListPullRequests	지정된 리포지토리에 대한 풀 요청을 나열할 수 있는 권한을 부여합니다.	List	repository* (p. 826)		
ListRepositories	AWS 계정의 현재 리전에 있는 AWS CodeCommit 리포지토리에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List			
ListRepositoriesForApprovalRuleTemplate	승인 규칙 템플릿과 연결된 리포지토리를 나열할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	CodeCommit 리소스 ARN에 연결된 리소스를 나열할 수 있는 권한을 부여합니다.	List	repository (p. 826)		
MergeBranchesByFastForward	패스트 포워드 병합 옵션을 사용하여 두 개의 커밋을 지정된 대상 브랜치로 병합할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
MergeBranchesBySquash	스쿼시 병합 옵션을 사용하여 두 개의 커밋을 지정된 대상 브랜치로 병합할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
MergeBranchesByThreeWay	3방향 병합 옵션을 사용하여 두 개의 커밋을 지정된 대상 브랜치로 병합할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
MergePullRequestByFastForward	풀 요청을 닫고 패스트 포워드 병합 옵션을 사용하여 지정된 커밋에서 해당 풀 요청을 위해 지정된 대상 브랜치로 병합을 시도할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
MergePullRequestBySquash	풀 요청을 닫고 스쿼시 병합 옵션을 사용하여 지정된 커밋에서 해당 풀 요청을 위해 지정된 대상 브랜치로 병합을 시도할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
MergePullRequestByThreeWay	풀 요청을 닫고 3방향 병합 옵션을 사용하여 지정된 커밋에서 해당 풀 요청을 위해 지정된 대상 브랜치로 병합을 시도할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
OverridePullRequestApprovalRules	템플릿에 의해 생성된 승인 규칙을 포함하여 풀 요청에 대한 모든 승인 규칙을 재정의할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
PostCommentForComparedCommit	두 커밋 간 비교에 대한 설명을 게시할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
PostCommentForPullRequest	풀 요청에 대한 설명을 게시할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
PostCommentReply	커밋 간 비교 또는 풀 요청에 대한 설명에 회신하는 설명을 게시할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
PutFile	사용자가 AWS CodeCommit 리포지토리의 브랜치에 파일을 추가하거나 업데이트하고 지정된 브랜치에서 추가를 위한 커밋을 생성할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
				codecommit:References (p. 826)	
PutRepositoryTriggers	리포지토리에 대한 트리거를 생성, 업데이트 또는 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
TagResource	CodeCommit 리소스 ARN에 리소스 태그를 연결할 수 있는 권한을 부여합니다.	쓰기	repository (p. 826)		
				aws:ResourceTag/${TagKey} (p. 826) aws:RequestTag/${TagKey} (p. 826) aws:TagKeys (p. 826)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
TestRepositoryTriggers	트리거 대상으로 정보를 전송하여 리포지토리 트리거의 기능을 테스트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
UntagResource	CodeCommit 리소스 ARN에서 리소스 태그를 연결 해제할 수 있는 권한을 부여합니다.	쓰기	repository (p. 826)		
				aws:TagKeys (p. 826)	
UpdateApprovalRuleTemplateContent	승인 규칙 템플릿의 콘텐츠를 업데이트할 수 있는 권한을 부여합니다. 풀 요청용으로 특별히 생성된 승인 규칙의 콘텐츠를 업데이트할 수 있는 권한은 부여하지 않습니다.	쓰기			
UpdateApprovalRuleTemplateDescription	승인 규칙 템플릿의 설명을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateApprovalRuleTemplateName	승인 규칙 템플릿의 이름을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateComment	자격 증명이 설명을 생성하는 데 사용된 자격 증명과 일치할 경우 설명의 내용을 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
UpdateDefaultBranch	AWS CodeCommit 리포지토리에서 기본 브랜치를 변경할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
UpdatePullRequestApprovalRuleContent	특정 풀 요청에 대해 생성된 승인 규칙의 콘텐츠를 업데이트할 수 있는 권한을 부여합니다. 승인 규칙 템플릿으로 생성된 규칙의 승인 규칙 콘텐츠를 업데이트할 수 있는 권한은 부여하지 않습니다.	쓰기	repository* (p. 826)		
UpdatePullRequestApprovalState	풀 요청에 대한 승인 상태를 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
UpdatePullRequestDescription	풀 요청의 설명을 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
UpdatePullRequestStatus	풀 요청의 상태를 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
UpdatePullRequestTitle	풀 요청의 제목을 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateRepositoryDescription	AWS CodeCommit 리포지토리의 설명을 변경할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
UpdateRepositoryName	AWS CodeCommit 리포지토리의 이름을 변경할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		
UploadArchive [권한만 해당]	AWS CodePipeline의 서비스 역할이 리포지토리 변경 사항을 파이프라인으로 업로드할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 826)		

AWS CodeCommit에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 818)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
repository	`arn:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}`	aws:ResourceTag/${TagKey} (p. 826)

AWS CodeCommit에 사용되는 조건 키

AWS CodeCommit은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
codecommit:References	지정된 AWS CodeCommit 작업에 대한 Git 참조를 기준으로 액세스를 필터링합니다.	문자열

AWS CodeDeploy에 사용되는 작업, 리소스 및 조건 키

AWS CodeDeploy(서비스 접두사: `codedeploy`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CodeDeploy에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTagsToOnPremisesInstances	하나 이상의 온프레미스 인스턴스에 태그를 추가합니다.	태그 지정	instance* (p. 831)		
BatchGetApplicationRevisions	하나 이상의 애플리케이션 개정에 대한 정보를 가져옵니다.	Read	application* (p. 831)		
BatchGetApplications	IAM 사용자와 연결된 여러 애플리케이션에 대한 정보를 가져옵니다.	Read	application* (p. 831)		
BatchGetDeploymentGroups	하나 이상의 배포 그룹에 대한 정보를 가져옵니다.	Read	deploymentgroup* (p. 831)		
BatchGetDeploymentInstances	배포 그룹의 일부인 하나 이상의 인스턴스에 대한 정보를 가져옵니다.	Read	deploymentgroup* (p. 831)		
BatchGetDeploymentTargets	배포와 연결된 하나 이상의 대상에 대한 배열을 반환합니다. 이 메서드는 모든 컴퓨팅 유형에서 작동하며, 사용되지 않는	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	atchGetDeploymentInstances 대신에 사용해야 합니다. 반환할 수 있는 최대 대상 수는 25개입니다.				
BatchGetDeploymentGroups	IAM 사용자와 연결된 여러 배포에 대한 정보를 가져옵니다.	Read	deploymentgroup* (p. 831)		
BatchGetOnPremisesInstances	하나 이상의 온프레미스 인스턴스에 대한 정보를 가져옵니다.	Read	instance* (p. 831)		
ContinueDeployment	지정된 경과 시간을 기다리지 않고 원본 환경의 인스턴스로부터 트래픽을 대체 환경의 인스턴스로 다시 라우팅하는 프로세스를 시작합니다.	쓰기			
CreateApplication	IAM 사용자와 연결된 애플리케이션을 만듭니다.	쓰기	application* (p. 831)		
				aws:RequestTag/${TagKey} (p. 831) aws:TagKeys (p. 831)	
CreateDeployment	IAM 사용자와 연결된 애플리케이션에 대한 배포를 만듭니다.	쓰기	deploymentgroup* (p. 831)		
CreateDeploymentConfig	IAM 사용자와 연결된 사용자 지정 배포 구성을 만듭니다.	쓰기	deploymentconfig* (p. 831)		
CreateDeploymentGroup	IAM 사용자와 연결된 애플리케이션에 대한 배포 그룹을 만듭니다.	쓰기	deploymentgroup* (p. 831)		
				aws:RequestTag/${TagKey} (p. 831) aws:TagKeys (p. 831)	
DeleteApplication	IAM 사용자와 연결된 애플리케이션을 삭제합니다.	쓰기	application* (p. 831)		
DeleteDeploymentConfig	IAM 사용자와 연결된 사용자 지정 배포 구성을 삭제합니다.	쓰기	deploymentconfig* (p. 831)		
DeleteDeploymentGroup	IAM 사용자와 연결된 애플리케이션에 대한 배포 그룹을 삭제합니다.	쓰기	deploymentgroup* (p. 831)		
DeleteGitHubAccountToken	GitHub 계정 연결을 삭제합니다.	쓰기			
DeregisterOnPremisesInstance	온프레미스 인스턴스 등록을 취소합니다.	쓰기	instance* (p. 831)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetApplication	IAM 사용자와 연결된 단일 애플리케이션에 대한 정보를 가져옵니다.	List	application* (p. 831)		
GetApplicationRevision	IAM 사용자와 연결된 애플리케이션의 단일 애플리케이션 개정에 대한 정보를 가져옵니다.	List	application* (p. 831)		
GetDeployment	IAM 사용자와 연결된 애플리케이션의 배포 그룹에 대한 단일 배포에 대한 정보를 가져옵니다.	List	deploymentgroup* (p. 831)		
GetDeploymentConfig	IAM 사용자와 연결된 단일 배포 구성에 대한 정보를 가져옵니다.	List	deploymentconfig* (p. 831)		
GetDeploymentGroup	IAM 사용자와 연결된 애플리케이션의 단일 배포 그룹에 대한 정보를 가져옵니다.	List	deploymentgroup* (p. 831)		
GetDeploymentInstance	IAM 사용자와 연결된 배포의 단일 인스턴스에 대한 정보를 가져옵니다.	List	deploymentgroup* (p. 831)		
GetDeploymentTarget	배포 대상에 대한 정보를 반환합니다.	Read			
GetOnPremisesInstance	단일 온프레미스 인스턴스에 대한 정보를 가져옵니다.	List	instance* (p. 831)		
ListApplicationRevisions	IAM 사용자와 연결된 애플리케이션의 모든 애플리케이션 개정에 대한 정보를 가져옵니다.	List	application* (p. 831)		
ListApplications	IAM 사용자와 연결된 모든 애플리케이션에 대한 정보를 가져옵니다.	List			
ListDeploymentConfigs	IAM 사용자와 연결된 모든 배포 구성에 대한 정보를 가져옵니다.	List			
ListDeploymentGroups	IAM 사용자와 연결된 애플리케이션의 모든 배포 그룹에 대한 정보를 가져옵니다.	List	application* (p. 831)		
ListDeploymentInstances	IAM 사용자와 연결된 배포의 모든 인스턴스에 대한 정보를 가져옵니다.	List	deploymentgroup* (p. 831)		
ListDeploymentTargets	배포와 연결된 대상 ID의 배열을 반환합니다.	List			
ListDeployments	IAM 사용자와 연결된 배포 그룹에 대한 모든 배포의 정보를 가져오거나 IAM 사용자와 연결된 모든 배포를 가져옵니다.	List	deploymentgroup* (p. 831)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListGitHubAccountTokenNames	GitHub 계정에 대해 저장된 연결의 이름을 나열합니다.	List			
ListOnPremisesInstances	하나 이상의 온프레미스 인스턴스 이름의 목록을 가져옵니다.	List			
ListTagsForResource	지정된 ARN으로 식별된 리소스에 대한 태그 목록을 반환합니다. 태그는 CodeDeploy 리소스를 구성하고 분류하는 데 사용됩니다.	List	application (p. 831)		
			deploymentgroup (p. 831)		
PutLifecycleEventHookExecutionStatus	IAM 사용자와 연결된 배포에 대한 수명 주기 이벤트 훅 실행 상태를 알립니다.	쓰기			
RegisterApplicationRevision	IAM 사용자와 연결된 애플리케이션의 애플리케이션 개정에 대한 정보를 등록합니다.	쓰기	application* (p. 831)		
RegisterOnPremisesInstance	온프레미스 인스턴스를 등록합니다.	쓰기	instance* (p. 831)		
RemoveTagsFromOnPremisesInstances	하나 이상의 온프레미스 인스턴스에서 태그를 제거합니다.	태그 지정	instance* (p. 831)		
SkipWaitTimeForInstanceTermination	파란색/녹색 배포에서는 지정된 대기 시간을 무시하고 트래픽 라우팅이 완료된 직후 인스턴스 종료를 시작합니다.	쓰기			
StopDeployment	StopDeployment에 대한 설명	쓰기			
TagResource	입력 Tags 파라미터의 태그 목록을 ResourceArn 입력 파라미터로 식별되는 리소스와 연결합니다.	태그 지정	application (p. 831)		
			deploymentgroup (p. 831)		
				aws:RequestTag/${TagKey} (p. 831) aws:TagKeys (p. 831)	
UntagResource	태그 목록에서 리소스의 연결을 해제합니다. 리소스는 ResourceArn 입력 파라미터로 식별됩니다. 태그는 TagKeys 입력 파라미터의 키 목록으로 식별됩니다.	태그 지정	application (p. 831)		
			deploymentgroup (p. 831)		
				aws:TagKeys (p. 831)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateApplication	UpdateApplication에 대한 설명	쓰기	application* (p. 831)		
UpdateDeploymentGroup	IAM 사용자와 연결된 애플리케이션와 단일 배포 그룹에 대한 정보를 변경합니다.	쓰기	deploymentgroup* (p. 831)		

AWS CodeDeploy에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 827)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
application	`arn:${Partition}:codedeploy:${Region}:${Account}:application:${ApplicationName}`	
deploymentconfig	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentconfig:${DeploymentConfigurationName}`	
deploymentgroup	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentgroup:${ApplicationName}/${DeploymentGroupName}`	
instance	`arn:${Partition}:codedeploy:${Region}:${Account}:instance:${InstanceName}`	

AWS CodeDeploy에 사용되는 조건 키

AWS CodeDeploy는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon CodeGuru에 사용되는 작업, 리소스 및 조건 키

Amazon CodeGuru(서비스 접두사: `codeguru`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon CodeGuru에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetCodeGuruFreeTrialSummary [권한만 해당]	만료 날짜를 포함하는 CodeGuru 서비스에 대한 무료 평가판 요약을 가져옵니다.	Read			

Amazon CodeGuru에서 정의한 리소스 유형

Amazon CodeGuru는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon CodeGuru에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon CodeGuru에 사용되는 조건 키

CodeGuru에는 정책 문의 `Condition` 요소에서 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon CodeGuru 프로파일러에 대한 작업, 리소스 및 조건 키

Amazon CodeGuru 프로파일러(서비스 접두사: `codeguru-profiler`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon CodeGuru 프로파일러에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ConfigureAgent [권한만 해당]	에이전트가 오케스트레이션 서비스에 등록하고 프로파일링 구성 정보를 검색할 수 있는 권한을 부여합니다.	쓰기	ProfilingGroup* (p. 834)		
CreateProfilingGroup	프로파일링 그룹을 만들 수 있는 권한을 부여합니다.	쓰기	ProfilingGroup* (p. 834)		
DeleteProfilingGroup	프로파일링 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	ProfilingGroup* (p. 834)		
DescribeProfilingGroup	프로파일링 그룹을 설명할 수 있는 권한을 부여합니다.	Read	ProfilingGroup* (p. 834)		
GetFindingsReport	권장 사항 보고서를 가져올 수 있는 권한을 부여합니다.	Read	ProfilingGroup* (p. 834)		
GetFindingsReportAccountSummary	계정의 각 프로파일링 그룹에 대한 최근 권장 사항의 요약을 가져올 수 있는 권한을 부여합니다.	Read			
GetPolicy	지정된 프로파일링 그룹과 연결된 리소스 정책을 가져올 권한을 부여합니다.	Read	ProfilingGroup* (p. 834)		
GetProfile	특정 프로파일링 그룹에 대해 집계된 프로파일을 가져올 수 있는 권한을 부여합니다.	Read	ProfilingGroup* (p. 834)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListFindingsReports	특정 프로파일링 그룹에 대해 사용 가능한 권장 사항 보고서를 나열할 수 있는 권한을 부여합니다.	List	ProfilingGroup* (p. 834)		
ListProfileTimes	특정 프로파일링 그룹에 대해 사용 가능한 집계된 프로파일의 시작 시간을 나열할 수 있는 권한을 부여합니다.	List	ProfilingGroup* (p. 834)		
ListProfilingGroups	계정의 프로파일링 그룹을 나열할 수 있는 권한을 부여합니다.	List			
PostAgentProfile [권한만 해당]	집계를 위해 특정 프로파일링 그룹에 속한 에이전트가 수집한 프로파일을 제출할 수 있는 권한을 부여합니다.	쓰기	ProfilingGroup* (p. 834)		
PutPermission	지정된 프로파일링 그룹과 연결된 리소스 정책에서 작업 그룹에 허용된 보안 주체의 목록을 업데이트할 수 있는 권한을 부여합니다.	권한 관리	ProfilingGroup* (p. 834)		
RemovePermission	지정된 프로파일링 그룹과 연결된 리소스 정책에서 지정된 작업 그룹의 권한을 제거할 수 있는 권한을 부여합니다.	권한 관리	ProfilingGroup* (p. 834)		
UpdateProfilingGroup	특정 프로파일링 그룹을 업데이트할 수 있는 권한을 부여합니다.	쓰기	ProfilingGroup* (p. 834)		

Amazon CodeGuru 프로파일러에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 833)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
ProfilingGroup	`arn:${Partition}:codeguru-profiler:${Region}:${Account}:profilingGroup/${profilingGroupName}`	

Amazon CodeGuru 프로파일러에 대한 조건 키

CodeGuru 프로파일러에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon CodeGuru 검토자의 작업, 리소스 및 조건 키

Amazon CodeGuru 검토자(서비스 접두사: `codeguru-reviewer`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon CodeGuru 검토자에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateRepository	리포지토리를 Amazon CodeGuru 검토자와 연결할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 836)		codecommit:ListRepositor codecommit:TagResource events:PutRule events:PutTargets iam:CreateServiceLinkedI
CreateConnectionToken [권한만 해당]	타사 공급자에 대한 웹 기반 oauth 핸드셰이크를 수행할 수 있는 권한을 부여합니다.	Read			
DescribeRepositoryAssociation	리포지토리 연결을 설명할 수 있는 권한을 부여합니다.	Read			
DisassociateRepository	Amazon CodeGuru 검토자와 리포지토리의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기	association* (p. 836)		codecommit:UntagResour events:DeleteRule events:RemoveTargets
GetMetricsData [권한만 해당]	콘솔에서 풀 요청 지표를 볼 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListRepositoryAssociations	리포지토리 연결 요약을 나열할 수 있는 권한을 부여합니다.	List			
ListThirdPartyRepositories [권한만 해당]	콘솔에서 타사 공급자 리포지토리를 나열할 수 있는 권한을 부여합니다.	Read			

Amazon CodeGuru 검토자에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 835)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
association	`arn:${Partition}:codeguru-reviewer::${Account}:association:${ResourceId}`	
repository	`arn:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}`	aws:ResourceTag/${TagKey} (p. 836)

Amazon CodeGuru 검토자의 조건 키

Amazon CodeGuru 검토자는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열

AWS CodePipeline에 사용되는 작업, 리소스 및 조건 키

AWS CodePipeline(서비스 접두사: `codepipeline`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CodePipeline에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcknowledgeJob	지정된 작업에 대한 정보를 보고 작업자가 해당 작업을 받았는지 여부를 확인할 수 있는 권한을 부여합니다.	쓰기			
AcknowledgeThirdPartyJob	작업자가 지정된 작업을 받았는지 확인할 수 있는 권한을 부여합니다(파트너 작업만 해당).	쓰기			
CreateCustomActionType	AWS 계정과 연결된 파이프라인에서 사용할 수 있는 사용자 지정 작업을 생성할 수 있는 권한을 부여합니다.	태그 지정	actiontype* (p. 841)		
				aws:RequestTag/${TagKey} (p. 841) aws:TagKeys (p. 841)	
CreatePipeline	고유한 이름의 파이프라인을 생성할 수 있는 권한을 부여합니다.	태그 지정	pipeline* (p. 841)		
				aws:RequestTag/${TagKey} (p. 841) aws:TagKeys (p. 841)	
DeleteCustomActionType	사용자 지정 작업을 삭제할 수 있는 권한을 부여합니다.	쓰기	actiontype* (p. 841)		
DeletePipeline	지정된 파이프라인을 삭제할 수 있는 권한을 부여합니다.	쓰기	pipeline* (p. 841)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteWebhook	지정된 Webhook을 삭제할 수 있는 권한을 부여합니다.	쓰기	webhook* (p. 841)		
DeregisterWebhookWithThirdParty	해당 구성에 지정된 타사 Webhook 등록을 제거할 수 있는 권한을 부여합니다.	쓰기	webhook* (p. 841)		
DisableStageTransition	개정이 파이프라인의 다음 단계로 전환하지 않도록 방지할 수 있는 권한을 부여합니다.	쓰기	stage* (p. 841)		
EnableStageTransition	개정을 파이프라인의 다음 단계로 전환할 수 있는 권한을 부여합니다.	쓰기	stage* (p. 841)		
GetJobDetails	작업에 대한 정보를 볼 수 있는 권한을 부여합니다(사용자 정의 작업에만 해당).	Read			
GetPipeline	파이프라인 구조에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	pipeline* (p. 841)		
GetPipelineExecution	아티팩트의 세부 정보, 파이프라인 실행 ID, 파이프라인의 이름과 버전 및 상태 등 파이프라인 실행에 대한 정보를 확인할 수 있는 권한을 부여합니다.	Read	pipeline* (p. 841)		
GetPipelineState	파이프라인의 단계 및 작업의 현재 상태에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read	pipeline* (p. 841)		
GetThirdPartyJobDetails	타사 작업에 대한 작업 세부 정보를 볼 수 있는 권한을 부여합니다(파트너 작업에만 해당).	Read			
ListActionExecutions	파이프라인에서 발생한 작업 실행을 나열할 수 있는 권한을 부여합니다.	Read	pipeline* (p. 841)		
ListActionTypes	계정의 파이프라인에 사용할 수 있는 모든 작업 유형의 요약을 나열할 수 있는 권한을 부여합니다.	Read	actiontype* (p. 841)		
ListPipelineExecutions	파이프라인의 가장 최근 실행에 대한 요약을 나열할 수 있는 권한을 부여합니다.	List	pipeline* (p. 841)		
ListPipelines	AWS 계정과 연결된 모든 파이프라인의 요약을 나열할 수 있는 권한을 부여합니다.	List	pipeline* (p. 841)		
ListTagsForResource	CodePipeline 리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	actiontype (p. 841)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			pipeline (p. 841)		
			webhook (p. 841)		
ListWebhooks	AWS 계정과 연결된 모든 Webhook을 나열할 수 있는 권한을 부여합니다.	List	webhook* (p. 841)		
PollForJobs	CodePipeline이 작동할 작업에 대한 정보를 볼 수 있는 권한을 부여합니다.	쓰기	actiontype* (p. 841)		
PollForThirdPartyJobs	작업자가 작업할 타사 작업이 있는지 확인할 수 있는 권한을 부여합니다(파트너 작업에만 해당).	쓰기			
PutActionRevision	파이프라인에서 작업을 편집할 수 있는 권한을 부여합니다.	쓰기	action* (p. 841)		
PutApprovalResult	CodePipeline의 수동 승인 요청에 대한 응답(승인됨 또는 거부됨)을 제공할 수 있는 권한을 부여합니다.	쓰기	action* (p. 841)		
PutJobFailureResult	작업자가 파이프라인으로 반환한 작업의 실패를 나타낼 수 있는 권한을 부여합니다(사용자 지정 작업에만 해당).	쓰기			
PutJobSuccessResult	작업자가 파이프라인으로 반환한 작업의 성공을 나타낼 수 있는 권한을 부여합니다(사용자 지정 작업에만 해당).	쓰기			
PutThirdPartyJobFailureResult	작업자가 파이프라인으로 반환한 타사 작업의 실패를 나타낼 수 있는 권한을 부여합니다(파트너 작업에만 해당).	쓰기			
PutThirdPartyJobSuccessResult	작업자가 파이프라인으로 반환한 타사 작업의 성공을 나타낼 수 있는 권한을 부여합니다(파트너 작업에만 해당).	쓰기			
PutWebhook	Webhook을 생성하거나 업데이트할 수 있는 권한을 부여합니다.	태그 지정	pipeline* (p. 841)		
			webhook* (p. 841)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 841) aws:TagKeys (p. 841)	
RegisterWebhookWithThirdParty	구성에 지정된 타사에 Webhook을 등록할 수 있는 권한을 부여합니다.	쓰기	webhook* (p. 841)		
RetryStageExecution	단계에서 마지막으로 실패한 작업을 재시도함으로써 파이프라인 실행을 재개할 수 있는 권한을 부여합니다.	쓰기	stage* (p. 841)		
StartPipelineExecution	파이프라인을 통해 최신 개정을 실행할 수 있는 권한을 부여합니다.	쓰기	pipeline* (p. 841)		
StopPipelineExecution	진행 중인 파이프라인 실행을 중지할 수 있는 권한을 부여합니다.	쓰기	pipeline* (p. 841)		
TagResource	CodePipeline 리소스에 태그를 지정할 수 있는 권한을 부여합니다.	태그 지정	actiontype (p. 841)		
			pipeline (p. 841)		
			webhook (p. 841)		
				aws:RequestTag/${TagKey} (p. 841) aws:TagKeys (p. 841)	
UntagResource	CodePipeline 리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	actiontype (p. 841)		
			pipeline (p. 841)		
			webhook (p. 841)		
				aws:TagKeys (p. 841)	
UpdatePipeline	파이프라인의 구조에 대한 변경으로 파이프라인을 업데이트할 수 있는 권한을 부여합니다.	쓰기	pipeline* (p. 841)		

AWS CodePipeline에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 837)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
action	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}/${ActionName}`	aws:ResourceTag/${TagKey} (p. 841)
actiontype	`arn:${Partition}:codepipeline:${Region}:${Account}:actiontype:${Owner}/${Category}/${Provider}/${Version}`	aws:ResourceTag/${TagKey} (p. 841)
pipeline	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}`	aws:ResourceTag/${TagKey} (p. 841)
stage	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}`	aws:ResourceTag/${TagKey} (p. 841)
webhook	`arn:${Partition}:codepipeline:${Region}:${Account}:webhook:${WebhookName}`	aws:ResourceTag/${TagKey} (p. 841)

AWS CodePipeline의 조건 키

AWS CodePipeline은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS CodeStar에 사용되는 작업, 리소스 및 조건 키

AWS CodeStar(서비스 접두사: `codestar`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CodeStar에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateTeamMember	AWS CodeStar 프로젝트의 팀에 사용자를 추가합니다.	권한 관리	project* (p. 844)		
CreateProject	리소스 없이 최소한의 구조 및 고객 정책으로 프로젝트를 생성합니다.	권한 관리		aws:RequestTag/${TagKey} (p. 844) aws:TagKeys (p. 844)	
CreateUserProfile	사용자 기본 설정, 표시 이름 및 이메일이 포함된 사용자의 프로필을 생성합니다.	쓰기	user* (p. 844)		
DeleteExtendedAccess [권한만 해당]	확장된 삭제 API에 대한 액세스 권한을 부여합니다.	쓰기	project* (p. 844)		
DeleteProject	프로젝트 리소스를 포함하여 프로젝트를 삭제합니다. 프로젝트와 연결된 사용자는 삭제하지 말고, 프로젝트에 대한 액세스를 허용한 IAM 역할을 삭제합니다.	권한 관리	project* (p. 844)		
DeleteUserProfile	표시 이름 및 이메일 주소와 같은 해당 프로필과 연결된 모든 개인 기본 설정 데이터를 포함하여, AWS CodeStar에서 사용자 프로필을 삭제합니다. 이렇게 해도 해당 사용자의 기록(예: 해당 사용자	쓰기	user* (p. 844)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	가 수행한 커밋 이력)은 삭제되지 않습니다.				
DescribeProject	프로젝트 및 해당 리소스에 대해 설명합니다.	Read	project* (p. 844)		
DescribeUserProfile	AWS CodeStar에 속한 사용자 및 모든 프로젝트에서 해당 사용자 속성을 설명합니다.	Read			
DisassociateTeamMember	프로젝트에서 사용자를 제거합니다. 프로젝트에서 사용자를 제거하면 프로젝트 및 해당 리소스에 액세스를 허용한 사용자의 IAM 정책 또한 제거됩니다.	권한 관리	project* (p. 844)		
GetExtendedAccess [권한만 해당]	확장된 읽기 API에 대한 액세스 권한을 부여합니다.	Read	project* (p. 844)		
ListProjects	AWS 계정과 연결된 CodeStar의 모든 프로젝트를 나열합니다.	List			
ListResources	CodeStar의 프로젝트와 연결된 모든 리소스를 나열합니다.	List	project* (p. 844)		
ListTagsForProject	CodeStar의 프로젝트와 연결된 태그를 나열합니다.	List	project* (p. 844)		
ListTeamMembers	프로젝트와 연결된 모든 팀원을 나열합니다.	List	project* (p. 844)		
ListUserProfiles	AWS CodeStar 내 사용자 프로필을 나열합니다.	List			
PutExtendedAccess [권한만 해당]	확장된 쓰기 API에 대한 액세스 권한을 부여합니다.	쓰기	project* (p. 844)		
TagProject	CodeStar의 프로젝트에 태그를 추가합니다.	태그 지정	project* (p. 844)		
				aws:RequestTag/${TagKey} (p. 844) aws:TagKeys (p. 844)	
UntagProject	CodeStar의 프로젝트에서 태그를 제거합니다.	태그 지정	project* (p. 844)		
				aws:TagKeys (p. 844)	
UpdateProject	CodeStar에서 프로젝트를 업데이트합니다.	쓰기	project* (p. 844)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateTeamMember	CodeStar 프로젝트 내 팀원 속성을 업데이트합니다.	권한 관리	project* (p. 844)		
UpdateUserProfile	사용자 기본 설정, 표시 이름 및 이메일이 포함된 사용자의 프로필을 업데이트합니다.	쓰기	user* (p. 844)		

AWS CodeStar에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 842)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
project	`arn:${Partition}:codestar:${Region}:${Account}:project/${ProjectId}`	aws:ResourceTag/${TagKey} (p. 844)
user	`arn:${Partition}:iam::${Account}:user/${aws:username}`	iam:ResourceTag/${TagKey} (p. 844)

AWS CodeStar에 사용되는 조건 키

AWS CodeStar는 `Condition` 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열
iam:ResourceTag/${TagKey}		문자열

AWS CodeStar 알림에 사용되는 작업, 리소스 및 조건 키

AWS CodeStar 알림(서비스 접두사: `codestar-notifications`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS CodeStar 알림에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateNotificationRule	리소스에 대한 알림 규칙을 생성할 수 있는 권한을 부여합니다.	쓰기	notificationrule* (p. 848)		
				aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848) codestar-notifications:NotificationsForResource (p. 849)	
DeleteNotificationRule	리소스에 대한 알림 규칙을 삭제할 수 있는 권한을 부여합니다.	쓰기	notificationrule* (p. 848)		
				aws:ResourceTag/${TagKey} (p. 848) aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				codestar-notifications:NotificationsForResource (p. 849)	
DeleteTarget	알림 규칙에 대한 대상을 삭제할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848)	
DescribeNotificationRule	알림 규칙에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	notificationrule* (p. 848)		
				aws:ResourceTag/${TagKey} (p. 848) aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848) codestar-notifications:NotificationsForResource (p. 849)	
ListEventTypes	알림 이벤트 유형을 나열할 수 있는 권한을 부여합니다.	List			
ListNotificationRules	AWS 계정의 알림 규칙을 나열할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	알림 규칙 리소스 ARN에 연결된 태그를 나열할 수 있는 권한을 부여합니다.	List	notificationrule* (p. 848)		
				aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848)	
ListTargets	AWS 계정에 대한 알림 규칙 대상을 나열할 수 있는 권한을 부여합니다.	List		aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848)	
Subscribe	알림 규칙과 Amazon SNS 주제 간의 연결을 생성할 수 있는 권한을 부여합니다.	쓰기	notificationrule* (p. 848)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:ResourceTag/${TagKey} (p. 848) aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848) codestar-notifications:NotificationsForResource (p. 849)	
TagResource	알림 규칙 리소스 ARN에 리소스 태그를 연결할 수 있는 권한을 부여합니다.	태그 지정	notificationrule* (p. 848)		
				aws:ResourceTag/${TagKey} (p. 848) aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848)	
Unsubscribe	알림 규칙과 Amazon SNS 주제 간의 연결을 제거할 수 있는 권한을 부여합니다.	쓰기	notificationrule* (p. 848)		
				aws:ResourceTag/${TagKey} (p. 848) aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848) codestar-notifications:NotificationsForResource (p. 849)	
UntagResource	알림 규칙 리소스 ARN에서 리소스 태그의 연결을 해제할 수 있는 권한을 부여합니다.	태그 지정	notificationrule* (p. 848)		
				aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateNotificationRule	리소스에 대한 알림 규칙을 변경할 수 있는 권한을 부여합니다.	쓰기	notificationrule* (p. 848)		
				aws:ResourceTag/${TagKey} (p. 848) aws:RequestTag/${TagKey} (p. 848) aws:TagKeys (p. 848) codestar-notifications:NotificationsForResource (p. 849)	

AWS CodeStar Notifications에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 845)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
notificationrule	`arn:${Partition}:codestar-notifications:${Region}:${Account}:notificationrule/${NotificationRuleId}`	aws:ResourceTag/${TagKey} (p. 848)

AWS CodeStar 알림에 사용되는 조건 키

AWS CodeStar 알림은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
codestar-notifications:NotificationsForResource	알림이 구성된 리소스의 ARN을 기준으로 액세스를 필터링합니다.	ARN

Amazon Cognito Identity에 사용되는 작업, 리소스 및 조건 키

Amazon Cognito Identity(서비스 접두사: `cognito-identity`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Cognito Identity에서 정의한 작업 (p. 849)
- Amazon Cognito Identity에서 정의한 리소스 유형 (p. 851)
- Amazon Cognito Identity에 사용되는 조건 키 (p. 852)

Amazon Cognito Identity에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateIdentityPool	새 자격 증명 풀을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 852) aws:TagKeys (p. 852) aws:ResourceTag/${TagKey} (p. 852)	
DeleteIdentities	자격 증명 풀에서 자격 증명을 삭제합니다. 삭제하려는 자격 증명	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	을 1-60개까지 지정할 수 있습니다.				
DeleteIdentityPool	사용자 풀을 삭제합니다. 풀이 삭제된 후에는 사용자가 풀을 사용하여 인증할 수 없습니다.	쓰기	identitypool* (p. 852)		
DescribeIdentity	자격 증명이 생성된 시기 및 연결된 로그인(있는 경우)을 포함하여 주어진 자격 증명에 관련된 메타데이터를 반환합니다.	Read			
DescribeIdentityPool	풀 이름, ID 설명, 생성일 및 현재 사용자 수를 포함하여 특정 자격 증명 풀에 대한 세부 정보를 가져옵니다.	Read	identitypool* (p. 852)		
GetCredentialsForIdentity	제공된 자격 증명 ID에 대한 자격 증명을 반환합니다.	Read			
GetId	Cognito ID를 생성합니다(또는 검색합니다). 여러 개의 로그인을 제공하면 묵시적인 연결된 계정을 생성합니다.	쓰기			
GetIdentityPoolRoles	자격 증명 풀을 위한 역할을 가져옵니다.	Read	identitypool* (p. 852)		
GetOpenIdToken	알려진 Cognito ID를 사용하여 OpenID 토큰을 가져옵니다.	Read			
GetOpenIdTokenForDeveloperIdentity	백엔드 인증 프로세스에 의해 인증된 사용자에 대한 Cognito IdentityId 및 OpenID Connect 토큰을 등록하거나 검색합니다.	Read	identitypool* (p. 852)		
ListIdentities	풀에 있는 자격 증명을 나열합니다.	List	identitypool* (p. 852)		
ListIdentityPools	계정에 대하여 등록된 Cognito 자격 증명 풀을 모두 나열합니다.	List			
ListTagsForResource	Amazon Cognito 자격 증명 풀에 할당된 태그를 나열합니다.	List	identitypool (p. 852)		
				aws:ResourceTag/${TagKey} (p. 852)	
LookupDeveloperIdentity	DeveloperUserIdentifier와 연결된 IdentityID 또는 기존 자격 증명에 대한 IdentityId와 연결된 DeveloperUserIdentifiers의 목록을 검색합니다.	Read	identitypool* (p. 852)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
MergeDeveloperIdentities	서로 다른 IdentityId를 소유하면서 동일한 자격 증명 풀에 존재하고 동일한 개발자 공급자로 식별되며 두 사용자를 병합합니다.	쓰기	identitypool* (p. 852)		
SetIdentityPoolRoles	자격 증명 풀을 위한 역할을 설정합니다. 이러한 역할은 GetCredentialsForIdentity 작업을 호출할 때 사용됩니다.	쓰기			
TagResource	Amazon Cognito 자격 증명 풀에 태그 집합을 할당합니다.	태그 지정	identitypool (p. 852)		
				aws:RequestTag/${TagKey} (p. 852) aws:TagKeys (p. 852) aws:ResourceTag/${TagKey} (p. 852)	
UnlinkDeveloperIdentity	기존 자격 증명에서 DeveloperUserIdentifier를 링크 해제합니다.	쓰기	identitypool* (p. 852)		
UnlinkIdentity	기존 계정에서 연동 자격 증명을 링크 해제합니다.	쓰기			
UntagResource	Amazon Cognito 자격 증명 풀에서 지정된 태그를 제거합니다.	태그 지정	identitypool (p. 852)		
				aws:TagKeys (p. 852) aws:ResourceTag/${TagKey} (p. 852)	
UpdateIdentityPool	사용자 풀을 업데이트합니다.	쓰기	identitypool* (p. 852)		

Amazon Cognito Identity에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 849)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
identitypool	`arn:${Partition}:cognito-identity:${Region}:${Account}:identitypool/${IdentityPoolId}`	aws:ResourceTag/${TagKey} (p. 852)

Amazon Cognito Identity에 사용되는 조건 키

Amazon Cognito Identity는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 포함된 키를 기준으로 액세스를 필터링합니다.	문자열

Amazon Cognito Sync에 사용되는 작업, 리소스 및 조건 키

Amazon Cognito Sync(서비스 접두사: `cognito-sync`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Cognito Sync에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있

으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BulkPublish	구성된 스트림에 대한 자격 증명 풀의 모든 기존 데이터 세트의 대량 게시를 시작합니다.	쓰기	identitypool* (p. 854)		
DeleteDataset	지정된 데이터 세트를 삭제합니다.	쓰기	dataset* (p. 854)		
DescribeDataset	자격 증명 및 데이터 세트 이름을 기준으로 데이터세트에 대한 메타데이터를 가져옵니다.	Read	dataset* (p. 854)		
DescribeIdentityPoolUsage	특정 자격 증명 풀에 대한 사용량 세부 정보(에: 데이터 스토리지)를 가져옵니다.	Read	identitypool* (p. 854)		
DescribeIdentityUsage	데이터 세트 수 및 데이터 사용량을 포함한 자격 증명에 대한 사용량 정보를 가져옵니다.	Read	identity* (p. 854)		
GetBulkPublishDetails	자격 증명 풀의 마지막 BulkPublish 작업의 상태를 가져옵니다.	Read	identitypool* (p. 854)		
GetCognitoEvents	자격 증명 풀과 연결된 이벤트 및 해당 Lambda 함수를 가져옵니다.	Read	identitypool* (p. 854)		
GetIdentityPoolConfiguration	자격 증명 풀의 구성 설정을 가져옵니다.	Read	identitypool* (p. 854)		
ListDatasets	자격 증명에 대한 데이터 세트를 나열합니다.	List	dataset* (p. 854)		
ListIdentityPoolUsage	Cognito에 등록된 자격 증명 풀의 목록을 가져옵니다.	Read	identitypool* (p. 854)		
ListRecords	데이터 세트 및 자격 증명에 대한 특정 동기화 수 이후에 선택적으로 변경된 페이지 매김 레코드를 가져옵니다.	Read	dataset* (p. 854)		
QueryRecords [권한만 해당]	레코드에 쿼리할 수 있도록 부여하는 권한	Read			
RegisterDevice	푸시 동기화 알림을 받을 장치를 등록합니다.	쓰기	identity* (p. 854)		
SetCognitoEvents	자격 증명 풀에 대해 지정된 이벤트 유형에 대한 AWS Lambda 함수를 설정합니다.	쓰기	identitypool* (p. 854)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SetDatasetConfiguration [권한만 해당]	데이터 세트를 구성할 수 있도록 부여하는 권한	쓰기	dataset* (p. 854)		
SetIdentityPoolConfiguration	푸시 동기화에 필요한 구성을 설정합니다.	쓰기	identitypool* (p. 854)		
SubscribeToDataset	데이터 세트가 다른 장치에 의해 수정된 경우 알림을 받도록 신청합니다.	쓰기	dataset* (p. 854)		
UnsubscribeFromDataset	데이터 세트가 다른 장치에 의해 수정된 경우 알림을 받는 신청을 취소합니다.	쓰기	dataset* (p. 854)		
UpdateRecords	레코드에 대한 업데이트를 게시하고 데이터 세트 및 사용자에 대한 레코드를 삭제합니다.	쓰기	dataset* (p. 854)		

Amazon Cognito Sync에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 852)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
dataset	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}/dataset/${DatasetName}`	
identity	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}`	
identitypool	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}`	

Amazon Cognito Sync에 사용되는 조건 키

Cognito Sync에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Cognito User Pools에 사용되는 작업, 리소스 및 조건 키

Amazon Cognito User Pools(서비스 접두사: `cognito-idp`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Cognito User Pools에서 정의한 작업 (p. 855)
- Amazon Cognito User Pools에서 정의한 리소스 유형 (p. 862)
- Amazon Cognito User Pools의 조건 키 (p. 862)

Amazon Cognito User Pools에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddCustomAttributes	사용자 풀 스키마에 추가 사용자 속성을 추가합니다.	쓰기	userpool* (p. 862)		
AdminAddUserToGroup	지정된 사용자를 지정된 그룹에 추가합니다.	쓰기	userpool* (p. 862)		
AdminConfirmSignUp	확인 코드를 사용하지 않고 사용자 등록을 관리자로 확인합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		
AdminCreateUser	지정된 사용자 풀에서 새 사용자를 생성하고 이메일 또는 전화(SMS)를 통해 환영 인사 메시지를 전송합니다.	쓰기	userpool* (p. 862)		
AdminDeleteUser	사용자를 관리자로 삭제합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		
AdminDeleteUserAttributes	사용자 풀에서 사용자 속성을 관리자로 삭제합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		
AdminDisableProviderForUser	사용자가 지정된 외부(SAML 또는 소셜) 자격 증명 공급자를 사용하여 로그인하는 것을 금지합니다.	쓰기	userpool* (p. 862)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AdminDisableUser	지정된 사용자를 관리자로 비활성화합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		
AdminEnableUser	지정된 사용자를 관리자로 활성화합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		
AdminForgetDevice	디바이스를 관리자로 잊어버립니다.	쓰기	userpool* (p. 862)		
AdminGetDevice	디바이스를 관리자로 가져옵니다.	Read	userpool* (p. 862)		
AdminGetUser	사용자 풀에서 사용자 이름을 기준으로 지정된 사용자를 관리자로 가져옵니다. 모든 사용자에게 적용됩니다.	Read	userpool* (p. 862)		
AdminInitiateAuth	사용자 풀의 사용자를 관리자로 인증합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		
AdminLinkProviderForUser	외부 자격 증명 공급자의 지정된 속성 이름 및 값에 따라 사용자 풀(DestinationUser)의 기존 사용자 계정을 기존 자격 증명 공급자(SourceUser)의 자격 증명에 연결합니다.	쓰기	userpool* (p. 862)		
AdminListDevices	디바이스를 관리자로 나열합니다.	List	userpool* (p. 862)		
AdminListGroupsForUser	사용자가 속한 그룹을 나열합니다.	List	userpool* (p. 862)		
AdminListUserAuthEvents	사용자에 대한 인증 이벤트를 나열합니다.	Read	userpool* (p. 862)		
AdminRemoveUserFromGroup	지정된 그룹에서 지정된 사용자를 제거합니다.	쓰기	userpool* (p. 862)		
AdminResetUserPassword	사용자 풀에서 지정된 사용자의 암호를 관리자로 재설정합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		
AdminRespondToAuthChallenge	관리자로 인증 문제에 응답합니다.	쓰기	userpool* (p. 862)		
AdminSetUserMFAPreference	사용자 풀의 사용자에 대한 MFA 기본 설정을 지정합니다.	쓰기	userpool* (p. 862)		
AdminSetUserPassword	사용자 풀에서 지정된 사용자의 암호를 관리자로 설정합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AdminSetUserSettings	지정된 사용자 이름에 대한 모든 사용자 설정을 지정합니다. 모든 사용자에게 적용됩니다.	쓰기	userpool* (p. 862)		
AdminUpdateAuthEventFeedback	사용자 인증 이벤트에 대한 피드백을 업데이트합니다.	쓰기	userpool* (p. 862)		
AdminUpdateDeviceStatus	디바이스 상태를 관리자로 업데이트합니다.	쓰기	userpool* (p. 862)		
AdminUpdateUserAttributes	개발자 속성을 포함하여 지정된 사용자의 속성을 관리자로 업데이트합니다.	쓰기	userpool* (p. 862)		
AdminUserGlobalSignOut	모든 디바이스에서 사용자를 관리자로 로그아웃합니다.	쓰기	userpool* (p. 862)		
AssociateSoftwareToken	사용자 계정에 대해 고유하게 생성된 공유 비밀 키 코드를 반환합니다.	쓰기			
ChangePassword	사용자 풀에서 지정된 사용자의 암호를 변경합니다.	쓰기			
ConfirmDevice	디바이스의 추적을 확인합니다. 이 API 호출은 디바이스 추적을 시작하는 호출입니다.	쓰기			
ConfirmForgotPassword	사용자가 확인 코드를 입력하여 잊어버린 암호를 재설정하도록 허용합니다.	쓰기			
ConfirmSignUp	사용자의 등록을 확인하고 이전 사용자의 기존 별칭을 처리합니다.	쓰기			
CreateGroup	지정된 사용자 풀에서 새 그룹을 생성합니다.	쓰기	userpool* (p. 862)		
CreateIdentityProvider	사용자 풀의 자격 증명 공급자를 생성합니다.	쓰기	userpool* (p. 862)		
CreateResourceServer	새로운 OAuth2.0 리소스 서버를 생성하고 여기에서 사용자 지정 범위를 정의합니다.	쓰기	userpool* (p. 862)		
CreateUserImportJob	사용자 가져오기 작업을 생성합니다.	쓰기	userpool* (p. 862)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateUserPool	새로운 Amazon Cognito 사용자 풀을 생성하고 풀에 대한 암호 정책을 설정합니다.	쓰기		aws:RequestTag/${TagKey} (p. 862) aws:TagKeys (p. 862) aws:ResourceTag/${TagKey} (p. 862)	
CreateUserPoolClient	사용자 풀 클라이언트를 생성합니다.	쓰기	userpool* (p. 862)		
CreateUserPoolDomain	사용자 풀의 새 도메인을 생성합니다.	쓰기	userpool* (p. 862)		
DeleteGroup	그룹을 삭제합니다. 현재 멤버가 없는 그룹만 삭제할 수 있습니다.	쓰기	userpool* (p. 862)		
DeleteIdentityProvider	사용자 풀의 자격 증명 공급자를 삭제합니다.	쓰기	userpool* (p. 862)		
DeleteResourceServer	리소스 서버를 삭제합니다.	쓰기	userpool* (p. 862)		
DeleteUser	사용자가 자신을 삭제하도록 허용합니다.	쓰기			
DeleteUserAttributes	사용자에 대한 속성을 삭제합니다.	쓰기			
DeleteUserPool	지정된 Amazon Cognito 사용자 풀을 삭제합니다.	쓰기	userpool* (p. 862)		
DeleteUserPoolClient	개발자가 사용자 풀 클라이언트를 삭제하도록 허용합니다.	쓰기	userpool* (p. 862)		
DeleteUserPoolDomain	사용자 풀의 도메인을 삭제합니다.	쓰기	userpool* (p. 862)		
DescribeIdentityProvider	특정 자격 증명 공급자에 대한 정보를 가져옵니다.	Read	userpool* (p. 862)		
DescribeResourceServer	리소스 서버를 설명합니다.	Read	userpool* (p. 862)		
DescribeRiskConfiguration	사용자 풀/사용자 풀 클라이언트에 대한 위험 구성 설정을 설명합니다.	Read	userpool* (p. 862)		
DescribeUserImportJob	사용자 가져오기 작업을 설명합니다.	Read	userpool* (p. 862)		
DescribeUserPool	지정된 사용자 풀의 구성 정보 및 메타데이터를 반환합니다.	Read	userpool* (p. 862)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeUserPoolClient	지정된 사용자 풀 클라이언트의 구성 정보 및 메타데이터를 반환하는 클라이언트 메서드입니다.	Read	userpool* (p. 862)		
DescribeUserPoolDomain	도메인에 대한 정보를 가져옵니다.	Read			
ForgetDevice	지정된 디바이스를 잊어버립니다.	쓰기			
ForgotPassword	이 API를 호출하면 사용자의 암호를 변경하는 데 필요한 확인 코드와 함께 최종 사용자에게 메시지가 전송됩니다.	쓰기			
GetCSVHeader	사용자 가져오기 작업에 대한 입력으로 사용할 .csv 파일의 헤더 정보를 가져옵니다.	Read	userpool* (p. 862)		
GetDevice	디바이스를 가져옵니다.	Read			
GetGroup	그룹을 가져옵니다.	Read	userpool* (p. 862)		
GetIdentityProviderByIdentifier	지정된 자격 증명 공급자를 가져옵니다.	Read	userpool* (p. 862)		
GetSigningCertificate	서명 인증서를 반환합니다.	Read	userpool* (p. 862)		
GetUICustomization	설정된 항목이 있을 경우, 특정 앱 클라이언트의 앱에 대한 UI 사용자 지정 정보를 가져옵니다.	Read	userpool* (p. 862)		
GetUser	사용자에 대한 사용자 속성 및 메타데이터를 가져옵니다.	Read			
GetUserAttributeVerificationCode	지정된 속성 이름에 대한 사용자 속성 확인 코드를 가져옵니다.	Read			
GetUserPoolMfaConfig	사용자 풀에 대한 MFA 구성을 가져옵니다.	Read	userpool* (p. 862)		
GlobalSignOut	모든 디바이스에서 사용자를 로그아웃합니다.	쓰기			
InitiateAuth	인증 흐름을 시작합니다.	쓰기			
ListDevices	디바이스를 나열합니다.	List			
ListGroups	사용자 풀과 연결된 그룹을 나열합니다.	List	userpool* (p. 862)		
ListIdentityProviders	사용자 풀의 모든 자격 증명 공급자에 대한 정보를 나열합니다.	List	userpool* (p. 862)		
ListResourceServers	사용자 풀의 리소스 서버를 나열합니다.	List	userpool* (p. 862)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTagsForResource	Amazon Cognito 사용자 풀에 할당된 태그를 나열합니다.	List	userpool (p. 862)		
ListUserImportJobs	사용자 가져오기 작업을 나열합니다.	List	userpool* (p. 862)		
ListUserPoolClients	지정된 사용자 풀에 대해 생성된 클라이언트를 나열합니다.	List	userpool* (p. 862)		
ListUserPools	AWS 계정과 연결된 사용자 풀을 나열합니다.	List			
ListUsers	Amazon Cognito 사용자 풀의 사용자를 나열합니다.	List	userpool* (p. 862)		
ListUsersInGroup	지정된 그룹의 사용자를 나열합니다.	List	userpool* (p. 862)		
ResendConfirmationCode	사용자 풀의 특정 사용자에게 확인(등록 확인용)을 재전송합니다.	쓰기			
RespondToAuthChallenge	인증 문제에 응답합니다.	쓰기			
SetRiskConfiguration	사용자 풀/사용자 풀 클라이언트에 대한 위험 구성 설정을 지정합니다.	쓰기	userpool* (p. 862)		
SetUICustomization	사용자 풀의 내장 앱 UI에 대한 UI 사용자 지정을 설정합니다.	쓰기	userpool* (p. 862)		
SetUserMFAPreference	사용자 풀의 사용자에 대한 MFA 기본 설정을 지정합니다.	쓰기			
SetUserPoolMfaConfig	사용자 풀에 대한 MFA 구성을 설정합니다.	쓰기	userpool* (p. 862)		
SetUserSettings	멀티 팩터 인증(MFA)과 같은 사용자 설정을 지정합니다.	쓰기			
SignUp	지정된 사용자 풀에 사용자를 등록하고 사용자 이름, 암호 및 사용자 속성을 생성합니다.	쓰기			
StartUserImportJob	사용자 가져오기를 시작합니다.	쓰기	userpool* (p. 862)		
StopUserImportJob	사용자 가져오기 작업을 중지합니다.	쓰기	userpool* (p. 862)		
TagResource	Amazon Cognito 사용자 풀에 태그 집합을 할당합니다.	태그 지정	userpool (p. 862)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 862) aws:TagKeys (p. 862)	
UntagResource	Amazon Cognito 사용자 풀에서 지정된 태그를 제거합니다.	태그 지정	userpool (p. 862)		
				aws:TagKeys (p. 862)	
UpdateAuthEventFeedback	사용자 인증 이벤트에 대한 피드백을 업데이트합니다.	쓰기	userpool* (p. 862)		
UpdateDeviceStatus	디바이스 상태를 업데이트합니다.	쓰기			
UpdateGroup	지정된 그룹을 지정된 속성으로 업데이트합니다.	쓰기	userpool* (p. 862)		
UpdateIdentityProvider	사용자 풀의 자격 증명 공급자 정보를 업데이트합니다.	쓰기	userpool* (p. 862)		
UpdateResourceServer	리소스 서버의 이름 및 범위를 업데이트합니다.	쓰기	userpool* (p. 862)		
UpdateUserAttributes	사용자가 특정 속성을 업데이트하도록 허용합니다(한 번에 하나씩).	쓰기			
UpdateUserPool	지정된 사용자 풀을 지정된 속성으로 업데이트합니다.	쓰기	userpool* (p. 862)		
				aws:RequestTag/${TagKey} (p. 862) aws:TagKeys (p. 862)	
UpdateUserPoolClient	개발자가 지정된 사용자 풀 클라이언트 및 암호 정책을 업데이트하도록 허용합니다.	쓰기	userpool* (p. 862)		
UpdateUserPoolDomain	사용자 풀의 사용자 지정 도메인에 대한 SSL(Secure Sockets Layer) 인증서를 업데이트합니다.	쓰기	userpool* (p. 862)		
VerifySoftwareToken	사용자가 입력한 TOTP 코드를 등록하고, 성공할 경우 사용자의 소프트웨어 토큰 MFA 상태를 확인됨으로 표시합니다.	쓰기			
VerifyUserAttribute	일회성 확인 코드를 사용하여 사용자 속성을 확인합니다.	쓰기			

Amazon Cognito User Pools에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 855)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
userpool	`arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}`	aws:ResourceTag/${TagKey} (p. 862)

Amazon Cognito User Pools의 조건 키

Amazon Cognito User Pools는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 포함된 키를 기준으로 액세스를 필터링합니다.	문자열

Amazon Comprehend에 사용되는 작업, 리소스 및 조건 키

Amazon Comprehend(서비스 접두사: `comprehend`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Comprehend에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchDetectDominantLanguage	텍스트 문서의 목록에 있는 언어를 감지합니다.	Read			
BatchDetectEntities	지정된 텍스트 문서의 목록 내에서 명명된 개체("People", "Places", "Locations" 등)를 감지합니다.	Read			
BatchDetectKeyPhrases	콘텐츠를 가장 잘 나타내는 텍스트 문서 목록의 구를 감지합니다.	Read			
BatchDetectSentiment	문서 목록에 있는 텍스트의 감정을 감지합니다(Positive, Negative, Neutral 또는 Mixed).	Read			
BatchDetectSyntax	텍스트 문서의 목록에서 구문 정보(예: 음성의 일부, 토큰)를 감지합니다.	Read			
ClassifyDocument	이전에 생성 및 훈련한 사용자 지정 모델과 엔드포인트를 사용하여 단일 문서를 실시간으로 분석하는 새 문서 분류 요청을 생성합니다.	Read	document-classifier-endpoint* (p. 867)		
CreateDocumentClassifier	문서를 범주화하는 데 사용할 수 있는 새 문서 분류자를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 867) aws:TagKeys (p. 868)	
CreateEndpoint	이전에 훈련된 사용자 지정 모델에 대한 동기식 추론을 위해 모델별 엔드포인트를 생성합니다.	쓰기	document-classifier (p. 867)		
				aws:RequestTag/${TagKey} (p. 867) aws:TagKeys (p. 868)	
CreateEntityRecognizer	제출된 파일을 사용하여 엔터티 인식기를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 867)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 868)	
DeleteDocumentClassifier	이전에 생성한 문서 분류자를 삭제합니다.	쓰기	document-classifier* (p. 867)		
DeleteEndpoint	이전에 훈련된 사용자 지정 모델에 대한 모델별 엔드포인트를 삭제합니다. 모델을 삭제하려면 모든 엔드포인트를 삭제해야 합니다.	쓰기	document-classifier-endpoint* (p. 867)		
DeleteEntityRecognizer	제출된 엔터티 인식기를 삭제합니다.	쓰기	entity-recognizer* (p. 867)		
DescribeDocumentClassificationJob	문서 분류 작업과 연결된 속성을 가져옵니다.	Read			
DescribeDocumentClassifier	문서 분류기와 연결된 속성을 가져옵니다.	Read	document-classifier* (p. 867)		
DescribeDominantLanguageDetectionJob	중심 언어 감지 작업과 관련된 속성을 가져옵니다.	Read			
DescribeEndpoint	특정 엔드포인트와 연결된 속성을 가져옵니다. 이 작업을 사용하여 엔드포인트의 상태를 가져옵니다.	Read	document-classifier-endpoint* (p. 867)		
DescribeEntitiesDetectionJob	엔터티 감지 작업과 연결된 속성을 가져옵니다.	Read			
DescribeEntityRecognizer	상태, 훈련 데이터가 들어 있는 S3 버킷, 인식기 메타데이터, 지표 등 엔터티 인식기 세부 정보를 제공합니다.	Read	entity-recognizer* (p. 867)		
DescribeKeyPhrasesDetectionJob	핵심 문구 감지 작업과 연결된 속성을 가져옵니다.	Read			
DescribeSentimentDetectionJob	감성 감지 작업과 연결된 속성을 가져옵니다.	Read			
DescribeTopicsDetectionJob	주제 감지 작업과 연결된 속성을 가져옵니다.	Read			
DetectDominantLanguage	텍스트에 있는 언어를 감지합니다.	Read			
DetectEntities	지정된 텍스트 문서 내에서 명명된 개체("People", "Places", "Locations" 등)를 감지합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DetectKeyPhrases	콘텐츠를 가장 잘 나타내는 텍스트의 구를 감지합니다.	Read			
DetectSentiment	문서에 있는 텍스트의 감정을 감지합니다(Positive, Negative, Neutral 또는 Mixed).	Read			
DetectSyntax	텍스트 문서에서 구문 정보(예: 음성의 일부, 토큰)를 감지합니다.	Read			
ListDocumentClassificationJobs	제출한 문서 분류 작업의 목록을 가져옵니다.	List			
ListDocumentClassifiers	생성한 문서 분류기의 목록을 가져옵니다.	List			
ListDominantLanguageDetectionJobs	제출한 중심 언어 감지 작업의 목록을 가져옵니다.	List			
ListEndpoints	기존에 생성한 모든 엔드포인트의 목록을 가져옵니다.	List			
ListEntitiesDetectionJobs	제출한 엔터티 감지 작업의 목록을 가져옵니다.	List			
ListEntityRecognizers	현재 훈련 중인 인식기를 포함하여 생성한 모든 엔터티 인식기의 속성 목록을 가져옵니다.	List			
ListKeyPhrasesDetectionJobs	제출한 핵심 문구 감지 작업의 목록을 가져옵니다.	List			
ListSentimentDetectionJobs	제출한 감성 감지 작업의 목록을 가져옵니다.	List			
ListTagsForResource	리소스에 대한 태그를 나열합니다.	List	document-classifier (p. 867)		
			document-classifier-endpoint (p. 867)		
			entity-recognizer (p. 867)		
ListTopicsDetectionJobs	제출한 주제 감지 작업의 목록을 가져옵니다.	List			
StartDocumentClassificationJob	비동기식 문서 분류 작업을 시작합니다.	쓰기	document-classifier* (p. 867)		
StartDominantLanguageDetectionJob	문서 모음에 대해 비동기식 중심 언어 감지 작업을 시작합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartEntitiesDetectionJob	문서 모음에 대해 비동기식 엔터티 감지 작업을 시작합니다.	쓰기			
StartKeyPhrasesDetectionJob	문서 모음에 대해 비동기식 핵심 문구 감지 작업을 시작합니다.	쓰기			
StartSentimentDetectionJob	문서 모음에 대해 비동기식 감성 감지 작업을 시작합니다.	쓰기			
StartTopicsDetectionJob	비동기 작업을 시작하여 문서 모음에서 가장 일반적인 주제 및 각 주제와 연결된 구를 감지합니다.	쓰기			
StopDominantLanguageDetectionJob	중심 언어 감지 작업을 중지합니다.	쓰기			
StopEntitiesDetectionJob	엔터티 감지 작업을 중지합니다.	쓰기			
StopKeyPhrasesDetectionJob	핵심 문구 감지 작업을 중지합니다.	쓰기			
StopSentimentDetectionJob	감성 감지 작업을 중지합니다.	쓰기			
StopTrainingDocumentClassifier	이전에 생성한 문서 분류자 훈련 작업을 중지합니다.	쓰기	document-classifier* (p. 867)		
StopTrainingEntityRecognizer	이전에 생성한 엔터티 인식기 훈련 작업을 중지합니다.	쓰기	entity-recognizer* (p. 867)		
TagResource	지정된 키 값 페어로 리소스에 태그를 지정합니다.	태그 지정	document-classifier (p. 867)		
			document-classifier-endpoint (p. 867)		
			entity-recognizer (p. 867)		
				aws:RequestTag/${TagKey} (p. 867) aws:TagKeys (p. 868)	
UntagResource	지정된 키를 갖는 리소스에서 태그를 제거합니다.	태그 지정	document-classifier (p. 867)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			document-classifier-endpoint (p. 867)		
			entity-recognizer (p. 867)		
				aws:TagKeys (p. 868)	
UpdateEndpoint	지정된 엔드포인트에 대한 정보를 업데이트합니다.	쓰기	document-classifier-endpoint* (p. 867)		

Amazon Comprehend에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 862)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
document-classifier	`arn:${Partition}:comprehend:${Region}:${Account}:document-classifier/${DocumentClassifierName}`	aws:ResourceTag/${TagKey} (p. 868)
entity-recognizer	`arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer/${EntityRecognizerName}`	aws:ResourceTag/${TagKey} (p. 868)
document-classifier-endpoint	`arn:${Partition}:comprehend:${Region}:${Account}:document-classifier-endpoint/${DocumentClassifierEndpointName}`	aws:ResourceTag/${TagKey} (p. 868)

Amazon Comprehend의 조건 키

Amazon Comprehend는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 필수 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열

조건 키	설명	유형
aws:ResourceTag/${TagKey}	리소스와 연결된 태그 값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열

Comprehend Medical에 사용되는 작업, 리소스 및 조건 키

Comprehend Medical(서비스 접두사: `comprehendmedical`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Comprehend Medical에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DetectEntities	지정된 텍스트에서 지정된 유형의 개체를 검사하고 해당 개체에 대한 설명을 반환합니다.	Read			
DetectPHI	지정된 텍스트에서 PHI 개체를 검사하고 해당 개체에 대한 설명을 반환합니다.	Read			

Comprehend Medical에서 정의한 리소스 유형

Comprehend Medical은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Comprehend Medical에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Comprehend Medical에 사용되는 조건 키

Comprehend Medical에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Compute Optimizer를 위한 작업, 리소스 및 조건 키

Compute Optimizer(서비스 접두사: `compute-optimizer`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Compute Optimizer에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetAutoScalingGroupRecommendations	제공된 자동 크기 조정 그룹에 대한 권장 사항을 가져올 수 있는 권한을 부여합니다.	List			
GetEC2InstanceRecommendations	제공된 EC2 인스턴스에 대한 권장 사항을 가져올 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetEC2RecommendationProjectedMetrics	지정된 인스턴스의 권장 예상 지표를 가져올 수 있는 권한을 부여합니다.	List			
GetEnrollmentStatus	지정된 계정의 등록 상태를 가져올 수 있는 권한을 부여합니다.	List			
GetRecommendationSummaries	지정된 계정(들)에 대한 권장 사항 요약을 가져올 수 있는 권한을 부여합니다.	List			
UpdateEnrollmentStatus	등록 상태를 업데이트할 수 있는 권한을 부여합니다.	쓰기			

Compute Optimizer에서 정의한 리소스 유형

Compute Optimizer는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Compute Optimizer에 대한 액세스를 허용하려면 정책에 `"Resource": "*"`을 지정합니다.

Compute Optimizer에 대한 조건 키

Compute Optimizer에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Config에 사용되는 작업, 리소스 및 조건 키

AWS Config(서비스 접두사: `config`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Config에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchGetAggregateResourceConfig	AWS Config 집계자에 있는 리소스에 대한 현재 구성 항목을 반환합니다.	Read	ConfigurationAggregator* (p. 877)		
BatchGetResourceConfig	하나 이상의 요청된 리소스에 대한 현재 구성을 반환합니다.	Read			
DeleteAggregationAuthorization	지정된 리전의 지정된 구성 집계자 계정에 부여된 권한 부여를 삭제합니다.	쓰기	AggregationAuthorization* (p. 877)		
DeleteConfigRule	지정된 AWS Config 규칙과 모든 평가 결과를 삭제합니다.	쓰기	ConfigRule* (p. 877)		
DeleteConfigurationAggregator	지정된 구성 집계자 및 해당 집계자와 연결된 집계된 데이터를 삭제합니다.	쓰기	ConfigurationAggregator* (p. 877)		
DeleteConfigurationRecorder	구성 레코더를 삭제합니다.	쓰기			
DeleteConformancePack	지정된 적합성 팩과 모든 AWS Config 규칙 및 해당 적합성 팩 내의 모든 평가 결과를 삭제합니다.	쓰기			
DeleteDeliveryChannel	전송 채널을 삭제합니다.	쓰기			
DeleteEvaluationResults	지정된 Config 규칙의 평가 결과를 삭제합니다.	쓰기	ConfigRule* (p. 877)		
DeleteOrganizationConfigRule	지정된 조직 구성 규칙과 해당 조직의 모든 멤버 계정에서 나온 모든 평가 결과를 삭제합니다.	쓰기			
DeleteOrganizationConformancePack	지정된 조직 적합성 팩과 해당 조직의 모든 멤버 계정에서 나온 모든 평가 결과를 삭제합니다.	쓰기			
DeletePendingAggregationRequest	지정된 리전의 지정된 집계자 계정에 대한 대기중인 권한 부여 요청을 삭제합니다.	쓰기			
DeleteRemediationConfiguration	수정 구성을 삭제합니다.	쓰기	RemediationConfiguration* (p. 877)		
DeleteRemediationExceptions	특정 AWS Config 규칙에서 특정 리소스 키에 대한 수정 예외를 하나 이상 삭제합니다.	쓰기			
DeleteRetentionConfiguration	보존 구성을 삭제합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeliverConfigSnapshot	지정된 전송 채널의 Amazon S3 버킷에 구성 스냅샷을 전달하도록 예약합니다.	Read			
DescribeAggregateComplianceByConfigRules	준수 및 미준수 규칙의 목록을 준수 및 미준수 규칙의 리소스 수와 함께 반환합니다.	List	ConfigurationAggregator* (p. 877)		
DescribeAggregationAuthorizations	다양한 집계자 계정 및 리전에 부여된 권한 부여의 목록을 반환합니다.	List			
DescribeComplianceByConfigRule	지정된 AWS Config 규칙의 준수 여부를 나타냅니다.	List	ConfigRule* (p. 877)		
DescribeComplianceByResource	지정된 AWS 리소스의 준수 여부를 나타냅니다.	List			
DescribeConfigRuleEvaluationStatus	각 AWS Config 관리형 규칙에 대한 상태 정보를 반환합니다.	List	ConfigRule* (p. 877)		
DescribeConfigRules	AWS Config 규칙에 대한 세부 정보를 반환합니다.	List	ConfigRule* (p. 877)		
DescribeConfigurationAggregatorSourcesStatus	집계자 내부의 소스에 대한 상태 정보를 반환합니다.	List	ConfigurationAggregator* (p. 877)		
DescribeConfigurationAggregators	하나 이상의 구성 집계자에 대한 세부 정보를 반환합니다.	List			
DescribeConfigurationRecorderStatus	지정된 구성 레코더의 현재 상태를 반환합니다.	List			
DescribeConfigurationRecorders	하나 이상의 지정된 구성 레코더의 이름을 반환합니다.	List			
DescribeConformancePackCompliance	해당 적합성 팩의 각 규칙에 대한 규정 준수 정보를 반환합니다.	Read			
DescribeConformancePackStatus	하나 이상의 적합성 팩 배포 상태를 제공합니다.	Read			
DescribeConformancePacks	하나 이상의 적합성 팩 목록을 반환합니다.	Read			
DescribeDeliveryChannelStatus	지정된 전송 채널의 현재 상태를 반환합니다.	List			
DescribeDeliveryChannels	지정된 전송 채널에 대한 세부 정보를 반환합니다.	List			
DescribeOrganizationConfigRuleStatuses	조직에 대한 조직 구성 규칙 배포 상태를 제공합니다.	Read			
DescribeOrganizationConfigRules	조직 구성 규칙 목록을 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeOrganizationConformancePackStatuses	조직에 대한 조직 적합성 팩 배포 상태를 제공합니다.	Read			
DescribeOrganizationConformancePacks	조직 적합성 팩 목록을 반환합니다.	Read			
DescribePendingAggregationRequests	모든 대기 중인 집계 요청의 목록을 반환합니다.	List			
DescribeRemediationConfigurations	하나 이상의 수정 구성에 대한 세부 정보를 반환합니다.	List	RemediationConfiguration* (p. 877)		
DescribeRemediationExceptions	하나 이상의 수정 예외에 대한 세부 정보를 반환합니다.	List			
DescribeRemediationExecutionStatus	실패한 단계의 상태, 타임스탬프 및 오류 메시지를 포함하여 리소스 집합에 대한 수정 실행에 대한 상세 보기를 제공합니다.	List	RemediationConfiguration* (p. 877)		
DescribeRetentionConfigurations	하나 이상의 보존 구성에 대한 세부 정보를 반환합니다.	List			
GetAggregateComplianceDetailsByConfigRule	규칙의 특정 리소스에 대해 지정된 AWS Config 규칙의 평가 결과를 반환합니다.	Read	ConfigurationAggregator* (p. 877)		
GetAggregateConfigRuleComplianceSummary	집계자의 하나 이상의 계정 및 리전에 대한 준수 및 미준수 규칙의 수를 반환합니다.	Read	ConfigurationAggregator* (p. 877)		
GetAggregateDiscoveredResourceCounts	AWS Config 집계자에 있는 계정 및 리전의 리소스 수를 반환합니다.	Read	ConfigurationAggregator* (p. 877)		
GetAggregateResourceConfig	특정 소스 계정 및 리전의 특정 리소스에 대해 집계되는 구성 항목을 반환합니다.	Read	ConfigurationAggregator* (p. 877)		
GetComplianceDetailsByConfigRule	지정된 AWS Config 규칙의 평가 결과를 반환합니다.	Read	ConfigRule* (p. 877)		
GetComplianceDetailsByResource	지정된 AWS 리소스의 평가 결과를 반환합니다.	Read			
GetComplianceSummaryByConfigRule	준수 및 미준수 AWS Config 규칙의 수를 반환합니다(각각 최대 25개).	Read			
GetComplianceSummaryByResourceType	규칙을 준수하는 리소스의 수와 규칙을 미준수하는 리소스의 수를 반환합니다.	Read			
GetConformancePackComplianceDetails	적합성 팩에 의해 모니터링되는 모든 AWS 리소스에 대한 적합성 팩의 규정 준수 세부 정보를 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetConformancePackComplianceSummary	하나 이상의 준수 팩에 대한 규정 준수 요약을 제공합니다.	Read			
GetDiscoveredResourceCounts	AWS Config가 AWS 계정의 이 리전에서 기록 중인 리소스 유형, 각 리소스 유형의 수, 총 리소스 수를 반환합니다.	Read			
GetOrganizationConfigRuleDetailedStatus	주어진 조직 구성 규칙에 대한 조직 내 각 멤버 계정의 세부 상태를 반환합니다.	Read			
GetOrganizationConformancePackDetailedStatus	주어진 조직 적합성 팩에 대한 조직 내 각 멤버 계정의 세부 상태를 반환합니다.	Read			
GetResourceConfigHistory	지정된 리소스에 대한 구성 항목의 목록을 반환합니다.	Read			
ListAggregateDiscoveredResources	리소스 유형을 수락하고 계정 및 리전에서 특정 리소스 유형에 대해 집계되는 리소스 식별자의 목록을 반환합니다.	List	ConfigurationAggregator* (p. 877)		
ListDiscoveredResources	리소스 유형을 허용하고 해당 유형의 리소스에 대한 리소스 식별자의 목록을 반환합니다.	List			
ListTagsForResource	AWS Config 리소스에 대한 태그를 나열합니다.	List	AggregationAuthorization (p. 877)		
			ConfigRule (p. 877)		
			ConfigurationAggregator (p. 877)		
PutAggregationAuthorization	집계자 계정 및 리전이 소스 계정 및 리전에서 데이터를 수집하도록 권한을 부여합니다.	쓰기	AggregationAuthorization* (p. 877)		
				aws:RequestTag/${TagKey} (p. 877) aws:TagKeys (p. 877)	
PutConfigRule	AWS 리소스가 원하는 구성을 준수하는지 여부를 평가하기 위한 AWS Config 규칙을 추가 또는 업데이트합니다.	쓰기	ConfigRule* (p. 877)		
				aws:RequestTag/${TagKey} (p. 877) aws:TagKeys (p. 877)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutConfigurationAggregator	선택된 소스 계정 및 리전으로 구성 집계자를 생성 및 업데이트합니다.	쓰기	ConfigurationAggregator* (p. 877)		
				aws:RequestTag/${TagKey} (p. 877) aws:TagKeys (p. 877)	
PutConfigurationRecorder	새 구성 레코더를 생성하여 선택한 리소스 구성을 기록합니다.	쓰기			
PutConformancePack	적합성 팩을 생성하거나 업데이트합니다.	쓰기			
PutDeliveryChannel	전송 채널 객체를 생성하여 구성 정보를 Amazon S3 버킷 및 Amazon SNS 주제로 전송합니다.	쓰기			
PutEvaluations	AWS Lambda 함수에서 평가 결과를 AWS Config로 전달하는 데 사용됩니다.	쓰기			
PutOrganizationConfigRule	전체 조직에 대한 조직 구성 규칙을 추가하거나 업데이트하여 AWS 리소스가 원하는 구성을 준수하는지 여부를 평가합니다.	쓰기			
PutOrganizationConformancePack	전체 조직에 대한 조직 적합성 팩을 추가하거나 업데이트하여 AWS 리소스가 원하는 구성을 준수하는지 여부를 평가합니다.	쓰기			
PutRemediationConfigurations	선택된 대상 또는 작업을 사용하여 특정 AWS Config 규칙으로 수정 구성을 추가 또는 업데이트합니다.	쓰기	RemediationConfiguration* (p. 877)		
PutRemediationExceptions	특정 AWS Config 규칙의 특정 리소스에 대한 수정 예외를 추가하거나 업데이트합니다.	쓰기			
PutRetentionConfiguration	AWS Config가 과거 정보를 저장하는 보존 기간(단위: 일)에 대한 세부 정보로 보존 구성을 생성 및 업데이트합니다.	쓰기			
SelectResourceConfig	SQL(구조화 질의 언어) SELECT 명령을 수락하고, 해당 검색을 수행하고, 속성과 일치하는 리소스 구성을 반환합니다.	Read			
StartConfigRulesEvaluation	지정된 Config 규칙에 따라 리소스를 평가합니다.	쓰기	ConfigRule* (p. 877)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartConfigurationRecorder	AWS 계정에 기록하도록 선택한 AWS 리소스의 구성 기록을 시작합니다.	쓰기			
StartRemediationExecution	마지막으로 알려진 수정 구성에 대해 지정된 AWS Config 규칙의 온디맨드 수정을 실행합니다.	쓰기	RemediationConfiguration* (p. 877)		
StopConfigurationRecorder	AWS 계정에 기록하도록 선택한 AWS 리소스의 구성 기록을 중지합니다.	쓰기			
TagResource	리소스에 지정된 태그를 지정된 resourceArn과 연결합니다.	태그 지정	AggregationAuthorization (p. 877)		
			ConfigRule (p. 877)		
			ConfigurationAggregator (p. 877)		
			ConformancePack (p. 877)		
				aws:RequestTag/${TagKey} (p. 877) aws:TagKeys (p. 877)	
UntagResource	리소스에서 지정된 태그를 삭제합니다.	태그 지정	AggregationAuthorization (p. 877)		
			ConfigRule (p. 877)		
			ConfigurationAggregator (p. 877)		
			ConformancePack (p. 877)		
				aws:TagKeys (p. 877)	

AWS Config에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 870)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
AggregationAuthorization	`arn:${Partition}:config:${Region}:${Account}:aggregation-authorization/${AggregatorAccount}/${AggregatorRegion}`	aws:ResourceTag/${TagKey} (p. 877)
ConfigurationAggregator	`arn:${Partition}:config:${Region}:${Account}:config-aggregator/${AggregatorId}`	aws:ResourceTag/${TagKey} (p. 877)
ConfigRule	`arn:${Partition}:config:${Region}:${Account}:config-rule/${ConfigRuleId}`	aws:ResourceTag/${TagKey} (p. 877)
ConformancePack	`arn:${Partition}:config:${Region}:${Account}:conformance-pack/${ConformancePackName}/${ConformancePackId}`	aws:ResourceTag/${TagKey} (p. 877)
OrganizationConfigRule	`arn:${Partition}:config:${Region}:${Account}:organization-config-rule/${OrganizationConfigRuleId}`	
OrganizationConformancePack	`arn:${Partition}:config:${Region}:${Account}:organization-conformance-pack/${OrganizationConformancePackId}`	
RemediationConfiguration	`arn:${Partition}:config:${Region}:${Account}:remediation-configuration/${RemediationConfigurationId}`	

AWS Config의 조건 키

AWS Config는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon Connect에 사용되는 작업, 리소스 및 조건 키

Amazon Connect(서비스 접두사: `connect`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Connect에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateInstance	새 Amazon Connect 인스턴스를 생성할 수 있는 권한을 부여합니다. 연결된 필수 작업은 인스턴스 설정을 구성할 수 있는 권한을 부여합니다.	쓰기			ds:CreateAlias ds:DeleteDirectory ds:DescribeDirectories firehose:DescribeDelivery firehose:ListDeliveryStrea iam:CreateServiceLinkedI kinesis:DescribeStream kinesis:ListStreams kms:CreateGrant kms:DescribeKey kms:ListAliases kms:RetireGrant s3:CreateBucket s3:ListAllMyBuckets

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateUser	지정된 Amazon Connect 인스턴스에 대해 사용자를 생성할 수 있는 권한을 부여합니다.	쓰기	routing-profile* (p. 883)		
			security-profile* (p. 883)		
			user* (p. 883)		
			hierarchy-group (p. 883)		
				aws:RequestTag/${TagKey} (p. 884) aws:TagKeys (p. 884)	
DeleteUser	Amazon Connect 인스턴스의 사용자를 삭제할 수 있는 권한을 부여합니다.	쓰기	user* (p. 883)		
				aws:ResourceTag/${TagKey} (p. 884)	
DescribeInstance	Amazon Connect 인스턴스의 세부 정보를 볼 수 있는 권한을 부여합니다. 인스턴스를 생성하려면 필요합니다.	Read	instance* (p. 883)		firehose:DescribeDelivery firehose:ListDeliveryStrea kinesis:DescribeStream kinesis:ListStreams kms:DescribeKey kms:ListAliases s3:ListAllMyBuckets
DescribeUser	Amazon Connect 인스턴스의 사용자를 설명할 수 있는 권한을 부여합니다.	Read	user* (p. 883)		
				aws:ResourceTag/${TagKey} (p. 884)	
DescribeUserHierarchyGroup	Amazon Connect 인스턴스의 계층 구조 그룹을 설명할 수 있는 권한을 부여합니다.	Read	hierarchy-group* (p. 883)		
DescribeUserHierarchyStructure	Amazon Connect 인스턴스의 계층 구조를 설명할 수 있는 권한을 부여합니다.	Read	instance* (p. 883)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DestroyInstance	Amazon Connect 인스턴스를 삭제할 수 있는 권한을 부여합니다. 인스턴스를 제거하면 기존 AWS 디렉터리에 대한 링크 또한 제거됩니다.	쓰기	instance* (p. 883)		
GetContactAttributes	지정된 연락처의 연락처 속성을 검색할 수 있는 권한을 부여합니다.	Read	contact* (p. 883)		
GetCurrentMetricData	Amazon Connect 인스턴스에서 대기열에 대한 현재 지표 데이터를 검색할 수 있는 권한을 부여합니다.	Read	queue* (p. 883)		
GetFederationToken	자격 증명 관리를 위해 SAML 기반 인증을 사용할 때 인스턴스로의 연동을 허용합니다.	Read	instance* (p. 883)		
GetFederationTokens	Amazon Connect 인스턴스로 연동할 수 있는 권한을 부여합니다(AWS 콘솔에서 관리자로 로그인 기능).	쓰기	instance* (p. 883)		connect:DescribeInstance connect:ListInstances ds:DescribeDirectories
GetMetricData	Amazon Connect 인스턴스에서 대기열에 대한 과거 지표 데이터를 검색할 수 있는 권한을 부여합니다.	Read	queue* (p. 883)		
ListContactFlows	Amazon Connect 인스턴스의 연락처 흐름 리소스를 나열할 수 있는 권한을 부여합니다.	List	instance* (p. 883)		
ListHoursOfOperations	Amazon Connect 인스턴스의 작업 시간 리소스를 나열할 수 있는 권한을 부여합니다.	List	instance* (p. 883)		
ListInstances	AWS 계정과 연결된 Amazon Connect 인스턴스를 볼 수 있는 권한을 부여합니다.	List			
ListPhoneNumbers	Amazon Connect 인스턴스의 전화 번호 리소스를 나열할 수 있는 권한을 부여합니다.	List	instance* (p. 883)		
ListQueues	Amazon Connect 인스턴스의 대기열 리소스를 나열할 수 있는 권한을 부여합니다.	List	instance* (p. 883)		
ListRoutingProfiles	Amazon Connect 인스턴스의 라우팅 프로파일 리소스를 나열할 수 있는 권한을 부여합니다.	List	instance* (p. 883)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListSecurityProfiles	Amazon Connect 인스턴스의 보안 프로파일 리소스를 나열할 수 있는 권한을 부여합니다.	List	instance* (p. 883)		
ListTagsForResource	Amazon Connect 리소스의 태그를 나열할 수 있는 권한을 부여합니다.	Read	user (p. 883)		
				aws:ResourceTag/${TagKey} (p. 884)	
ListUserHierarchyGroups	Amazon Connect 인스턴스의 계층 구조 그룹 리소스를 나열할 수 있는 권한을 부여합니다.	List	instance* (p. 883)		
ListUsers	Amazon Connect 인스턴스의 사용자 리소스를 나열할 수 있는 권한을 부여합니다.	List	instance* (p. 883)		
ModifyInstance	기존 Amazon Connect 인스턴스의 구성 설정을 수정할 수 있는 권한을 부여합니다. 연결된 필수 작업은 인스턴스에 대한 설정을 수정할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 883)		firehose:DescribeDelivery firehose:ListDeliveryStrea kinesis:DescribeStream kinesis:ListStreams kms:CreateGrant kms:DescribeKey kms:ListAliases kms:RetireGrant s3:CreateBucket s3:ListAllMyBuckets
StartChatContact	Amazon Connect API를 사용하여 채팅을 시작할 수 있는 권한을 부여합니다.	쓰기	contact-flow* (p. 883)		
StartOutboundVoiceContact	Amazon Connect API를 사용하여 아웃바운드 호출을 시작할 수 있는 권한을 부여합니다.	쓰기	contact* (p. 883)		
StopContact	Amazon Connect API를 사용하여 시작된 연락처를 중지할 수 있는 권한을 부여합니다. 활성 연락처에서 이 작업을 사용하면 에이전트가 고객과의 통화에서 활성화된 경우에도 연락처가 종료됩니다.	쓰기	contact* (p. 883)		
TagResource	Amazon Connect 리소스에 태그를 지정할 수 있는 권한을 부여합니다.	태그 지정	user (p. 883)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 884) aws:RequestTag/${TagKey} (p. 884) aws:ResourceTag/${TagKey} (p. 884)	
UntagResource	Amazon Connect 리소스의 태그를 해제할 수 있는 권한을 부여합니다.	태그 지정	user (p. 883)		
				aws:TagKeys (p. 884) aws:ResourceTag/${TagKey} (p. 884)	
UpdateContactAttributes	지정된 연락처와 연결된 연락처 속성을 생성하거나 업데이트할 수 있는 권한을 부여합니다.	쓰기	contact* (p. 883)		
UpdateUserHierarchy	Amazon Connect 인스턴스의 사용자에 대한 계층 구조 그룹을 업데이트할 수 있는 권한을 부여합니다.	쓰기	user* (p. 883)		
			hierarchy-group (p. 883)		
				aws:ResourceTag/${TagKey} (p. 884)	
UpdateUserIdentityInfo	Amazon Connect 인스턴스의 사용자에 대한 자격 증명 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기	user* (p. 883)		
				aws:ResourceTag/${TagKey} (p. 884)	
UpdateUserPhoneConfig	Amazon Connect 인스턴스의 사용자에 대한 전화 구성 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기	user* (p. 883)		
				aws:ResourceTag/${TagKey} (p. 884)	
UpdateUserRoutingProfile	Amazon Connect 인스턴스의 사용자에 대한 라우팅 프로파일을 업데이트할 수 있는 권한을 부여합니다.	쓰기	routing-profile* (p. 883)		
			user* (p. 883)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:ResourceTag/${TagKey} (p. 884)	
UpdateUserSecurityProfiles	Amazon Connect 인스턴스의 사용자에 대한 보안 프로파일을 업데이트할 수 있는 권한을 부여합니다.	쓰기	security-profile* (p. 883)		
			user* (p. 883)		
				aws:ResourceTag/${TagKey} (p. 884)	

Amazon Connect에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 878)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
instance	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}`	
contact	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact/${ContactId}`	
user	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent/${UserId}`	aws:ResourceTag/${TagKey} (p. 884)
routing-profile	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/routing-profile/${RoutingProfileId}`	
security-profile	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/security-profile/${SecurityProfileId}`	
hierarchy-group	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent-group/${HierarchyGroupId}`	
queue	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/queue/${QueueId}`	
contact-flow	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact-flow/${ContactFlowId}`	

리소스 유형	ARN	조건 키
hours-of-operation	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/operating-hours/${HoursOfOperationId}`	
phone-number	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/phone-numbers/${PhoneNumberId}`	

Amazon Connect에 사용되는 조건 키

Amazon Connect는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Connector Service에 사용되는 작업, 리소스 및 조건 키

AWS Connect Service(서비스 접두사: `awsconnector`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Connector Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetConnectorHealth [권한만 해당]	서버 마이그레이션 커넥터에서 게시된 모든 상태 지표를 검색합니다.	Read			
RegisterConnector [권한만 해당]	AWS Connector Service에 AWS Connector를 등록합니다.	쓰기			
ValidateConnectorId [권한만 해당]	AWS Connector Service에 등록된 서버 마이그레이션 커넥터 ID를 확인합니다.	Read			

AWS Connector Service에서 정의한 리소스 유형

AWS Connector Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Connector Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Connector Service에 사용되는 조건 키

Connector Service에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Cost and Usage Report에 사용되는 작업, 리소스 및 조건 키

AWS Cost and Usage Report(서비스 접두사: `cur`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Cost and Usage Report에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteReportDefinition	Cost and Usage Report 정의를 삭제합니다.	쓰기	cur* (p. 886)		
DescribeReportDefinitions	Cost and Usage Report 정의를 가져옵니다.	Read			
ModifyReportDefinition	Cost and Usage Report 정의를 수정합니다.	쓰기	cur* (p. 886)		
PutReportDefinition	Cost and Usage Report 정의를 씁니다.	쓰기	cur* (p. 886)		

AWS Cost and Usage Report에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 885)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
cur	`arn:${Partition}:cur:${Region}:${Account}:definition/${ReportName}`	

AWS Cost and Usage Report의 조건 키

Cost and Usage Report에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Cost Explorer Service에 사용되는 작업, 리소스 및 조건 키

AWS Cost Explorer Service(서비스 접두사: `ce`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Cost Explorer Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCostCategoryDefinition	요청된 이름과 규칙을 사용하여 새로운 비용 범주를 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteCostCategoryDefinition	비용 범주를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DescribeCostCategoryDefinition	비용 범주의 이름, ARN, 규칙, 정의 및 유효 날짜와 같은 설명을 검색할 수 있는 권한을 부여합니다.	Read			
GetCostAndUsage	계정의 비용 및 사용 지표를 검색할 수 있는 권한을 부여합니다.	Read			
GetCostAndUsageWithResources	계정 리소스를 사용하여 비용 및 사용량 지표를 검색할 수 있는 권한을 부여합니다.	Read			
GetCostForecast	예측 기간에 대한 비용 예측을 검색할 수 있는 권한을 부여합니다.	Read			
GetDimensionValues	일정 기간 동안 필터에 사용할 수 있는 모든 필터 값을 검색할 수 있는 권한을 부여합니다.	Read			
GetReservationCoverage	계정의 예약 비율을 검색할 수 있는 권한을 부여합니다.	Read			
GetReservationPurchaseRecommendation	계정의 예약 권장 사항을 검색할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetReservationUtilization	계정의 사용률을 검색할 수 있는 권한을 부여합니다.	Read			
GetRightsizingRecommendation	계정의 규모 조정 권장 사항을 검색할 수 있는 권한을 부여합니다.	Read			
GetSavingsPlansCoverage	계정의 Savings Plans 적용 범위를 검색할 수 있는 권한을 부여합니다.	Read			
GetSavingsPlansPurchaseRecommendation	계정의 Savings Plans 권장 사항을 검색할 수 있는 권한을 부여합니다.	Read			
GetSavingsPlansUtilization	계정의 Savings Plans 사용률을 검색할 수 있는 권한을 부여합니다.	Read			
GetSavingsPlansUtilizationDetails	계정의 Savings Plans 사용률 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read			
GetTags	지정된 기간 동안 태그를 쿼리할 수 있는 권한을 부여합니다.	Read			
GetUsageForecast	예측 기간에 대한 사용량 예측을 검색할 수 있는 권한을 부여합니다.	Read			
ListCostCategoryDefinitions	모든 비용 범주에 대한 이름, ARN 및 유효 날짜를 검색할 수 있는 권한을 부여합니다.	List			
UpdateCostCategoryDefinition	기존 비용 범주를 업데이트할 수 있는 권한을 부여합니다.	쓰기			

AWS Cost Explorer Service에서 정의한 리소스 유형

AWS Cost Explorer Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Cost Explorer Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Cost Explorer Service에 사용되는 조건 키

Cost Explorer Service에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Data Exchange에 사용되는 작업, 리소스 및 조건 키

AWS Data Exchange(서비스 접두사: `dataexchange`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Data Exchange에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelJob	작업을 취소할 수 있는 권한을 부여합니다.	쓰기	jobs* (p. 891)		
CreateDataSet	데이터 세트를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 891) aws:ResourceTag/${TagKey} (p. 892) aws:TagKeys (p. 892)	
CreateJob	자산을 가져오거나 내보낼 작업을 생성할 수 있는 권한을 부여합니다.	쓰기	jobs* (p. 891)		
CreateRevision	개정을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 891) aws:ResourceTag/${TagKey} (p. 892) aws:TagKeys (p. 892)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteAsset	자산을 삭제할 수 있는 권한을 부여합니다.	쓰기	assets* (p. 891)		
DeleteDataSet	데이터 세트를 삭제할 수 있는 권한을 부여합니다.	쓰기	data-sets* (p. 891)		
DeleteRevision	개정을 삭제할 수 있는 권한을 부여합니다.	쓰기	revisions* (p. 891)		
GetAsset	자산에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	assets* (p. 891)		
GetDataSet	데이터 세트에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	data-sets* (p. 891)		
GetJob	작업에 대한 정보를 가져올 수 있는 권한을 부여합니다.	쓰기	jobs* (p. 891)		
GetRevision	개정에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	revisions* (p. 891)		
ListDataSetRevisions	데이터 세트의 개정을 나열할 수 있는 권한을 부여합니다.	List	revisions* (p. 891)		
ListDataSets	계정의 데이터 세트를 나열할 수 있는 권한을 부여합니다.	List	data-sets* (p. 891)		
ListJobs	계정에 대한 작업을 나열할 수 있는 권한을 부여합니다.	List	jobs* (p. 891)		
ListRevisionAssets	개정의 자산을 나열할 수 있는 권한을 부여합니다.	List	assets* (p. 891)		
ListTagsForResource	지정된 리소스와 연결한 태그를 나열할 수 있는 권한을 부여합니다.	Read	data-sets (p. 891)		
			revisions (p. 891)		
StartJob	작업을 시작할 수 있는 권한을 부여합니다.	쓰기	jobs* (p. 891)		
TagResource	지정된 리소스에 하나 이상의 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	data-sets (p. 891)		
			revisions (p. 891)		
				aws:RequestTag/${TagKey} (p. 891) aws:TagKeys (p. 892)	
UntagResource	지정된 리소스에서 하나 이상의 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	data-sets (p. 891)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			revisions (p. 891)		
				aws:TagKeys (p. 892)	
UpdateAsset	자산에 대한 업데이트 정보를 가져올 수 있는 권한을 부여합니다.	쓰기	assets* (p. 891)		
UpdateDataSet	데이터 세트에 대한 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기	data-sets* (p. 891)		
UpdateRevision	개정에 대한 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기	revisions* (p. 891)		

AWS Data Exchange에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 889)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
jobs	`arn:${Partition}:dataexchange:${Region}:${Account}:jobs/${JobId}`	dataexchange:JobType (p. 892)
data-sets	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}`	
revisions	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}`	
assets	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}`	

AWS Data Exchange에 사용되는 조건 키

AWS Data Exchange는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 필수 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열

조건 키	설명	유형
aws:ResourceTag/${TagKey}	리소스와 연결된 태그 값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열
dataexchange:JobType	지정된 작업 유형에서만 이 작업을 수행할 수 있음을 표시합니다.	문자열

Amazon Data Lifecycle Manager에 사용되는 작업, 리소스 및 조건 키

Amazon Data Lifecycle Manager(서비스 접두사: `dlm`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Data Lifecycle Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateLifecyclePolicy	Amazon EBS 스냅샷의 예약 생성 및 보존을 관리하는 데이터 수명 주기 정책을 생성합니다. 최대 100개의 정책을 관리할 수 있습니다.	쓰기		aws:RequestTag/${TagKey} (p. 893)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 894)	
DeleteLifecyclePolicy	기존 데이터 수명 주기 정책을 삭제합니다. 또한 이 작업은 정책이 지정한 스냅샷의 생성 및 보존을 중지합니다. 기존 스냅샷은 영향을 받지 않습니다.	쓰기	policy* (p. 893)		
GetLifecyclePolicies	데이터 수명 주기 정책에 대한 요약 설명의 목록을 반환합니다.	List			
GetLifecyclePolicy	단일 데이터 수명 주기 정책에 대한 전체 설명을 반환합니다.	Read	policy* (p. 893)		
ListTagsForResource	리소스와 연결된 태그를 나열할 수 있는 권한을 부여합니다.	Read	policy* (p. 893)		
TagResource	리소스 태그를 추가 또는 업데이트할 수 있는 권한을 부여합니다.	태그 지정	policy* (p. 893)		
UntagResource	리소스와 연결된 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	policy* (p. 893)		
UpdateLifecyclePolicy	기존 데이터 수명 주기 정책을 업데이트합니다.	쓰기	policy* (p. 893)		

Amazon Data Lifecycle Manager에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 892)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
policy	`arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}`	aws:ResourceTag/${TagKey} (p. 894)

Amazon Data Lifecycle Manager에 사용되는 조건 키

Amazon Data Lifecycle Manager는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Data Pipeline에 사용되는 작업, 리소스 및 조건 키

Data Pipeline(서비스 접두사: `datapipeline`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Data Pipeline에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ActivatePipeline	지정된 파이프라인을 검증하고 처리 파이프라인 작업을 시작합니다. 파이프라인이 검증에 통과하지 못한 경우 활성화에 실패합니다.	쓰기		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897) datapipeline:workerGroup (p. 897)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTags	지정된 파이프라인에 대한 태그를 추가 또는 수정합니다.	태그 지정		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897)	
CreatePipeline	비어있는 새로운 파이프라인을 만듭니다.	쓰기		datapipeline:Tag (p. 897)	
DeactivatePipeline	지정된 실행 중인 파이프라인을 비활성화합니다.	쓰기		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897) datapipeline:workerGroup (p. 897)	
DeletePipeline	파이프라인, 해당 파이프라인 정의 및 실행 내역을 삭제합니다.	쓰기		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897)	
DescribeObjects	파이프라인과 연결된 객체 집합에 대한 객체 정의를 가져옵니다.	Read		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897)	
DescribePipelines	하나 이상의 파이프라인에 대한 메타데이터를 검색합니다.	List		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897)	
EvaluateExpression	작업 실행기가 지정된 객체의 컨텍스트에서 문자열을 평가하기 위해 EvaluateExpression을 호출합니다.	Read		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897)	
GetAccountLimits	GetAccountLimits에 대한 설명	List			
GetPipelineDefinition	지정된 파이프라인의 정의를 가져옵니다.	Read		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897) datapipeline:workerGroup (p. 897)	
ListPipelines	액세스할 권한이 있는 모든 활성 파이프라인에 대한 파이프라인 식별자를 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PollForTask	작업 실행기가 AWS Data Pipeline에서 수행할 작업을 검색하기 위해 PollForTask를 호출합니다.	쓰기		datapipeline:workerGroup (p. 897)	
PutAccountLimits	PutAccountLimits에 대한 설명	쓰기			
PutPipelineDefinition	지정된 파이프라인에 작업, 일정 및 사전 조건을 추가합니다.	쓰기		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897) datapipeline:workerGroup (p. 897)	
QueryObjects	지정된 조건 집합에 일치하는 객체의 이름에 대해 지정된 파이프라인을 쿼리합니다.	Read		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897)	
RemoveTags	지정된 파이프라인에서 기존 태그를 제거합니다.	태그 지정		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897)	
ReportTaskProgress	작업 실행기가 작업이 있음을 확인하기 위해 작업을 할당했을 때 ReportTaskProgress를 호출합니다.	쓰기			
ReportTaskRunnerHeartbeat	작업 실행기가 작동되고 있음을 나타내기 위해 15분마다 ReportTaskRunnerHeartbeat를 호출합니다.	쓰기			
SetStatus	지정된 파이프라인에서 지정된 물리적 또는 논리적 파이프라인 객체의 상태가 업데이트되도록 요청합니다.	쓰기		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897)	
SetTaskStatus	작업 실행기가 AWS Data Pipeline에 작업이 완료되었음을 알리고 최종 상태에 대한 정보를 제공하기 위해 SetTaskStatus 요청을 호출합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ValidatePipelineDefinition	잘 형성되고 오류 없이 실행될 수 있도록 지정된 파이프라인 정의를 검증합니다.	Read		datapipeline:PipelineCreator (p. 897) datapipeline:Tag (p. 897) datapipeline:workerGroup (p. 897)	

Data Pipeline에서 정의한 리소스 유형

Data Pipeline은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Data Pipeline에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Data Pipeline에 사용되는 조건 키

Data Pipeline은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
datapipeline:PipelineCreator	파이프라인을 생성한 IAM 사용자.	ARN
datapipeline:Tag	리소스에 연결할 수 있는 고객이 지정한 키/값 페어입니다.	ARN
datapipeline:workerGroup	작업 실행기가 작업을 검색할 작업자 그룹의 이름입니다.	ARN

AWS Database Migration Service에 사용되는 작업, 리소스 및 조건 키

AWS Database Migration Service(서비스 접두사: `dms`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Database Migration Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTagsToResource	복제 인스턴스, 엔드포인트, 보안 그룹 및 마이그레이션 작업을 포함하여 DMS 리소스에 메타데이터 태그를 추가합니다.	태그 지정	Certificate (p. 903)		
			Endpoint (p. 903)		
			EventSubscription (p. 903)		
			ReplicationInstance (p. 903)		
			ReplicationSubnetGroup (p. 904)		
			ReplicationTask (p. 903)		
				aws:RequestTag/${TagKey} (p. 904) aws:TagKeys (p. 904) dms:req-tag/${TagKey} (p. 904)	
ApplyPendingMaintenanceAction	대기 중인 유지 관리 작업을 리소스(예: 복제 인스턴스)에 적용합니다.	쓰기	ReplicationInstance* (p. 903)		
CreateEndpoint	제공된 설정을 사용하여 엔드포인트를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 904) aws:TagKeys (p. 904)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				dms:req-tag/${TagKey} (p. 904)	
CreateEventSubscription	AWS DMS 이벤트 알림 구독을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 904) aws:TagKeys (p. 904) dms:req-tag/${TagKey} (p. 904)	
CreateReplicationInstance	지정된 파라미터를 사용하여 복제 인스턴스를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 904) aws:TagKeys (p. 904) dms:req-tag/${TagKey} (p. 904)	
CreateReplicationSubnetGroup	VPC의 서브넷 ID 목록이 지정된 복제 서브넷 그룹을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 904) aws:TagKeys (p. 904) dms:req-tag/${TagKey} (p. 904)	
CreateReplicationTask	지정된 파라미터를 사용하여 복제 작업을 생성합니다.	쓰기	Endpoint* (p. 903)		
			ReplicationInstance* (p. 903)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 904) aws:TagKeys (p. 904) dms:req-tag/${TagKey} (p. 904)	
DeleteCertificate	지정된 인증서를 삭제합니다.	쓰기	Certificate* (p. 903)		
DeleteEndpoint	지정된 엔드포인트를 삭제합니다.	쓰기	Endpoint* (p. 903)		
DeleteEventSubscription	AWS DMS 이벤트 구독을 삭제합니다.	쓰기	EventSubscription* (p. 903)		
DeleteReplicationInstance	지정된 복제 인스턴스를 삭제합니다.	쓰기	ReplicationInstance* (p. 903)		
DeleteReplicationSubnetGroup	서브넷 그룹을 삭제합니다.	쓰기	ReplicationSubnetGroup* (p. 904)		
DeleteReplicationTask	지정된 복제 작업을 삭제합니다.	쓰기	ReplicationTask* (p. 903)		
DescribeAccountAttributes	고객 계정에 대한 모든 AWS DMS 속성을 나열합니다.	Read			
DescribeCertificates	인증서의 설명을 제공합니다.	Read			
DescribeConnections	복제 인스턴스와 엔드포인트 간의 연결 상태를 설명합니다.	Read			
DescribeEndpointTypes	사용 가능한 엔드포인트 유형에 대한 정보를 반환합니다.	Read			
DescribeEndpoints	현재 리전에 있는 계정의 엔드포인트에 대한 정보를 반환합니다.	Read			
DescribeEventCategories	모든 이벤트 소스 유형 또는 지정된 경우 지정된 소스 유형에 대한 범주를 나열합니다.	Read			
DescribeEventSubscriptions	고객 계정에 대한 모든 이벤트 구독을 나열합니다.	Read			
DescribeEvents	지정된 소스 식별자 및 소스 유형에 대한 이벤트를 나열합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeOrderableReplicationInstances	지정된 리전에서 생성할 수 있는 복제 인스턴스 유형에 대한 정보를 반환합니다.	Read			
DescribeRefreshSchemasStatus	RefreshSchemas 작업의 상태를 반환합니다.	Read	Endpoint* (p. 903)		
DescribeReplicationInstanceTaskLogs	지정된 작업의 작업 로그에 대한 정보를 반환합니다.	Read	ReplicationInstance* (p. 903)		
				aws:ResourceTag/${TagKey} (p. 904) aws:TagKeys (p. 904)	
DescribeReplicationInstances	현재 리전에 있는 계정의 복제 인스턴스에 대한 정보를 반환합니다.	Read			
DescribeReplicationSubnetGroups	복제 서브넷 그룹에 대한 정보를 반환합니다.	Read			
DescribeReplicationTaskAssessmentResults	Amazon S3의 작업 평가 결과를 반환합니다. 이 작업은 항상 최신 결과를 반환합니다.	Read	ReplicationTask (p. 903)		
DescribeReplicationTasks	현재 리전에 있는 계정의 복제 작업에 대한 정보를 반환합니다.	Read			
DescribeSchemas	지정된 엔드포인트의 스키마에 대한 정보를 반환합니다.	Read	Endpoint* (p. 903)		
DescribeTableStatistics	테이블 이름, 삽입된 행, 업데이트된 행, 삭제된 행을 포함하여 데이터베이스 마이그레이션 작업에 대한 테이블 통계를 반환합니다.	Read	ReplicationTask* (p. 903)		
ImportCertificate	지정된 인증서를 업로드합니다.	쓰기		aws:RequestTag/${TagKey} (p. 904) aws:TagKeys (p. 904)	
ListTagsForResource	AWS DMS 리소스의 모든 태그를 나열합니다.	List	Certificate (p. 903)		
			Endpoint (p. 903)		
			EventSubscription (p. 903)		
			ReplicationInstance (p. 903)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			ReplicationSubnetGroup (p. 904)		
			ReplicationTask (p. 903)		
ModifyEndpoint	지정된 엔드포인트를 수정합니다.	쓰기	Endpoint* (p. 903)		
			Certificate (p. 903)		
ModifyEventSubscription	기존 AWS DMS 이벤트 알림 구독을 수정합니다.	쓰기			
ModifyReplicationInstance	복제 인스턴스를 수정하여 새 설정을 적용합니다.	쓰기	ReplicationInstance* (p. 903)		
ModifyReplicationSubnetGroup	지정된 복제 서브넷 그룹에 대한 설정을 수정합니다.	쓰기			
ModifyReplicationTask	지정된 복제 작업을 수정합니다.	쓰기	ReplicationTask* (p. 903)		
RebootReplicationInstance	복제 인스턴스를 재부팅합니다. 재부팅하면 복제 인스턴스가 다시 사용 가능할 때까지 잠시 중단됩니다.	쓰기	ReplicationInstance* (p. 903)		
RefreshSchemas	지정된 엔드포인트에 대한 스키마를 채웁니다.	쓰기	Endpoint* (p. 903)		
			ReplicationInstance* (p. 903)		
ReloadTables	소스 데이터로 대상 데이터베이스 테이블을 다시 로드합니다.	쓰기	ReplicationTask* (p. 903)		
RemoveTagsFromResource	DMS 리소스에서 메타데이터 태그를 제거합니다.	태그 지정	Certificate (p. 903)		
			Endpoint (p. 903)		
			EventSubscription (p. 903)		
			ReplicationInstance (p. 903)		
			ReplicationSubnetGroup (p. 904)		
			ReplicationTask (p. 903)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 904)	
StartReplicationTask	복제 작업을 시작합니다.	쓰기	ReplicationTask* (p. 903)		
StartReplicationTaskAssessment	소스 데이터베이스에서 지원되지 않는 데이터 형식에 대한 복제 작업 평가를 시작합니다.	쓰기	ReplicationTask* (p. 903)		
StopReplicationTask	복제 작업을 중지합니다.	쓰기	ReplicationTask* (p. 903)		
TestConnection	복제 인스턴스와 엔드포인트 간의 연결을 테스트합니다.	Read	Endpoint* (p. 903)		
			ReplicationInstance* (p. 903)		

AWS Database Migration Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 898)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
ReplicationInstance	`arn:${Partition}:dms:${Region}:${Account}:rep:*`	aws:ResourceTag/${TagKey} (p. 904) dms:rep-tag/${TagKey} (p. 904)
ReplicationTask	`arn:${Partition}:dms:${Region}:${Account}:task:*`	aws:ResourceTag/${TagKey} (p. 904) dms:task-tag/${TagKey} (p. 904)
Endpoint	`arn:${Partition}:dms:${Region}:${Account}:endpoint:*`	aws:ResourceTag/${TagKey} (p. 904) dms:endpoint-tag/${TagKey} (p. 904)
Certificate	`arn:${Partition}:dms:${Region}:${Account}:cert:*`	aws:ResourceTag/${TagKey} (p. 904) dms:cert-tag/${TagKey} (p. 904)
EventSubscription	`arn:${Partition}:dms:${Region}:${Account}:es:*`	aws:ResourceTag/${TagKey} (p. 904)

리소스 유형	ARN	조건 키
		dms:es-tag/${TagKey} (p. 904)
ReplicationSubnetGroup	`arn:${Partition}:dms:${Region}:${Account}:subgrp:*`	aws:ResourceTag/${TagKey} (p. 904) dms:subgrp-tag/${TagKey} (p. 904)

AWS Database Migration Service의 조건 키

AWS Database Migration Service는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
dms:cert-tag/${TagKey}	인증서 요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
dms:endpoint-tag/${TagKey}	엔드포인트 요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
dms:es-tag/${TagKey}	EventSubscription 요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
dms:rep-tag/${TagKey}	ReplicationInstance 요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
dms:req-tag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
dms:subgrp-tag/${TagKey}	ReplicationSubnetGroup 요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
dms:task-tag/${TagKey}	ReplicationTask 요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Database Query Metadata Service에 사용되는 작업, 리소스 및 조건 키

Database Query Metadata Service(서비스 접두사: `dbqms`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Database Query Metadata Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateFavoriteQuery	새로운 즐겨찾기 쿼리를 생성합니다	쓰기			
CreateQueryHistory	기록에 쿼리를 추가합니다.	쓰기			
DeleteFavoriteQueries	저장된 쿼리를 삭제합니다.	쓰기			
DeleteQueryHistory	기록 쿼리를 삭제합니다.	쓰기			
DescribeFavoriteQueries	저장된 쿼리 및 관련 메타데이터를 나열합니다.	List			
DescribeQueryHistory	실행된 쿼리의 기록을 나열합니다	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetQueryString	ID로 즐겨찾기 쿼리 또는 기록 쿼리 문자열을 검색합니다.	Read			
UpdateFavoriteQuery	저장된 쿼리 및 설명을 업데이트합니다.	쓰기			
UpdateQueryHistory	쿼리 기록을 업데이트합니다.	쓰기			

Database Query Metadata Service에서 정의한 리소스 유형

Database Query Metadata Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Database Query Metadata Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Database Query Metadata Service에 사용되는 조건 키

DBQMS에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Note

${ConceptsDocRoot}

DataSync에 사용되는 작업, 리소스 및 조건 키

DataSync(서비스 접두사: `datasync`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

DataSync에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시

됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelTaskExecution	동기화 작업의 실행을 취소합니다.	쓰기	taskexecution* (p. 909)		
CreateAgent	호스트에 배포한 에이전트를 활성화합니다.	쓰기		aws:RequestTag/${TagKey} (p. 910) aws:TagKeys (p. 910)	
CreateLocationEfs	Amazon EFS 파일 시스템의 엔드포인트를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 910) aws:TagKeys (p. 910)	
CreateLocationNfs	NFS 파일 시스템의 엔드포인트를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 910) aws:TagKeys (p. 910)	
CreateLocationS3	Amazon S3 버킷의 엔드포인트를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 910) aws:TagKeys (p. 910)	
CreateLocationSmb	SMB 파일 시스템의 엔드포인트를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 910) aws:TagKeys (p. 910)	
CreateTask	동기화 작업을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 910) aws:TagKeys (p. 910)	
DeleteAgent	에이전트를 삭제합니다.	쓰기	agent* (p. 909)		
DeleteLocation	AWS DataSync가 사용하는 위치의 구성을 삭제합니다.	쓰기	location* (p. 909)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteTask	동기화 작업을 삭제합니다.	쓰기	task* (p. 909)		
DescribeAgent	동기화 에이전트에 대한 메타데이터, 즉 이름, 네트워크 인터페이스 및 상태(에이전트 실행 여부)를 반환합니다.	Read	agent* (p. 909)		
DescribeLocationEfs	Amazon EFS 동기화 위치에 대한 메타데이터를 반환합니다(예: 경로 정보).	Read	location* (p. 909)		
DescribeLocationNfs	NFS 동기화 위치에 대한 메타데이터를 반환합니다(예: 경로 정보).	Read	location* (p. 909)		
DescribeLocationS3	Amazon S3 버킷 동기화 위치에 대한 메타데이터를 반환합니다(예: 버킷 이름).	Read	location* (p. 909)		
DescribeLocationSmb	SMB 동기화 위치에 대한 경로 정보와 같은 메타데이터를 반환합니다.	Read	location* (p. 909)		
DescribeTask	동기화 작업에 대한 메타데이터를 반환합니다.	Read	task* (p. 909)		
DescribeTaskExecution	실행되지 않는 동기화 작업에 대한 세부 메타데이터를 반환합니다.	Read	taskexecution* (p. 909)		
ListAgents	요청에 지정된 리전의 AWS 계정이 소유하는 에이전트의 목록을 반환합니다.	List			
ListLocations	원본 및 대상 동기화 위치의 목록을 반환합니다.	List			
ListTagsForResource	이 작업은 지정된 리소스에 추가된 태그를 나열합니다.	Read	agent (p. 909)		
			location (p. 909)		
			task (p. 909)		
ListTaskExecutions	실행된 동기화 작업의 목록을 반환합니다.	List			
ListTasks	모든 동기화 작업의 목록을 반환합니다.	List			
StartTaskExecution	동기화 작업의 특정 호출을 시작합니다.	쓰기	task* (p. 909)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
TagResource	AWS 리소스에 키-값 페어를 적용합니다.	쓰기	agent (p. 909)		
			location (p. 909)		
			task (p. 909)		
				aws:RequestTag/${TagKey} (p. 910) aws:TagKeys (p. 910)	
UntagResource	이 작업은 지정된 리소스에서 하나 이상의 태그를 제거합니다.	태그 지정	agent (p. 909)		
			location (p. 909)		
			task (p. 909)		
				aws:TagKeys (p. 910)	
UpdateAgent	에이전트의 이름을 업데이트합니다.	쓰기	agent* (p. 909)		
UpdateTask	동기화 작업과 연결된 메타데이터를 업데이트합니다.	쓰기	task* (p. 909)		

DataSync에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 906)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
agent	`arn:${Partition}:datasync:${Region}:${AccountId}:agent/${AgentId}`	aws:ResourceTag/${TagKey} (p. 910)
location	`arn:${Partition}:datasync:${Region}:${AccountId}:location/${LocationId}`	aws:ResourceTag/${TagKey} (p. 910)
task	`arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}`	aws:ResourceTag/${TagKey} (p. 910)
taskexecution	`arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}/execution/${ExecutionId}`	

DataSync에 사용되는 조건 키

DataSync는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열

AWS DeepComposer에 사용되는 작업, 리소스 및 조건 키

AWS DeepComposer(서비스 접두사: `deepcomposer`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS DeepComposer에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateCoupon [권한만 해당]	DeepComposer 쿠폰(또는 DSN)을 요청의 발신자와 연결된 계정에 연결합니다.	쓰기			
CreateAudio [권한만 해당]	미디 구성을 wav 또는 mp3 파일로 변환하여 오디오 파일을 만듭니다.	쓰기	composition* (p. 912)		
CreateComposition [권한만 해당]	멀티 트랙 미디 구성을 만듭니다.	쓰기			
CreateModel [권한만 해당]	사용자가 제공한 피아노 멜로디에 대한 추론을 수행하여 다중 트랙 미디 구성을 만들 수 있는 생성 모델을 생성/학습하기 시작합니다.	쓰기			
DeleteComposition [권한만 해당]	구성을 삭제합니다.	쓰기	composition* (p. 912)		
DeleteModel	모델을 삭제합니다.	쓰기	model* (p. 912)		
GetComposition [권한만 해당]	구성에 대한 정보를 반환합니다.	Read	composition* (p. 912)		
GetModel [권한만 해당]	모델에 대한 정보를 반환합니다.	Read	model* (p. 912)		
GetSampleModel [권한만 해당]	샘플/사전 학습된 DeepComposer 모델에 대한 정보를 반환합니다.	Read			
ListCompositions [권한만 해당]	요청의 발신자가 소유한 모든 구성의 목록을 반환합니다.	List			
ListModels [권한만 해당]	요청의 발신자가 소유한 모든 모델의 목록을 반환합니다.	List			
ListSampleModels [권한만 해당]	DeepComposer 서비스에서 제공하는 모든 샘플/사전 학습된 모델의 목록을 반환합니다.	List			
ListTrainingTopics [권한만 해당]	모델을 생성/학습하기 위한 모든 교육 옵션 또는 주제의 목록을 반환합니다.	List			
UpdateComposition [권한만 해당]	구성과 연결된 변경 가능 속성을 수정합니다.	쓰기	composition* (p. 912)		
UpdateModel [권한만 해당]	모델과 연결된 변경 가능 속성을 수정합니다.	쓰기	model* (p. 912)		

AWS DeepComposer에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 910)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
model	`arn:${Partition}:deepcomposer:${Region}:${Account}:model/${ModelId}`	
composition	`arn:${Partition}:deepcomposer:${Region}:${Account}:composition/${CompositionId}`	
audio	`arn:${Partition}:deepcomposer:${Region}:${Account}:audio/${AudioId}`	

AWS DeepComposer에 사용되는 조건 키

DeepComposer에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS DeepLens에 사용되는 작업, 리소스 및 조건 키

AWS DeepLens(서비스 접두사: `deeplens`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

주제

AWS DeepLens에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateServiceRoleToAccount	사용자의 계정을 AWS DeepLens 서비스와 연결하는 데 필요한 다	권한 관리			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	양한 권한을 제어하는 IAM 역할과 연결합니다.				
BatchGetDevice	AWS DeepLens 디바이스의 목록을 검색합니다.	Read	device* (p. 914)		
BatchGetModel	AWS DeepLens 모델의 목록을 검색합니다.	Read	model* (p. 914)		
BatchGetProject	AWS DeepLens 프로젝트의 목록을 검색합니다.	Read	project* (p. 914)		
CreateDeviceCertificates	AWS DeepLens 디바이스를 성공적으로 인증하고 등록하는 데 사용되는 인증서 패키지를 생성합니다.	쓰기			
CreateModel	새 AWS DeepLens 모델을 생성합니다.	쓰기			
CreateProject	새 AWS DeepLens 프로젝트를 생성합니다.	쓰기			
DeleteModel	AWS DeepLens 모델을 삭제합니다.	쓰기	model* (p. 914)		
DeleteProject	AWS DeepLens 프로젝트를 삭제합니다.	쓰기	project* (p. 914)		
DeployProject	AWS DeepLens 프로젝트를 등록된 AWS DeepLens 디바이스에 배포합니다.	쓰기	device* (p. 914)		
			project* (p. 914)		
DeregisterDevice	등록된 AWS DeepLens 디바이스에 대해 디바이스 등록 해제 워크플로를 시작합니다.	쓰기	device* (p. 914)		
GetAssociatedResources	사용자의 계정과 연결된 계정 수준 리소스를 검색합니다.	Read			
GetDeploymentStatus	특정 AWS DeepLens 디바이스의 배포 상태를 연결된 메타데이터와 함께 검색합니다.	Read			
GetDevice	AWS DeepLens 디바이스에 대한 정보를 검색합니다.	Read	device* (p. 914)		
GetModel	AWS DeepLens 모델을 검색합니다.	Read	model* (p. 914)		
GetProject	AWS DeepLens 프로젝트를 검색합니다.	Read	project* (p. 914)		
ImportProjectFromTemplate	샘플 프로젝트 템플릿에서 새 AWS DeepLens 프로젝트를 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListDeployments	AWS DeepLens 배포 식별자의 목록을 검색합니다.	List			
ListDevices	AWS DeepLens 디바이스 식별자의 목록을 검색합니다.	List			
ListModels	AWS DeepLens 모델 식별자의 목록을 검색합니다.	List			
ListProjects	AWS DeepLens 프로젝트 식별자의 목록을 검색합니다.	List			
RegisterDevice	AWS DeepLens 디바이스에 대해 디바이스 등록 워크플로를 시작합니다.	쓰기			
RemoveProject	AWS DeepLens 디바이스에서 배포된 AWS DeepLens 프로젝트를 제거합니다.	쓰기	device* (p. 914)		
UpdateProject	기존 AWS DeepLens 프로젝트를 업데이트합니다.	쓰기	project* (p. 914)		

AWS DeepLens에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 912)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
device	`arn:${Partition}:deeplens:${Region}:${Account}:device/${DeviceName}`	
project	`arn:${Partition}:deeplens:${Region}:${Account}:project/${ProjectName}`	
model	`arn:${Partition}:deeplens:${Region}:${Account}:model/${ModelName}`	

AWS DeepLens에 사용되는 조건 키

DeepLens에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS DeepRacer에 사용되는 작업, 리소스 및 조건 키

AWS DeepRacer(서비스 접두사: `deepracer`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS DeepRacer에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CloneReinforcementLearningModel [권한만 해당]	기존 DeepRacer 모델을 복제할 수 있는 권한을 부여합니다.	쓰기	reinforcement_learning_model* (p. 917)		
			track* (p. 917)		
CreateAccountResources [권한만 해당]	사용자를 대신하여 DeepRacer가 필요로 하는 리소스를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateLeaderboardSubmission [권한만 해당]	리더보드에 대해 평가할 DeepRacer 모델을 제출할 수 있는 권한을 부여합니다.	쓰기	leaderboard* (p. 918)		
			reinforcement_learning_model* (p. 917)		
CreateReinforcementLearningModel [권한만 해당]	DeepRacer를 위한 강화 학습 모델을 생성할 수 있는 권한을 부여합니다.	쓰기	track* (p. 917)		
DeleteAccountResources [권한만 해당]	사용자를 대신하여 DeepRacer가 생성한 리소스를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteModel [권한만 해당]	DeepRacer 모델을 삭제할 수 있는 권한을 부여합니다.	쓰기	reinforcement_learning_model* (p. 917)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetAccountResources [권한만 해당]	사용자를 대신하여 DeepRacer가 생성한 리소스를 검색할 수 있는 권한을 부여합니다.	Read			
GetAlias [권한만 해당]	리더보드에 DeepRacer 모델을 제출하기 위해 사용자의 별칭을 검색할 수 있는 권한을 부여합니다.	Read			
GetEvaluation [권한만 해당]	기존 DeepRacer 모델의 평가 작업에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	evaluation_job* (p. 917)		
GetLatestUserSubmission [권한만 해당]	사용자를 위해 최근에 제출된 DeepRacer 모델이 리더보드에서 어떻게 수행되었는지에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	leaderboard* (p. 918)		
GetLeaderboard [권한만 해당]	리더보드에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	leaderboard* (p. 918)		
GetModel [권한만 해당]	기존 DeepRacer 모델에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	reinforcement_learning_model* (p. 917)		
GetRankedUserSubmission [권한만 해당]	리더보드에 배치된 사용자의 DeepRacer 모델 성능에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	leaderboard* (p. 918)		
GetTrack [권한만 해당]	DeepRacer 트랙에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	track* (p. 917)		
GetTrainingJob [권한만 해당]	기존 DeepRacer 모델의 교육 작업에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	training_job* (p. 917)		
ListEvaluations [권한만 해당]	DeepRacer 모델의 평가 작업을 나열할 수 있는 권한을 부여합니다.	List	reinforcement_learning_model* (p. 917)		
ListLeaderboardSubmissions [권한만 해당]	리더보드에 사용자의 DeepRacer 모델에 대한 모든 제출물을 나열할 수 있는 권한을 부여합니다.	List	leaderboard* (p. 918)		
ListLeaderboards [권한만 해당]	사용 가능한 모든 리더보드를 나열할 수 있는 권한을 부여합니다.	List			
ListModels [권한만 해당]	기존의 모든 DeepRacer 모델을 나열할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTracks [권한만 해당]	모든 DeepRacer 트랙을 나열할 수 있는 권한을 부여합니다.	List			
ListTrainingJobs [권한만 해당]	DeepRacer 모델의 교육 작업을 나열할 수 있는 권한을 부여합니다.	List	reinforcement_learning_model* (p. 917)		
SetAlias [권한만 해당]	리더보드에 DeepRacer 모델을 제출하기 위한 사용자의 별칭을 설정할 수 있는 권한을 부여합니다.	쓰기			
StartEvaluation [권한만 해당]	시뮬레이션된 환경에서 DeepRacer 모델을 평가할 수 있는 권한을 부여합니다.	쓰기	reinforcement_learning_model* (p. 917)		
			track* (p. 917)		
StopEvaluation [권한만 해당]	DeepRacer 모델 평가를 중지할 수 있는 권한을 부여합니다.	쓰기	evaluation_job* (p. 917)		
StopTrainingReinforcementLearningModel [권한만 해당]	DeepRacer 모델 교육을 중지할 수 있는 권한을 부여합니다.	쓰기	reinforcement_learning_model* (p. 917)		
TestRewardFunction [권한만 해당]	보상 기능의 정확성을 테스트할 수 있는 권한을 부여합니다.	쓰기			

AWS DeepRacer에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 915)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
reinforcement_learning_model	`arn:${Partition}:deepracer:${Region}:${Account}:model/reinforcement_learning/${ResourceId}`	
training_job	`arn:${Partition}:deepracer:${Region}:${Account}:training_job/${ResourceId}`	
evaluation_job	`arn:${Partition}:deepracer:${Region}:${Account}: evaluation_job/${ResourceId}`	
leaderboard_evaluation_job	`arn:${Partition}:deepracer:${Region}:${Account}:leaderboard_evaluation_job/${ResourceId}`	
track	`arn:${Partition}:deepracer:${Region}::track/${ResourceId}`	

리소스 유형	ARN	조건 키
leaderboard	`arn:${Partition}:deepracer:${Region}::leaderboard/${ResourceId}`	

AWS DeepRacer에 사용되는 조건 키

DeepRacer에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Detective에 사용되는 작업, 리소스 및 조건 키

Amazon Detective(서비스 접두사: `detective`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Detective에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptInvitation	동작 그래프의 멤버가 되라는 초대를 수락할 수 있는 권한을 부여합니다.	쓰기	Graph* (p. 920)		
CreateGraph	동작 그래프를 생성하고 보안 정보의 집계를 시작할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateMembers	이 계정에서 관리하는 동작 그래프에서 하나 이상의 계정에 대해 멤버십을 요청할 수 있는 권한을 부여합니다.	쓰기	Graph* (p. 920)		
DeleteGraph	동작 그래프를 삭제하고 보안 정보 집계를 중지할 수 있는 권한을 부여합니다.	쓰기	Graph* (p. 920)		
DeleteMembers	이 계정에서 관리하는 동작 그래프에서 멤버 계정을 제거할 수 있는 권한을 부여합니다.	쓰기	Graph* (p. 920)		
DisassociateMembership	동작 그래프와 이 계정의 연결을 제거할 수 있는 권한을 부여합니다.	쓰기	Graph* (p. 920)		
GetFreeTrialEligibility [권한만 해당]	무료 평가판 기간에 대한 동작 그래프의 자격을 검색할 수 있는 권한을 부여합니다.	Read	Graph* (p. 920)		
GetGraphIngestState [권한만 해당]	동작 그래프의 데이터 수집 상태를 검색할 수 있는 권한을 부여합니다.	Read	Graph* (p. 920)		
GetMembers	동작 그래프의 지정된 멤버에 대한 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read	Graph* (p. 920)		
GetPricingInformation [권한만 해당]	Amazon Detective의 요금에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read			
GetUsageInformation [권한만 해당]	동작 그래프의 사용 정보를 나열할 수 있는 권한을 부여합니다.	Read	Graph* (p. 920)		
ListGraphs	이 계정에서 관리하는 동작 그래프를 나열할 수 있는 권한을 부여합니다.	List			
ListInvitations	이 계정이 가입 초대를 받은 동작 그래프에 대한 세부 정보를 검색할 수 있는 권한을 부여합니다.	List			
ListMembers	동작 그래프의 모든 멤버에 대한 세부 정보를 검색할 수 있는 권한을 부여합니다.	List	Graph* (p. 920)		
RejectInvitation	동작 그래프의 멤버가 되라는 초대를 거부할 수 있는 권한을 부여합니다.	쓰기	Graph* (p. 920)		
SearchGraph [권한만 해당]	동작 그래프에 저장된 데이터를 검색할 수 있는 권한을 부여합니다.	Read	Graph* (p. 920)		

Amazon Detective에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 918)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Graph	`arn:${Partition}:detective:${Region}:${Account}:graph:${ResourceId}`	

Amazon Detective의 조건 키

Detective에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Device Farm에 사용되는 작업, 리소스 및 조건 키

AWS Device Farm(서비스 접두사: `devicefarm`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Device Farm에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateDevicePool	프로젝트에서 디바이스 풀을 생성할 수 있는 권한을 부여합니다.	쓰기	project* (p. 928)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateInstanceProfile	디바이스 인스턴스 프로파일을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateNetworkProfile	프로젝트에서 네트워크 프로파일을 생성할 수 있는 권한을 부여합니다.	쓰기	project* (p. 928)		
CreateProject	모바일 테스트를 위한 프로젝트를 생성할 수 있는 권한을 부여합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 930) aws:TagKeys (p. 930)	
CreateRemoteAccessSession	디바이스 인스턴스에 대한 원격 액세스 세션을 시작할 수 있는 권한을 부여합니다.	쓰기	device* (p. 929)		
			project* (p. 928)		
			deviceinstance (p. 929)		
			upload (p. 929)		
CreateTestGridProject	데스크톱 테스트를 위한 프로젝트를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateTestGridUrl	테스트 그리드 서비스에 액세스하는 데 사용되는 미리 서명된 새로운 URL을 생성 할 수 있는 권한을 부여합니다.	쓰기	testgrid-project* (p. 929)		
CreateUpload	프로젝트에서 새로운 파일 또는 앱을 업로드할 수 있는 권한을 부여합니다.	쓰기	project* (p. 928)		
CreateVPCEConfiguration	Amazon Virtual Private Cloud(VPC) 엔드포인트 구성을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteDevicePool	사용자가 생성한 디바이스 풀을 삭제할 수 있는 권한을 부여합니다.	쓰기	devicepool* (p. 929)		
DeleteInstanceProfile	사용자가 생성한 인스턴스 프로파일을 삭제할 수 있는 권한을 부여합니다.	쓰기	instanceprofile* (p. 929)		
DeleteNetworkProfile	사용자가 생성한 네트워크 프로파일을 삭제할 수 있는 권한을 부여합니다.	쓰기	networkprofile* (p. 929)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteProject	모바일 테스트 프로젝트를 삭제할 수 있는 권한을 부여합니다.	쓰기	project* (p. 928)		
DeleteRemoteAccessSession	완료된 원격 액세스 세션과 그 결과를 삭제할 수 있는 권한을 부여합니다.	쓰기	session* (p. 929)		
DeleteRun	실행을 삭제할 수 있는 권한을 부여합니다.	쓰기	run* (p. 928)		
DeleteTestGridProject	데스크톱 테스트 프로젝트를 삭제할 수 있는 권한을 부여합니다.	쓰기	testgrid-project* (p. 929)		
DeleteUpload	사용자가 업로드한 파일을 삭제할 수 있는 권한을 부여합니다.	쓰기	upload* (p. 929)		
DeleteVPCEConfiguration	Amazon Virtual Private Cloud(VPC) 엔드포인트 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기	vpceconfiguration* (p. 929)		
GetAccountSettings	계정에서 구매한 과금되지 않는 iOS 및/또는 과금되지 않는 Android 디바이스의 수를 가져올 수 있는 권한을 부여합니다.	Read			
GetDevice	고유한 디바이스 유형 정보를 가져올 수 있는 권한을 부여합니다.	Read	device* (p. 929)		
GetDeviceInstance	디바이스 인스턴스 정보를 가져올 수 있는 권한을 부여합니다.	Read	deviceinstance* (p. 929)		
GetDevicePool	디바이스 풀 정보를 가져올 수 있는 권한을 부여합니다.	Read	devicepool* (p. 929)		
GetDevicePoolCompatibility	테스트 및/또는 앱과 디바이스 풀의 호환성에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	devicepool* (p. 929) upload (p. 929)		
GetInstanceProfile	인스턴스 프로파일 정보를 가져올 수 있는 권한을 부여합니다.	Read	instanceprofile* (p. 929)		
GetJob	작업 정보를 가져올 수 있는 권한을 부여합니다.	Read	job* (p. 929)		
GetNetworkProfile	네트워크 프로파일 정보를 가져올 수 있는 권한을 부여합니다.	Read	networkprofile* (p. 929)		
GetOfferingStatus	AWS 계정에서 구매한 모든 상품의 현재 및 향후 상태를 가져올 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetProject	모바일 테스트 프로젝트에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	project* (p. 928)		
GetRemoteAccessSession	현재 실행 중인 원격 액세스 세션에 대한 링크를 가져올 수 있는 권한을 부여합니다.	Read	session* (p. 929)		
GetRun	실행 정보를 가져올 수 있는 권한을 부여합니다.	Read	run* (p. 928)		
GetSuite	테스트 제품군에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	suite* (p. 929)		
GetTest	테스트 사례에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	test* (p. 929)		
GetTestGridProject	데스크톱 테스트 프로젝트에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	testgrid-project* (p. 929)		
GetTestGridSession	테스트 그리드 세션에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	testgrid-project (p. 929)		
			testgrid-session (p. 929)		
GetUpload	업로드된 파일에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	upload* (p. 929)		
GetVPCEConfiguration	Amazon Virtual Private Cloud(VPC) 엔드포인트 구성에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	vpceconfiguration* (p. 929)		
InstallToRemoteAccessSession	원격 액세스 세션에서 애플리케이션을 디바이스에 설치할 수 있는 권한을 부여합니다.	쓰기	session* (p. 929)		
			upload* (p. 929)		
ListArtifacts	프로젝트에서 아티팩트를 나열할 수 있는 권한을 부여합니다.	List	job (p. 929)		
			run (p. 928)		
			suite (p. 929)		
			test (p. 929)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListDeviceInstances	디바이스 인스턴스에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List			
ListDevicePools	디바이스 풀에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List	project* (p. 928)		
ListDevices	고유한 디바이스 유형에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List			
ListInstanceProfiles	디바이스 인스턴스 프로파일에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List			
ListJobs	실행에서 작업 정보를 나열할 수 있는 권한을 부여합니다.	List	run* (p. 928)		
ListNetworkProfiles	프로젝트에서 네트워크 프로파일에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List	project* (p. 928)		
ListOfferingPromotions	상품 프로모션을 나열할 수 있는 권한을 부여합니다.	List			
ListOfferingTransactions	AWS 계정에 대한 모든 구매, 갱신 및 시스템 갱신 트래잭션 내역을 나열할 수 있는 권한을 부여합니다.	List			
ListOfferings	사용자가 API를 통해 관리할 수 있는 제품 또는 서비스를 나열할 수 있는 권한을 부여합니다.	List			
ListProjects	AWS 계정에서 모바일 테스트 프로젝트의 정보를 나열할 수 있는 권한을 부여합니다.	List			
ListRemoteAccessSessions	현재 실행 중인 원격 액세스 세션에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List	project* (p. 928)		
ListRuns	프로젝트에서 실행 정보를 나열할 수 있는 권한을 부여합니다.	List	project* (p. 928)		
ListSamples	프로젝트에서 샘플 정보를 나열할 수 있는 권한을 부여합니다.	List	job* (p. 929)		
ListSuites	작업에서 테스트 제품군에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List	job* (p. 929)		
ListTagsForResource	리소스 태그를 나열할 수 있는 권한을 부여합니다.	List	device (p. 929)		
			deviceinstance (p. 929)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			devicepool (p. 929)		
			instanceprofile (p. 929)		
			networkprofile (p. 929)		
			project (p. 928)		
			run (p. 928)		
			session (p. 929)		
			testgrid-project (p. 929)		
			testgrid-session (p. 929)		
			vpceconfiguration (p. 929)		
ListTestGridProjects	AWS 계정에서 데스크톱 테스트 프로젝트의 정보를 나열할 수 있는 권한을 부여합니다.	List			
ListTestGridSessionActions	테스트 그리드 세션 중에 수행된 세션 작업을 나열할 수 있는 권한을 부여합니다.	List	testgrid-session* (p. 929)		
ListTestGridSessionArtifacts	테스트 그리드 세션에서 생성된 아티팩트를 나열할 수 있는 권한을 부여합니다.	List	testgrid-session* (p. 929)		
ListTestGridSessions	테스트 그리드 프로젝트 내의 세션을 나열 할 수 있는 권한을 부여합니다.	List	testgrid-project* (p. 929)		
ListTests	테스트 제품군에서 테스트 정보를 나열할 수 있는 권한을 부여합니다.	List	suite* (p. 929)		
ListUniqueProblems	실행에서 고유한 문제에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List	run* (p. 928)		
ListUploads	프로젝트에서 업로드 정보를 나열할 수 있는 권한을 부여합니다.	List	project* (p. 928)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListVPCEConfigurations	Amazon Virtual Private Cloud(VPC) 엔드포인트 구성에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List			
PurchaseOffering	AWS 계정에서 상품을 구매할 수 있는 권한을 부여합니다.	쓰기			
RenewOffering	상품에 대해 갱신할 디바이스 수량을 설정할 수 있는 권한을 부여합니다.	쓰기			
ScheduleRun	실행을 예약할 수 있는 권한을 부여합니다.	쓰기	project* (p. 928)		
			devicepool (p. 929)		
			upload (p. 929)		
	시나리오: Device Pool as filter		devicepool* (p. 929) project* (p. 928) upload (p. 929)		
	시나리오: Device Selection Configuration as filter		project* (p. 928) upload (p. 929)		
StopJob	실행 중인 작업을 종료할 수 있는 권한을 부여합니다.	쓰기	job* (p. 929)		
StopRemoteAccessSession	실행 중인 원격 액세스 세션을 종료할 수 있는 권한을 부여합니다.	쓰기	session* (p. 929)		
StopRun	실행 중인 테스트를 종료할 수 있는 권한을 부여합니다.	쓰기	run* (p. 928)		
TagResource	리소스에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	device (p. 929)		
			deviceinstance (p. 929)		
			devicepool (p. 929)		
			instanceprofile (p. 929)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			networkprofile (p. 929)		
			project (p. 928)		
			run (p. 928)		
			session (p. 929)		
			testgrid-project (p. 929)		
			testgrid-session (p. 929)		
			vpceconfiguration (p. 929)		
				aws:RequestTag/${TagKey} (p. 930) aws:TagKeys (p. 930)	
UntagResource	리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	device (p. 929)		
			deviceinstance (p. 929)		
			devicepool (p. 929)		
			instanceprofile (p. 929)		
			networkprofile (p. 929)		
			project (p. 928)		
			run (p. 928)		
			session (p. 929)		
			testgrid-project (p. 929)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			testgrid-session (p. 929)		
			vpceconfiguration (p. 929)		
				aws:TagKeys (p. 930)	
UpdateDeviceInstance	기존 디바이스 인스턴스를 수정할 수 있는 권한을 부여합니다.	쓰기	deviceinstance* (p. 929)		
			instanceprofile (p. 929)		
UpdateDevicePool	기존 디바이스 풀을 수정할 수 있는 권한을 부여합니다.	쓰기	devicepool* (p. 929)		
UpdateInstanceProfile	기존 인스턴스 프로파일을 수정할 수 있는 권한을 부여합니다.	쓰기	instanceprofile* (p. 929)		
UpdateNetworkProfile	기존 네트워크 프로파일을 수정할 수 있는 권한을 부여합니다.	쓰기	networkprofile* (p. 929)		
UpdateProject	기존 모바일 테스트 프로젝트를 수정할 수 있는 권한을 부여합니다.	쓰기	project* (p. 928)		
UpdateTestGridProject	기존 데스크톱 테스트 프로젝트를 수정할 수 있는 권한을 부여합니다.	쓰기	testgrid-project* (p. 929)		
UpdateUpload	기존 업로드를 수정할 수 있는 권한을 부여합니다.	쓰기	upload* (p. 929)		
UpdateVPCEConfiguration	기존 Amazon Virtual Private Cloud(VPC) 엔드포인트 구성을 수정할 수 있는 권한을 부여합니다.	쓰기	vpceconfiguration* (p. 929)		

AWS Device Farm에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 920)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
project	`arn:${Partition}:devicefarm:${Region}:${Account}:project:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
run	`arn:${Partition}:devicefarm:${Region}:${Account}:run:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)

리소스 유형	ARN	조건 키
job	`arn:${Partition}:devicefarm:${Region}:${Account}:job:${ResourceId}`	
suite	`arn:${Partition}:devicefarm:${Region}:${Account}:suite:${ResourceId}`	
test	`arn:${Partition}:devicefarm:${Region}:${Account}:test:${ResourceId}`	
upload	`arn:${Partition}:devicefarm:${Region}:${Account}:upload:${ResourceId}`	
artifact	`arn:${Partition}:devicefarm:${Region}:${Account}:artifact:${ResourceId}`	
sample	`arn:${Partition}:devicefarm:${Region}:${Account}:sample:${ResourceId}`	
networkprofile	`arn:${Partition}:devicefarm:${Region}:${Account}:networkprofile:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
deviceinstance	`arn:${Partition}:devicefarm:${Region}::deviceinstance:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
session	`arn:${Partition}:devicefarm:${Region}:${Account}:session:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
devicepool	`arn:${Partition}:devicefarm:${Region}:${Account}:devicepool:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
device	`arn:${Partition}:devicefarm:${Region}::device:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
instanceprofile	`arn:${Partition}:devicefarm:${Region}:${Account}:instanceprofile:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
vpceconfiguration	`arn:${Partition}:devicefarm:${Region}:${Account}:vpceconfiguration:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
testgrid-project	`arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-project:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)
testgrid-session	`arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-session:${ResourceId}`	aws:ResourceTag/${TagKey} (p. 930)

AWS Device Farm에 사용되는 조건 키

AWS Device Farm은 `Condition` 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Direct Connect에 사용되는 작업, 리소스 및 조건 키

AWS Direct Connect(서비스 접두사: `directconnect`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Direct Connect에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptDirectConnectGatewayAssociationProposal	가상 프라이빗 게이트웨이를 Direct Connect 게이트웨이에 연결하라는 제안 요청을 수락합니다.	쓰기	dx-gateway* (p. 937)		
AllocateConnectionOnInterconnect	인터커넥트에서 호스팅 연결을 생성합니다.	쓰기	dxcon* (p. 936)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AllocateHostedConnection	AWS Direct Connect 파트너의 네트워크와 특정 AWS Direct Connect 위치 간에 새 호스팅 연결을 생성합니다.	쓰기	dxcon (p. 936)		
			dxlag (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
AllocatePrivateVirtualInterface	다른 고객이 소유할 프라이빗 가상 인터페이스를 프로비저닝합니다.	쓰기	dxcon (p. 936)		
			dxlag (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
AllocatePublicVirtualInterface	다른 고객이 소유할 퍼블릭 가상 인터페이스를 프로비저닝합니다.	쓰기	dxcon (p. 936)		
			dxlag (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
AllocateTransitVirtualInterface	다른 고객이 소유할 전송 가상 인터페이스를 프로비저닝합니다.	쓰기	dxcon (p. 936)		
			dxlag (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
AssociateConnectionWithLag	연결을 LAG와 연결합니다.	쓰기	dxcon* (p. 936)		
			dxlag* (p. 936)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateHostedConnection	호스팅 연결 및 그 가상 인터페이스를 링크 집계 그룹(LAG) 또는 인터커넥트와 연결합니다.	쓰기	dxcon* (p. 936)		
			dxcon (p. 936)		
			dxlag (p. 936)		
AssociateVirtualInterface	가상 인터페이스를 지정된 링크 집계 그룹(LAG) 또는 연결과 연결합니다.	쓰기	dxvif* (p. 937)		
			dxcon (p. 936)		
			dxlag (p. 936)		
ConfirmConnection	인터커넥트에서 호스팅 연결의 생성을 확인합니다.	쓰기	dxcon* (p. 936)		
ConfirmPrivateVirtualInterface	다른 고객이 생성한 프라이빗 가상 인터페이스의 소유권을 적용합니다.	쓰기	dxvif* (p. 937)		
ConfirmPublicVirtualInterface	다른 고객이 생성한 퍼블릭 가상 인터페이스의 소유권을 적용합니다	쓰기	dxvif* (p. 937)		
ConfirmTransitVirtualInterface	다른 고객이 생성한 전송 가상 인터페이스의 소유권을 적용합니다	쓰기	dxvif* (p. 937)		
CreateBGPPeer	지정된 가상 인터페이스에서 BGP 피어를 생성합니다.	쓰기	dxvif* (p. 937)		
CreateConnection	고객 네트워크와 특정 AWS Direct Connect 위치 간에 새 연결을 생성합니다.	쓰기	dxlag (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
CreateDirectConnectGateway	가상 인터페이스 집합을 가상 프라이빗 게이트웨이에 연결할 수 있게 해주는 중간 객체인 Direct Connect 게이트웨이를 생성합니다.	쓰기			
CreateDirectConnectGatewayAssociation	Direct Connect 게이트웨이와 가상 프라이빗 게이트웨이 간 연결을 생성합니다.	쓰기	dx-gateway* (p. 937)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateDirectConnectGatewayAssociationProposal	지정된 가상 프라이빗 게이트웨이를 지정된 Direct Connect 게이트웨이와 연결하라는 제안을 생성합니다.	쓰기	dx-gateway* (p. 937)		
CreateInterconnect	AWS Direct Connect 파트너의 네트워크와 특정 AWS Direct Connect 위치 간에 새 인터커넥트를 생성합니다.	쓰기	dxlag (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
CreateLag	고객과 AWS Direct Connect 위치 사이의 지정된 수의 번들 물리적 연결로 링크 집계 그룹(LAG)을 생성합니다.	쓰기	dxcon (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
CreatePrivateVirtualInterface	새로운 프라이빗 가상 인터페이스를 생성합니다.	쓰기	dxcon (p. 936)		
			dxlag (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
CreatePublicVirtualInterface	새로운 퍼블릭 가상 인터페이스를 생성합니다.	쓰기	dxcon (p. 936)		
			dxlag (p. 936)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
CreateTransitVirtualInterface	새 전송 가상 인터페이스를 생성합니다.	쓰기	dxcon (p. 936)		
			dxlag (p. 936)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
DeleteBGPPeer	지정된 고객 주소 및 ASN을 사용하여 지정된 가상 인터페이스에서 지정된 BGP를 삭제합니다.	쓰기	dxvif* (p. 937)		
DeleteConnection	연결을 삭제합니다.	쓰기	dxcon* (p. 936)		
DeleteDirectConnectGateway	지정된 Direct Connect 게이트웨이를 삭제합니다.	쓰기	dx-gateway* (p. 937)		
DeleteDirectConnectGatewayAssociation	지정된 Direct Connect 게이트웨이와 가상 프라이빗 게이트웨이 간 연결을 삭제합니다.	쓰기	dx-gateway* (p. 937)		
DeleteDirectConnectGatewayAssociationProposal	지정된 Direct Connect 게이트웨이와 가상 프라이빗 게이트웨이 간의 연결 제안 요청을 삭제합니다.	쓰기			
DeleteInterconnect	지정된 인터커넥트를 삭제합니다.	쓰기	dxcon* (p. 936)		
DeleteLag	지정된 링크 집계 그룹(LAG)을 삭제합니다.	쓰기	dxlag* (p. 936)		
DeleteVirtualInterface	가상 인터페이스를 삭제합니다.	쓰기	dxvif* (p. 937)		
DescribeConnectionLoa	연결에 대한 LOA-CFA를 반환합니다.	Read	dxcon* (p. 936)		
DescribeConnections	이 리전의 모든 연결을 표시합니다.	Read	dxcon (p. 936)		
DescribeConnectionsOnInterconnect	지정된 인터커넥트에서 프로비저닝된 연결 목록을 반환합니다.	Read	dxcon* (p. 936)		
DescribeDirectConnectGatewayAssociationProposals	가상 프라이빗 게이트웨이와 Direct Connect 게이트웨이 간 연결을 위한 하나 이상의 연결 제안을 설명합니다.	Read	dx-gateway (p. 937)		
DescribeDirectConnectGatewayAssociations	Direct Connect 게이트웨이와 가상 프라이빗 게이트웨이 간 연결을 나열합니다.	Read	dx-gateway (p. 937)		
DescribeDirectConnectGatewayAttachments	Direct Connect 게이트웨이와 가상 인터페이스 간 연결을 나열합니다.	Read	dx-gateway (p. 937)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeDirectConnectGateways	모든 Direct Connect 게이트웨이 또는 지정된 Direct Connect 게이트웨이만 나열합니다.	Read	dx-gateway (p. 937)		
DescribeHostedConnections	지정된 인터커넥트 또는 링크 집계 그룹(LAG)에서 프로비저닝된 호스팅 연결을 나열합니다.	Read	dxcon (p. 936)		
			dxlag (p. 936)		
DescribeInterconnectLoa	인터커넥트에 대한 LOA-CFA를 반환합니다.	Read	dxcon* (p. 936)		
DescribeInterconnects	AWS 계정이 소유한 인터커넥트 목록을 반환합니다.	Read	dxcon (p. 936)		
DescribeLags	모든 링크 집계 그룹(LAG) 또는 지정된 LAG를 설명합니다.	Read	dxlag (p. 936)		
DescribeLoa	연결, 인터커넥트 또는 링크 집계 그룹(LAG)에 대한 LOA-CFA를 가져옵니다.	Read	dxcon (p. 936)		
			dxlag (p. 936)		
DescribeLocations	현재 AWS 리전에서 AWS Direct Connect 위치의 목록을 반환합니다.	List			
DescribeTags	지정된 AWS Direct Connect 리소스와 연결된 태그를 설명합니다.	Read	dxcon (p. 936)		
			dxlag (p. 936)		
			dxvif (p. 937)		
DescribeVirtualGateways	AWS 계정이 소유한 가상 프라이빗 게이트웨이의 목록을 반환합니다.	Read			
DescribeVirtualInterfaces	AWS 계정의 모든 가상 인터페이스를 표시합니다.	Read	dxcon (p. 936)		
			dxlag (p. 936)		
			dxvif (p. 937)		
DisassociateConnectionFromLag	링크 집계 그룹(LAG)에서 연결을 연결 해제합니다.	쓰기	dxcon* (p. 936)		
			dxlag* (p. 936)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
TagResource	지정된 태그를 지정된 AWS Direct Connect 리소스에 추가합니다. 각 리소스는 최대 50개의 태그를 보유할 수 있습니다.	태그 지정	dxcon (p. 936)		
			dxlag (p. 936)		
			dxvif (p. 937)		
				aws:RequestTag/${TagKey} (p. 937) aws:TagKeys (p. 937)	
UntagResource	지정된 AWS Direct Connect 리소스에서 하나 이상의 태그를 제거합니다.	태그 지정	dxcon (p. 936)		
			dxlag (p. 936)		
			dxvif (p. 937)		
				aws:TagKeys (p. 937)	
UpdateDirectConnectGateway	Direct Connect 게이트웨이 연결의 지정된 속성을 업데이트합니다.	쓰기			
UpdateLag	지정된 링크 집계 그룹(LAG)의 속성을 업데이트합니다.	쓰기	dxlag* (p. 936)		
UpdateVirtualInterfaceAttributes	지정된 가상 프라이빗 인터페이스의 지정된 속성을 업데이트합니다.	쓰기	dxvif* (p. 937)		

AWS Direct Connect에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 930)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`	aws:ResourceTag/${TagKey} (p. 937)
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`	aws:ResourceTag/${TagKey} (p. 937)

리소스 유형	ARN	조건 키
dxvif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`	aws:ResourceTag/${TagKey} (p. 937)
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`	

AWS Direct Connect의 조건 키

AWS Direct Connect는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Directory Service에 사용되는 작업, 리소스 및 조건 키

AWS Directory Service(서비스 접두사: `ds`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Directory Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptSharedDirectory	디렉터리 소유자 계정에서 보낸 디렉터리 공유 요청을 수락합니다.	쓰기	directory* (p. 943)		
AddIpRoutes	CIDR 주소 블록을 추가하여 Amazon Web Services에서 Microsoft AD와의 트래픽을 올바르게 라우팅합니다.	쓰기	directory* (p. 943)		ec2:AuthorizeSecurityGro ec2:AuthorizeSecurityGro ec2:DescribeSecurityGrou
AddTagsToResource	지정된 Amazon Directory Services 디렉터리에 대한 하나 이상의 태그를 추가하거나 덮어씁니다.	태그 지정	directory* (p. 943)		ec2:CreateTags
				aws:RequestTag/${TagKey} (p. 943) aws:TagKeys (p. 944)	
AuthorizeApplication [권한만 해당]	AWS Directory용 애플리케이션을 승인합니다.	쓰기	directory* (p. 943)		
CancelSchemaExtension	Microsoft AD 디렉터리에 대해 진행 중인 스키마 확장을 취소합니다.	쓰기	directory* (p. 943)		
CheckAlias [권한만 해당]	별칭을 사용할 수 있는지 확인합니다.	Read			
ConnectDirectory	AD Connector를 생성하여 온프레미스 디렉터리에 연결합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 943) aws:TagKeys (p. 944)	ec2:AuthorizeSecurityGro ec2:AuthorizeSecurityGro ec2:CreateNetworkInterfa ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateAlias	디렉터리에 대한 별칭을 생성하고 별칭을 디렉터리에 할당합니다.	쓰기	directory* (p. 943)		
CreateComputer	지정된 디렉터리에 컴퓨터 계정을 생성하고 컴퓨터를 디렉터리에 조인합니다.	쓰기	directory* (p. 943)		
CreateConditionalForwarder	AWS 디렉터리와 연결된 조건부 전달자를 생성합니다.	쓰기	directory* (p. 943)		
CreateDirectory	Simple AD 디렉터리를 생성합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 943) aws:TagKeys (p. 944)	ec2:AuthorizeSecurityGro ec2:AuthorizeSecurityGro ec2:CreateNetworkInterfa ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs
CreateIdentityPoolDirectory [권한만 해당]	AWS 클라우드에서 IdentityPool 디렉터리를 생성합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 943) aws:TagKeys (p. 944)	
CreateLogSubscription	실시간 디렉터리 서비스 도메인 컨트롤러 보안 로그를 AWS 계정의 지정된 CloudWatch 로그 그룹으로 전달하기 위한 구독을 생성합니다.	쓰기	directory* (p. 943)		
CreateMicrosoftAD	AWS 클라우드에 Microsoft AD를 생성합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 943) aws:TagKeys (p. 944)	ec2:AuthorizeSecurityGro ec2:AuthorizeSecurityGro ec2:CreateNetworkInterfa ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateSnapshot	AWS 클라우드에 Simple AD 또는 Microsoft AD 디렉터리의 스냅샷을 생성합니다.	쓰기	directory* (p. 943)		
CreateTrust	AWS 클라우드의 Microsoft AD와 외부 도메인 간의 AWS 신뢰 관계 측 생성을 시작합니다.	쓰기	directory* (p. 943)		
DeleteConditionalForwarder	AWS 디렉터리에 대해 설정된 조건부 전달자를 삭제합니다.	쓰기	directory* (p. 943)		
DeleteDirectory	AWS Directory Service 디렉터리를 삭제합니다.	쓰기	directory* (p. 943)		ec2:DeleteNetworkInterfa ec2:DeleteSecurityGroup ec2:DescribeNetworkInter ec2:RevokeSecurityGroup ec2:RevokeSecurityGroup
DeleteLogSubscription	지정된 로그 구독을 삭제합니다.	쓰기	directory* (p. 943)		
DeleteSnapshot	디렉터리 스냅샷을 삭제합니다.	쓰기	directory* (p. 943)		
DeleteTrust	AWS 클라우드의 Microsoft AD와 외부 도메인 간의 기존 신뢰 관계를 삭제합니다.	쓰기	directory* (p. 943)		
DeregisterCertificate	보안 LDAP 연결을 위해 등록된 인증서를 시스템에서 삭제합니다.	쓰기	directory* (p. 943)		
DeregisterEventTopic	지정된 디렉터리를 지정된 SNS 주제에 대한 게시자로 제거합니다.	쓰기	directory* (p. 943)		
DescribeCertificate	보안 LDAP 연결을 위해 등록된 인증서에 대한 정보를 표시합니다.	Read	directory* (p. 943)		
DescribeConditionalForwarders	이 계정의 조건부 전달자에 대한 정보를 가져옵니다.	Read	directory* (p. 943)		
DescribeDirectories	이 계정에 속한 디렉터리에 대한 정보를 가져옵니다.	List			
DescribeDomainControllers	디렉터리의 모든 도메인 컨트롤러에 대한 정보를 제공합니다.	Read	directory* (p. 943)		
DescribeEventTopics	지정된 디렉터리에서 상태 메시지를 수신한 SNS 주제에 대한 정보를 가져옵니다.	Read	directory* (p. 943)		
DescribeLDAPSSettings	지정된 디렉터리에 대한 LDAP 보안 상태를 설명합니다.	Read	directory* (p. 943)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeSharedDirectories	계정의 공유 디렉터리를 반환합니다.	Read	directory* (p. 943)		
DescribeSnapshots	이 계정에 속한 디렉터리 스냅샷에 대한 정보를 가져옵니다.	Read			
DescribeTrusts	이 계정의 신뢰 관계에 대한 정보를 가져옵니다.	Read			
DisableLDAPS	지정된 디렉터리에 대한 LDAP 보안 호출을 비활성화합니다.	쓰기	directory* (p. 943)		
DisableRadius	AD Connector 디렉터리에 대한 RADIUS(Remote Authentication Dial In User Service) 서버를 사용하여 멀티 팩터 인증(MFA)을 비활성화합니다.	쓰기	directory* (p. 943)		
DisableSso	디렉터리에 대한 Single Sign-On을 비활성화합니다.	쓰기	directory* (p. 943)		
EnableLDAPS	특정 디렉터리의 스위치를 활성화하여 LDAP 보안 호출을 항상 사용합니다.	쓰기	directory* (p. 943)		
EnableRadius	AD Connector 디렉터리에 대한 RADIUS(Remote Authentication Dial In User Service) 서버를 사용하여 멀티 팩터 인증(MFA)을 활성화합니다.	쓰기	directory* (p. 943)		
EnableSso	디렉터리에 대한 Single Sign-On을 활성화합니다.	쓰기	directory* (p. 943)		
GetAuthorizedApplicationDetails [권한만 해당]		Read	directory* (p. 943)		
GetDirectoryLimits	현재 리전에 대한 디렉터리 제한 정보를 가져옵니다.	Read			
GetSnapshotLimits	디렉터리에 대한 수동 스냅샷 제한을 가져옵니다.	Read	directory* (p. 943)		
ListAuthorizedApplications [권한만 해당]	디렉터리에 대해 승인된 AWS 애플리케이션을 가져옵니다.	Read	directory* (p. 943)		
ListCertificates	지정된 디렉터리에 대해 보안 LDAP 연결을 위해 등록된 모든 인증서를 나열합니다.	List	directory* (p. 943)		
ListIpRoutes	디렉터리에 추가한 주소 블록을 나열합니다.	Read	directory* (p. 943)		
ListLogSubscriptions	AWS 계정의 활성 로그 구독을 나열합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListSchemaExtensions	Microsoft AD 디렉터리에 적용된 모든 스키마 확장을 나열합니다.	List	directory* (p. 943)		
ListTagsForResource	Amazon Directory Services 디렉터리의 모든 태그를 나열합니다.	Read	directory* (p. 943)		
RegisterCertificate	보안 LDAP 연결을 위한 인증서를 등록합니다.	쓰기	directory* (p. 943)		
RegisterEventTopic	디렉터리를 SNS 주제와 연결합니다.	쓰기	directory* (p. 943)		sns:GetTopicAttributes
RejectSharedDirectory	디렉터리 소유자 계정에서 보낸 디렉터리 공유 요청을 거부합니다.	쓰기	directory* (p. 943)		
RemoveIpRoutes	디렉터리에서 IP 주소 블록을 제거합니다.	쓰기	directory* (p. 943)		
RemoveTagsFromResource	Amazon Directory Services 디렉터리에서 태그를 제거합니다.	태그 지정	directory* (p. 943)		ec2:DeleteTags
				aws:RequestTag/${TagKey} (p. 943) aws:TagKeys (p. 944)	
ResetUserPassword	AWS Managed Microsoft AD 또는 Simple AD 디렉터리의 사용자에 대해 암호를 재설정합니다.	쓰기	directory* (p. 943)		
RestoreFromSnapshot	기존 디렉터리 스냅샷을 사용하여 디렉터리를 복원합니다.	쓰기	directory* (p. 943)		
ShareDirectory	AWS 계정(디렉터리 소유자)의 지정된 디렉터리를 다른 AWS 계정(디렉터리 소비자)와 공유합니다. 이 작업에서 모든 AWS 계정의 디렉터리와 AWS 리전 내 모든 Amazon VPC의 디렉터리를 사용할 수 있습니다.	쓰기	directory* (p. 943)		
StartSchemaExtension	스키마 확장을 Microsoft AD 디렉터리에 적용합니다.	쓰기	directory* (p. 943)		
UnauthorizeApplication [권한만 해당]	AWS Directory에서 애플리케이션 승인을 취소합니다.	쓰기	directory* (p. 943)		
UnshareDirectory	디렉터리 소유자와 디렉터리 소비자 간의 디렉터리 공유를 중지합니다.	쓰기	directory* (p. 943)		
UpdateConditionalForwarder	AWS 디렉터리에 대해 설정된 조건부 전달자를 업데이트합니다.	쓰기	directory* (p. 943)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateNumberOfDomainControllers	디렉터리에서 도메인 컨트롤러를 추가 또는 제거합니다. 현재 값과 (이 API 호출을 통해 제공된) 새 값 간의 차이에 따라 도메인 컨트롤러가 추가 또는 제거됩니다. 요청된 도메인 컨트롤러 수가 업데이트되면 새 도메인 컨트롤러가 완전히 활성 상태가 될 때까지 최대 45분이 걸릴 수 있습니다. 이 동안 다른 업데이트 요청을 할 수 없습니다.	쓰기	directory* (p. 943)		
UpdateRadius	AD Connector 디렉터리에 대한 RADIUS(Remote Authentication Dial In User Service) 서버 정보를 업데이트합니다.	쓰기	directory* (p. 943)		
UpdateTrust	AWS 관리형 Microsoft AD 디렉터리와 온프레미스 Active Directory 간에 설정된 신뢰 관계를 업데이트합니다.	쓰기	directory* (p. 943)		
VerifyTrust	AWS 클라우드의 Microsoft AD와 외부 도메인 간의 신뢰 관계를 확인합니다.	Read	directory* (p. 943)		

AWS Directory Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 937)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey} (p. 944)

AWS Directory Service의 조건 키

AWS Directory Service는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}		문자열

조건 키	설명	유형
aws:ResourceTag/${TagKey}		문자열
aws:TagKeys		문자열

Amazon DynamoDB에 사용되는 작업, 리소스 및 조건 키

Amazon DynamoDB(서비스 접두사: `dynamodb`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon DynamoDB에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchGetItem	하나 이상의 테이블에서 하나 이상의 항목 속성을 반환합니다.	Read	table* (p. 950)		
				dynamodb:Attributes (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				dynamodb:Select (p. 951)	
BatchWriteItem	하나 이상의 테이블에 여러 항목을 추가하거나 삭제합니다.	쓰기	table* (p. 950)		
				dynamodb:Attributes (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951)	
ConditionCheckItem	ConditionCheckItem 작업은 지정된 기본 키를 갖는 항목에 대한 속성 집합이 존재하는지 확인합니다.	Read	table* (p. 950)		
				dynamodb:Attributes (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951) dynamodb:ReturnValues (p. 951)	
CreateBackup	기존 테이블에 대해 백업을 생성합니다.	쓰기	table* (p. 950)		
CreateGlobalTable	사용자가 기존 테이블에서 전역 테이블을 생성할 수 있습니다.	쓰기	global-table* (p. 950)		
			table* (p. 950)		
CreateTable	CreateTable 작업은 사용자 계정에 새 테이블을 추가합니다.	쓰기	table* (p. 950)		
CreateTableReplica	새 복제본 테이블을 추가합니다.	쓰기	table* (p. 950)		
DeleteBackup	테이블의 기존 백업을 삭제합니다.	쓰기	backup* (p. 950)		
DeleteItem	기본 키로 테이블의 단일 항목을 삭제합니다	쓰기	table* (p. 950)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				dynamodb:Attributes (p. 951) dynamodb:EnclosingOperation (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951) dynamodb:ReturnValues (p. 951)	
DeleteTable	DeleteTable 작업은 테이블과 테이블에 속한 모든 항목을 삭제합니다.	쓰기	table* (p. 950)		
DeleteTableReplica	복제본 테이블과 해당 항목을 모두 삭제합니다.	쓰기	table* (p. 950)		
DescribeBackup	테이블의 기존 백업을 설명합니다.	Read	backup* (p. 950)		
DescribeContinuousBackups	지정된 테이블에서 백업 복원 설정의 상태를 점검합니다.	Read	table* (p. 950)		
DescribeContributorInsights	주어진 테이블 또는 전역 보조 인덱스에 대한 Contributor Insights 상태 및 관련 세부 정보를 설명합니다.	Read	table* (p. 950)		
			index (p. 950)		
DescribeGlobalTable	지정된 전역 테이블에 대한 정보를 반환합니다.	Read	global-table* (p. 950)		
DescribeGlobalTableSettings	지정된 전역 테이블에 대한 설정 정보를 반환합니다.	Read	global-table* (p. 950)		
DescribeLimits	한 리전의 AWS 계정에 대해 현재 프로비저닝된 용량 제한을 반환하는데, 리전 전체를 기준으로도 반환하고, 만들려는 하나의 DynamoDB 테이블을 기준으로도 반환합니다.	Read			
DescribeReservedCapacity	구입한 Reserved Capacity를 하나 이상 설명합니다.	Read			
DescribeReservedCapacityOfferings	구매 가능한 예약 용량 상품을 설명합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeStream	스트림의 현재 상태, Amazon 리소스 이름(ARN), 샤드의 구성 및 해당되는 DynamoDB 테이블을 포함하여 스트림에 대한 정보를 반환합니다.	Read	stream* (p. 950)		
DescribeTable	테이블에 대한 정보를 반환합니다.	Read	table* (p. 950)		
DescribeTableReplicaAutoScaling	전역 테이블의 모든 복제본에서 Auto Scaling 설정을 설명합니다.	Read	table* (p. 950)		
DescribeTimeToLive	지정된 테이블의 Time to Live(TTL) 상태에 대한 설명을 제공합니다.	Read	table* (p. 950)		
GetItem	GetItem 작업은 주어진 기본 키와 함께 항목에 대한 속성 집합을 반환합니다.	Read	table* (p. 950)		
				dynamodb:Attributes (p. 951) dynamodb:EnclosingOperation (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951) dynamodb:Select (p. 951)	
GetRecords	지정된 샤드에서 스트림 레코드를 반환합니다.	Read	stream* (p. 950)		
GetShardIterator	샤드 반복자를 반환합니다.	Read	stream* (p. 950)		
ListBackups	계정 및 엔드포인트와 연결된 백업을 나열합니다.	List			
ListContributorInsights	현재 계정 및 엔드포인트와 연결된 모든 테이블 및 전역 보조 인덱스에 대한 ContributorInsightsSummary를 나열합니다.	List			
ListGlobalTables	지정된 리전에 복제본을 보유한 모든 전역 테이블을 나열합니다.	List			
ListStreams	현재 계정 및 엔드포인트와 연동되어 있는 스트림 ARN의 배열을 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTables	현재 계정 및 엔드포인트와 연동되어 있는 테이블 이름의 배열을 반환합니다.	List			
ListTagsOfResource	Amazon DynamoDB 리소스의 모든 태그를 나열합니다.	Read	table* (p. 950)		
PurchaseReservedCapacityOfferings	계정에서 사용할 예약 용량을 구입합니다.	쓰기			
PutItem	새 항목을 만들거나 이전 항목을 새 항목으로 바꿉니다.	쓰기	table* (p. 950)		
				dynamodb:Attributes (p. 951) dynamodb:EnclosingOperation (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951) dynamodb:ReturnValues (p. 951)	
Query	테이블 또는 보조 인덱스의 기본 키를 사용하여 해당 테이블 또는 인덱스에서 직접 액세스합니다.	Read	table* (p. 950)		
			index (p. 950)		
				dynamodb:Attributes (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951) dynamodb:ReturnValues (p. 951) dynamodb:Select (p. 951)	
RestoreTableFromBackup	기존 백업에서 새 테이블을 생성합니다.	쓰기	backup* (p. 950)		
			table* (p. 950)		
RestoreTableToPointInTime	테이블을 특정 시점으로 복원합니다.	쓰기	table* (p. 950)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Scan	테이블 또는 보조 인덱스의 모든 항목에 액세스하여 하나 이상의 항목 및 항목 속성을 반환합니다.	Read	table* (p. 950)		
			index (p. 950)		
				dynamodb:Attributes (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951) dynamodb:ReturnValues (p. 951) dynamodb:Select (p. 951)	
TagResource	태그 세트를 Amazon DynamoDB 리소스와 연결합니다.	태그 지정	table* (p. 950)		
UntagResource	Amazon DynamoDB 리소스에서 태그의 연결을 제거합니다.	태그 지정	table* (p. 950)		
UpdateContinuousBackups	연속 백업을 활성화하거나 비활성화합니다.	쓰기	table* (p. 950)		
UpdateContributorInsights	특정 테이블 또는 전역 보조 인덱스에 대한 Contributor Insights 상태를 업데이트합니다.	쓰기	table* (p. 950)		
			index (p. 950)		
UpdateGlobalTable	사용자가 지정된 전역 테이블에서 복제본을 추가하거나 제거할 수 있습니다.	쓰기	global-table* (p. 950)		
			table* (p. 950)		
UpdateGlobalTableSettings	사용자가 지정된 전역 테이블의 설정을 업데이트할 수 있습니다.	쓰기	global-table* (p. 950)		
			table* (p. 950)		
UpdateItem	기존 항목의 속성을 편집합니다. 항목이 아직 없다면 테이블에 새 항목을 추가합니다.	쓰기	table* (p. 950)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				dynamodb:Attributes (p. 951) dynamodb:EnclosingOperation (p. 951) dynamodb:LeadingKeys (p. 951) dynamodb:ReturnConsumedCapacity (p. 951) dynamodb:ReturnValues (p. 951)	
UpdateTable	주어진 테이블에 대한 프로비저닝된 처리량 설정, 전역 보조 인덱스 또는 DynamoDB Streams 설정을 수정합니다.	쓰기	table* (p. 950)		
UpdateTableReplicaAutoScaling	복제본 테이블의 Auto Scaling 설정을 업데이트합니다.	쓰기	table* (p. 950)		
UpdateTimeToLive	지정된 테이블에 대한 TTL을 활성화하거나 비활성화합니다.	쓰기	table* (p. 950)		

Amazon DynamoDB에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 944)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
index	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/index/${IndexName}`	
stream	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/stream/${StreamLabel}`	
table	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}`	
backup	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/backup/${BackupName}`	
global-table	`arn:${Partition}:dynamodb::${Account}:global-table/${GlobalTableName}`	

Amazon DynamoDB에 사용되는 조건 키

Amazon DynamoDB는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

> **Note**
>
> IAM 정책을 사용하여 DynamoDB 액세스를 미세 조정하기 하기 위해 컨텍스트 키를 사용하는 방법에 대한 자세한 내용은 Amazon DynamoDB 개발자 안내서의 IAM 정책 조건을 사용하여 세부적인 액세스 제어 구현을 참조하십시오.

조건 키	설명	유형
dynamodb:Attributes	테이블의 속성(필드 또는 열) 이름을 기준으로 필터링합니다.	문자열
dynamodb:EnclosingOperation	트랜잭션 API 호출을 차단하고 비 트랜잭션 API 호출을 허용하는 데 또는 그 반대의 경우를 위해 사용됩니다.	문자열
dynamodb:LeadingKeys	테이블의 파티션 키를 기준으로 필터링합니다.	문자열
dynamodb:ReturnConsumedCapacity	요청의 ReturnConsumedCapacity 파라미터를 기준으로 필터링합니다. "TOTAL" 또는 "NONE"을 포함합니다.	문자열
dynamodb:ReturnValues	요청의 ReturnValues 파라미터를 기준으로 필터링합니다. 다음 중 하나를 포함합니다: "ALL_OLD", "UPDATED_OLD","ALL_NEW","UPDATED_NEW" 또는 "NONE".	문자열
dynamodb:Select	쿼리 또는 스캔 요청의 Select 파라미터를 기준으로 필터링합니다.	문자열

Amazon DynamoDB Accelerator(DAX)에 사용되는 작업, 리소스 및 조건 키

Amazon DynamoDB Accelerator(DAX)(서비스 접두사: `dax`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon DynamoDB Accelerator(DAX)에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchGetItem	BatchGetItem 작업은 하나 이상의 테이블에서 하나 이상의 항목 속성을 반환합니다.	Read	application* (p. 955)		
BatchWriteItem	BatchWriteItem 작업은 하나 이상의 테이블에서 다중 항목을 적용 또는 삭제합니다.	쓰기	application* (p. 955)		
ConditionCheckItem	ConditionCheckItem 작업은 지정된 기본 키를 갖는 항목에 대한 속성 집합이 존재하는지 확인합니다.	Read	application* (p. 955)		
CreateCluster	CreateCluster 작업은 DAX 클러스터를 생성합니다.	쓰기	application* (p. 955)		dax:CreateParameterGrou dax:CreateSubnetGroup ec2:CreateNetworkInterfa ec2:DeleteNetworkInterfa ec2:DescribeNetworkInter ec2:DescribeSecurityGrou ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole iam:PassRole
CreateParameterGroup	CreateParameterGroup 작업은 DAX 클러스터의 모든 노드에 적용하는 파라미터의 모음을 생성합니다.	쓰기			
CreateSubnetGroup	CreateSubnetGroup 작업은 새 서브넷 그룹을 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DecreaseReplicationFactor	DecreaseReplicationFactor 작업은 DAX 클러스터에서 하나 이상의 노드를 제거합니다.	쓰기	application* (p. 955)		
DeleteCluster	DeleteCluster 작업은 이전에 프로비저닝된 DAX 클러스터를 삭제합니다.	쓰기	application* (p. 955)		
DeleteItem	DeleteItem 작업은 기본 키로 테이블의 단일 항목을 삭제합니다.	쓰기	application* (p. 955)		
				dax:EnclosingOperation (p. 955)	
DeleteParameterGroup	DeleteParameterGroup 작업은 지정된 파라미터 그룹을 삭제합니다.	쓰기			
DeleteSubnetGroup	DeleteSubnetGroup 작업은 서브넷 그룹을 삭제합니다.	쓰기			
DescribeClusters	DescribeClusters 작업은 프로비저닝된 모든 DAX 클러스터에 대한 정보를 반환합니다.	List	application (p. 955)		
DescribeDefaultParameters	DescribeDefaultParameters 작업은 DAX에 대한 기본 시스템 파라미터 정보를 반환합니다.	List			
DescribeEvents	DescribeEvents 작업은 DAX 클러스터 및 파라미터 그룹과 관련된 이벤트를 반환합니다.	List			
DescribeParameterGroups	DescribeParameterGroups 작업은 파라미터 그룹 설명의 목록을 반환합니다.	List			
DescribeParameters	DescribeParameters 작업은 특정 파라미터 그룹에 대한 세부 파라미터 목록을 반환합니다.	Read			
DescribeSubnetGroups	DescribeSubnetGroups 작업은 서브넷 그룹 설명의 목록을 반환합니다.	List			
GetItem	GetItem 작업은 지정된 기본 키와 함께 항목에 대한 속성 세트를 반환합니다.	Read	application* (p. 955)		
				dax:EnclosingOperation (p. 955)	
IncreaseReplicationFactor	IncreaseReplicationFactor 작업은 하나 이상의 노드를 DAX 클러스터에 추가합니다.	쓰기	application* (p. 955)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTags	ListTags 작업은 DAX 클러스터에 대한 모든 태그 목록을 반환합니다.	Read	application* (p. 955)		
PutItem	PutItem 작업은 새 항목을 생성하거나 이전 항목을 새 항목으로 바꿉니다.	쓰기	application* (p. 955)		
				dax:EnclosingOperation (p. 955)	
Query	Query 작업은 기본 키 값을 기반으로 항목을 찾습니다. 복합 기본 키(파티션 키 및 정렬 키)가 있는 테이블 또는 보조 인덱스를 쿼리할 수 있습니다.	Read	application* (p. 955)		
RebootNode	RebootNode 작업은 DAX 클러스터의 단일 노드를 재부팅합니다.	쓰기	application* (p. 955)		
Scan	Scan 작업은 테이블 또는 보조 인덱스의 모든 항목에 액세스하여 하나 이상의 항목 및 항목 속성을 반환합니다.	Read	application* (p. 955)		
TagResource	TagResource 작업은 태그 세트를 DAX 리소스와 연결합니다.	태그 지정	application* (p. 955)		
UntagResource	UntagResource 작업은 DAX 리소스에서 태그 연결을 제거합니다.	태그 지정	application* (p. 955)		
UpdateCluster	UpdateCluster 작업은 DAX 클러스터에 대한 설정을 수정합니다.	쓰기	application* (p. 955)		
UpdateItem	UpdateItem 작업은 기존 항목의 속성을 편집하거나 항목이 아직 없는 경우 새 항목을 테이블에 추가합니다.	쓰기	application* (p. 955)		
				dax:EnclosingOperation (p. 955)	
UpdateParameterGroup	UpdateParameterGroup 작업은 파라미터 그룹의 파라미터를 수정합니다.	쓰기			
UpdateSubnetGroup	UpdateSubnetGroup 작업은 기존 서브넷 그룹을 수정합니다.	쓰기			

Amazon DynamoDB Accelerator(DAX)에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 952)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
application	`arn:${Partition}:dax:${Region}:${Account}:cache/${ClusterName}`	

Amazon DynamoDB Accelerator(DAX)의 조건 키

Amazon DynamoDB Accelerator(DAX)는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
dax:EnclosingOperation	트랜잭션 API 호출을 차단하고 비 트랜잭션 API 호출을 허용하는 데 또는 그 반대의 경우를 위해 사용됩니다.	문자열

Amazon EC2에 사용되는 작업, 리소스 및 조건 키

Amazon EC2(서비스 접두사: `ec2`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon EC2에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptReservedInstancesExchangeQuote	컨버터블 예약 인스턴스 교환 견적서를 수락할 수 있는 권한을 부여합니다.	쓰기			
AcceptTransitGatewayPeeringAttachment	전송 게이트웨이 피어링 연결 요청을 수락할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
AcceptTransitGatewayVpcAttachment	VPC를 전송 게이트웨이에 연결하라는 요청을 수락할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
AcceptVpcEndpointConnections	VPC 엔드포인트 서비스에 대한 하나 이상의 인터페이스 VPC 엔드포인트 연결을 수락할 수 있는 권한을 부여합니다.	쓰기	vpc-endpoint-service* (p. 1053)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
AcceptVpcPeeringConnection	VPC 피어링 연결 요청을 수락할 수 있는 권한을 부여합니다.	쓰기	vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	
			vpc-peering-connection* (p. 1053)	ec2:AccepterVpc (p. 1055) ec2:Region (p. 1057) ec2:RequesterVpc (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
AdvertiseByoipCidr	고유 IP 주소 가져오기(BYOIP)를 통해 AWS에서 사용하도록 프로비저닝되는 IP 주소 범위를 공급할 수 있는 권한을 부여합니다.	쓰기			
AllocateAddress	탄력적 IP 주소(EIP)를 계정에 할당할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AllocateHosts	계정에 전용 호스트를 할당할 수 있는 권한을 부여합니다.	쓰기	dedicated-host* (p. 1043)		
ApplySecurityGroupsToClientVpnTargetNetwork	Client VPN 엔드포인트와 대상 네트워크 간 연결에 보안 그룹을 적용할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
AssignIpv6Addresses	네트워크 인터페이스에 하나 이상의 IPv6 주소를 할당할 수 있는 권한을 부여합니다.	쓰기			
AssignPrivateIpAddresses	네트워크 인터페이스에 하나 이상의 보조 프라이빗 IP 주소를 할당할 수 있는 권한을 부여합니다.	쓰기			
AssociateAddress	인스턴스 또는 네트워크 인터페이스에 탄력적 IP 주소(EIP)를 연결할 수 있는 권한을 부여합니다.	쓰기			
AssociateClientVpnTargetNetwork	대상 네트워크를 Client VPN 엔드포인트와 연결할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			subnet* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
AssociateDhcpOptions	DHCP 옵션 세트를 VPC와 연결하거나 연결 해제할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateIamInstanceProfile	IAM 인스턴스 프로파일을 실행 중이거나 중지된 인스턴스와 연결할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	iam:PassRole
AssociateRouteTable	서브넷 또는 게이트웨이를 라우팅 테이블과 연결할 수 있는 권한을 부여합니다.	쓰기			
AssociateSubnetCidrBlock	CIDR 블록을 서브넷과 연결할 수 있는 권한을 부여합니다.	쓰기			
AssociateTransitGatewayMulticastDomain	연결 및 서브넷 목록을 전송 게이트웨이 멀티캐스트 도메인과 연결할 수 있는 권한을 부여합니다.	쓰기	subnet* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateTransitGatewayRouteTable	연결을 전송 게이트웨이 라우팅 테이블과 연결할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-route-table* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
AssociateVpcCidrBlock	CIDR 블록을 VPC와 연결할 수 있는 권한을 부여합니다.	쓰기			
AttachClassicLinkVpc	하나 이상의 VPC 보안 그룹을 통해 EC2-Classic 인스턴스를 ClassicLink가 활성화된 VPC에 연결할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
			security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	
AttachInternetGateway	VPC에 인터넷 게이트웨이를 연결할 수 있는 권한을 부여합니다.	쓰기			
AttachNetworkInterface	인스턴스에 네트워크 인터페이스를 연결할 수 있는 권한을 부여합니다.	쓰기			
AttachVolume	EBS 볼륨을 실행 중이거나 중지된 인스턴스에 연결하고 지정된 디바이스 이름이 있는 인스턴스에 공개할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			volume* (p. 1052)	ec2:AvailabilityZone (p. 1055) ec2:Encrypted (p. 1056) ec2:ParentSnapshot (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)	
AttachVpnGateway	VPC에 가상 프라이빗 게이트웨이를 연결할 수 있는 권한을 부여합니다.	쓰기			
AuthorizeClientVpnIngress	Client VPN 엔드포인트에 인바운드 권한 부여 규칙을 추가할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
AuthorizeSecurityGroupEgress	VPC 보안 그룹에 하나 이상의 아웃바운드 규칙을 추가할 수 있는 권한을 부여합니다.	쓰기	security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
AuthorizeSecurityGroupIngress	보안 그룹에 하나 이상의 인바운드 규칙을 추가할 수 있는 권한을 부여합니다.	쓰기	security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BundleInstance	인스턴스 스토어 지원 Windows 인스턴스를 번들링할 수 있는 권한을 부여합니다.	쓰기			
CancelBundleTask	번들링 작업을 취소할 수 있는 권한을 부여합니다.	쓰기			
CancelCapacityReservation	용량 예약을 취소하고 예약된 용량을 해제할 수 있는 권한을 부여합니다.	쓰기	capacity-reservation* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
CancelConversionTask	활성 변환 작업을 취소할 수 있는 권한을 부여합니다.	쓰기			
CancelExportTask	활성 내보내기 작업을 취소할 수 있는 권한을 부여합니다.	쓰기			
CancelImportTask	진행 중인 가상 머신 가져오기 또는 스냅샷 가져오기 작업을 취소할 수 있는 권한을 부여합니다.	쓰기			
CancelReservedInstancesListing	예약 인스턴스 마켓플레이스에서 예약 인스턴스 목록을 취소할 수 있는 권한을 부여합니다.	쓰기			
CancelSpotFleetRequests	하나 이상의 스팟 플릿 요청을 취소할 수 있는 권한을 부여합니다.	쓰기			
CancelSpotInstanceRequests	하나 이상의 스팟 인스턴스 요청을 취소할 수 있는 권한을 부여합니다.	쓰기			
ConfirmProductInstance	소유한 제품 코드가 인스턴스와 연결되어 있는지 여부를 확인할 수 있는 권한을 부여합니다.	쓰기			
CopyFpgaImage	소스 Amazon FPGA 이미지(AFI)를 현재 리전에 복사할 수 있는 권한을 부여합니다.	쓰기			
CopyImage	소스 리전에서 현재 리전으로 Amazon Machine Image(AMI)를 복사할 수 있는 권한을 부여합니다.	쓰기			
CopySnapshot	EBS 볼륨의 특정 시점 스냅샷을 복사하여 Amazon S3에 저장할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1049)	aws:TagKeys (p. 1055) aws:RequestTag/${TagKey} (p. 1055) ec2:Region (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCapacityReservation	용량 예약을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateClientVpnEndpoint	Client VPN 엔드포인트를 생성할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
CreateClientVpnRoute	Client VPN 엔드포인트의 라우팅 테이블에 네트워크 라우팅을 추가할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			subnet* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
CreateCustomerGateway	고객 게이트웨이 디바이스에 대한 정보를 AWS에 제공하는 고객 게이트웨이를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateDefaultSubnet	기본 VPC의 지정된 가용 영역에 기본 서브넷을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateDefaultVpc	각 가용 영역에 기본 VPC 및 기본 서브넷을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateDhcpOptions	VPC에 대한 DHCP 옵션 세트를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateEgressOnlyInternetGateway	VPC에 대한 외부 전용 인터넷 게이트웨이를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateFleet	EC2 플릿을 시작할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateFlowLogs	네트워크 인터페이스의 IP 트래픽을 캡처하는 흐름 로그를 하나 이상 생성할 수 있는 권한을 부여합니다.	쓰기	vpc-flow-log* (p. 1053)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	iam:PassRole
			network-interface (p. 1048)	ec2:Region (p. 1057) ec2:Subnet (p. 1058) ec2:Vpc (p. 1058)	
			subnet (p. 1050)	ec2:Region (p. 1057) ec2:Vpc (p. 1058)	
			vpc (p. 1052)	ec2:Region (p. 1057)	
CreateFpgaImage	설계 체크포인트(DCP)에서 Amazon FPGA 이미지(AFI)를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateImage	중지되거나 실행 중인 Amazon EBS 지원 인스턴스에서 Amazon EBS 지원 AMI를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateInstanceExportTask	Amazon S3 버킷으로 내보낼 수 있는 권한을 부여합니다.	쓰기			
CreateInternetGateway	VPC에 대한 인터넷 게이트웨이를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateKeyPair	2048비트 RSA 키 페어를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateLaunchTemplate	시작 템플릿을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateLaunchTemplateVersion	시작 템플릿의 새 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	launch-template* (p. 1046)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateLocalGatewayRoute	로컬 게이트웨이 라우팅 테이블에 고정 라우팅을 생성할 수 있는 권한을 부여합니다.	쓰기	local-gateway-route-table* (p. 1046)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			local-gateway-virtual-interface-group* (p. 1047)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
CreateLocalGatewayRouteTableVpcAssociation	VPC를 로컬 게이트웨이 라우팅 테이블과 연결할 수 있는 권한을 부여합니다.	쓰기	local-gateway-route-table* (p. 1046)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	
CreateNatGateway	서브넷에 NAT 게이트웨이를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateNetworkAcl	VPC에서 네트워크 ACL을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateNetworkAclEntry	네트워크 ACL에 번호가 지정된 항목(규칙)을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateNetworkInterface	서브넷에 네트워크 인터페이스를 생성할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateNetworkInterfacePermission	AWS 인증 사용자가 네트워크 인터페이스에 대한 특정 작업을 수행할 권한을 생성할 수 있는 권한을 부여합니다.	권한 관리	network-interface* (p. 1048)	ec2:AuthorizedUser (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Permission (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Subnet (p. 1058) ec2:Vpc (p. 1058) ec2:AuthorizedService (p. 1055)	
CreatePlacementGroup	배치 그룹을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateReservedInstancesListing	예약 인스턴스 마켓플레이스에서 판매할 표준 예약 인스턴스의 목록을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateRoute	VPC 라우팅 테이블에 라우팅을 생성할 수 있는 권한을 부여합니다.	쓰기	route-table* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
CreateRouteTable	VPC에 대한 라우팅 테이블을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateSecurityGroup	보안 그룹을 생성할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateSnapshot	EBS 볼륨의 스냅샷을 생성하여 Amazon S3에 저장할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1049)	aws:TagKeys (p. 1055) aws:RequestTag/${TagKey} (p. 1055) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057)	
			volume* (p. 1052)	ec2:Encrypted (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateSnapshots	여러 EBS 볼륨에 대한 장애 발생 시 일관성이 유지되는 스냅샷을 생성하여 Amazon S3에 저장할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
			snapshot* (p. 1049)	aws:TagKeys (p. 1055) aws:RequestTag/${TagKey} (p. 1055) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			volume* (p. 1052)	ec2:Encrypted (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)	
CreateSpotDatafeedSubscription	스팟 인스턴스 사용 로그를 볼 수 있도록 스팟 인스턴스에 대한 데이터 피드를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateSubnet	VPC에 서브넷을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateTags	Amazon EC2 리소스에 대해 하나 이상의 태그를 추가하거나 덮어쓸 수 있는 권한을 부여합니다.	태그 지정	capacity-reservation (p. 1043)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			client-vpn-endpoint (p. 1043)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			dedicated-host (p. 1043)		
			dhcp-options (p. 1044)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			fpga-image (p. 1044)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Owner (p. 1056) ec2:Public (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			image (p. 1045)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:ImageType (p. 1056) ec2:Owner (p. 1056) ec2:Public (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			instance (p. 1045)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
			internet-gateway (p. 1046)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			local-gateway (p. 1046)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			local-gateway-route-table (p. 1046)		
			local-gateway-route-table-virtual-interface-group-association (p. 1046)		
			local-gateway-route-table-vpc-association (p. 1047)		
			local-gateway-virtual-interface (p. 1047)		
			local-gateway-virtual-interface-group (p. 1047)		
			network-acl (p. 1047)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			network-interface (p. 1048)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Subnet (p. 1058) ec2:Vpc (p. 1058) ec2:AssociatePublicIpAddress (p. 1055)	
			reserved-instances (p. 1048)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:InstanceType (p. 1056) ec2:Region (p. 1057) ec2:ReservedInstancesOfferingType (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			route-table (p. 1049)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
			security-group (p. 1049)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			snapshot (p. 1049)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Owner (p. 1056) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:SnapshotTime (p. 1058) ec2:VolumeSize (p. 1058)	
			spot-instance-request (p. 1049)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			subnet (p. 1050)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
			traffic-mirror-filter (p. 1050)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			traffic-mirror-session (p. 1050)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			traffic-mirror-target (p. 1050)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-attachment (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			transit-gateway-route-table (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			volume (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Encrypted (p. 1056) ec2:ParentSnapshot (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			vpc (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	
			vpc-endpoint (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpc-endpoint-service (p. 1053)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpc-flow-log (p. 1053)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			vpn-connection (p. 1054)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpn-gateway (p. 1055)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
				ec2:CreateAction (p. 1055)	
CreateTrafficMirrorFilter	트래픽 미러 필터를 생성할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-filter* (p. 1050)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
CreateTrafficMirrorFilterRule	트래픽 미러 필터 규칙을 생성할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-filter* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			traffic-mirror-filter-rule* (p. 1050)	ec2:Region (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateTrafficMirrorSession	트래픽 미러 세션을 생성할 수 있는 권한을 부여합니다.	쓰기	network-interface* (p. 1048)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			traffic-mirror-filter* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			traffic-mirror-session* (p. 1050)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
			traffic-mirror-target* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
CreateTrafficMirrorTarget	트래픽 미러 대상을 생성할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-target* (p. 1050)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
			network-interface (p. 1048)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateTransitGateway	전송 게이트웨이를 생성할 수 있는 권한을 부여합니다.	쓰기	transit-gateway* (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
CreateTransitGatewayMulticastDomain	전송 게이트웨이에 대한 멀티캐스트 도메인을 생성할 수 있는 권한을 부여합니다.	쓰기	transit-gateway* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain* (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
CreateTransitGatewayPeeringAttachment	요청자와 수락자 전송 게이트웨이 간에 전송 게이트웨이 피어링 연결을 요청할 수 있는 권한을 부여합니다.	쓰기	transit-gateway* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-attachment* (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
CreateTransitGatewayRoute	전송 게이트웨이 라우팅 테이블에 고정 라우팅을 생성할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-route-table* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			transit-gateway-attachment (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
CreateTransitGatewayRouteTable	전송 게이트웨이에 대한 라우팅 테이블을 생성할 수 있는 권한을 부여합니다.	쓰기	transit-gateway* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-route-table* (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
CreateTransitGatewayVpcAttachment	VPC를 전송 게이트웨이에 연결할 수 있는 권한을 부여합니다.	쓰기	transit-gateway* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-attachment* (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057)	
			vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			subnet (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateVolume	EBS 볼륨을 생성할 수 있는 권한을 부여합니다.	쓰기	volume* (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Encrypted (p. 1056) ec2:ParentSnapshot (p. 1056) ec2:Region (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)	
CreateVpc	지정된 CIDR 블록으로 VPC를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateVpcEndpoint	AWS 서비스용 VPC 엔드포인트를 생성할 수 있는 권한을 부여합니다.	쓰기	vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	route53:AssociateVPCWit
			vpc-endpoint* (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:VpceServiceName (p. 1058) ec2:VpceServiceOwner (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			route-table (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			security-group (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			subnet (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
CreateVpcEndpointConnectionNotification	VPC 엔드포인트 또는 VPC 엔드포인트 서비스에 대한 연결 알림을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateVpcEndpointServiceConfiguration	서비스 소비자(AWS 계정, IAM 사용자 및 IAM 역할)가 연결할 수 있는 VPC 엔드포인트 서비스 구성을 생성할 수 있는 권한을 부여합니다.	쓰기	vpc-endpoint-service* (p. 1053)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:VpceServicePrivateDnsName (p. 1058)	
CreateVpcPeeringConnection	두 VPC 간의 VPC 피어링 연결을 요청할 수 있는 권한을 부여합니다.	쓰기	vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			vpc-peering-connection* (p. 1053)	ec2:AccepterVpc (p. 1055) ec2:Region (p. 1057) ec2:RequesterVpc (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateVpnConnection	가상 프라이빗 게이트웨이 또는 전송 게이트웨이와 고객 게이트웨이 간에 VPN 연결을 생성할 수 있는 권한을 부여합니다.	쓰기	vpn-connection* (p. 1054)	ec2:Region (p. 1057) ec2:AuthenticationType (p. 1055) ec2:DPDTimeoutSeconds (p. 1055) ec2:GatewayType (p. 1056) ec2:IKEVersions (p. 1056) ec2:InsideTunnelCidr (p. 1056) ec2:Phase1DHGroupNumbers (p. 1056) ec2:Phase2DHGroupNumbers (p. 1057) ec2:Phase1EncryptionAlgorithms (p. 1056) ec2:Phase2EncryptionAlgorithms (p. 1057) ec2:Phase1IntegrityAlgorithms (p. 1057) ec2:Phase2IntegrityAlgorithms (p. 1057) ec2:Phase1LifetimeSeconds (p. 1057) ec2:Phase2LifetimeSeconds (p. 1057) ec2:PresharedKeys (p. 1057) ec2:RekeyFuzzPercentage (p. 1057) ec2:RekeyMarginTimeSeconds (p. 1057) ec2:RoutingType (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateVpnConnectionRoute	가상 프라이빗 게이트웨이와 고객 게이트웨이 간의 VPN 연결에 대한 고정 라우팅을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateVpnGateway	가상 프라이빗 게이트웨이를 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteClientVpnEndpoint	Client VPN 엔드포인트를 삭제할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteClientVpnRoute	Client VPN 엔드포인트에서 라우팅을 삭제할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			subnet (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteCustomerGateway	고객 게이트웨이를 삭제할 수 있는 권한을 부여합니다.	쓰기	customer-gateway* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteDhcpOptions	DHCP 옵션 세트를 삭제할 수 있는 권한을 부여합니다.	쓰기	dhcp-options* (p. 1044)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteEgressOnlyInternetGateway	외부 전용 인터넷 게이트웨이를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteFleets	하나 이상의 EC2 플릿을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteFlowLogs	하나 이상의 흐름 로그를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteFpgaImage	Amazon FPGA 이미지(AFI)를 삭제할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteInternetGateway	인터넷 게이트웨이를 삭제할 수 있는 권한을 부여합니다.	쓰기	internet-gateway* (p. 1046)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteKeyPair	Amazon EC2에서 퍼블릭 키를 제거하여 키 페어를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteLaunchTemplate	시작 템플릿 및 관련 버전을 삭제할 수 있는 권한을 부여합니다.	쓰기	launch-template* (p. 1046)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteLaunchTemplateVersions	시작 템플릿의 버전을 하나 이상 삭제할 수 있는 권한을 부여합니다.	쓰기	launch-template* (p. 1046)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteLocalGatewayRoute	로컬 게이트웨이 라우팅 테이블에서 라우팅을 삭제할 수 있는 권한을 부여합니다.	쓰기	local-gateway-route-table* (p. 1046)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteLocalGatewayRouteTableVpcAssociation	VPC와 로컬 게이트웨이 라우팅 테이블 간의 연결을 삭제할 수 있는 권한을 부여합니다.	쓰기	local-gateway-route-table-vpc-association* (p. 1047)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteNatGateway	NAT 게이트웨이를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteNetworkAcl	네트워크 ACL을 삭제할 수 있는 권한을 부여합니다.	쓰기	network-acl* (p. 1047)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteNetworkAclEntry	네트워크 ACL에서 인바운드 또는 아웃바운드 항목(규칙)을 삭제할 수 있는 권한을 부여합니다.	쓰기	network-acl* (p. 1047)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
DeleteNetworkInterface	분리된 네트워크 인터페이스를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteNetworkInterfacePermission	네트워크 인터페이스와 연결된 권한을 삭제할 수 있는 권한을 부여합니다.	권한 관리			
DeletePlacementGroup	배치 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteRoute	라우팅 테이블에서 라우팅을 삭제할 수 있는 권한을 부여합니다.	쓰기	route-table* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
DeleteRouteTable	라우팅 테이블을 삭제할 수 있는 권한을 부여합니다.	쓰기	route-table* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
DeleteSecurityGroup	보안 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteSnapshot	EBS 볼륨의 스냅샷을 삭제할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1049)	ec2:Owner (p. 1056) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:SnapshotTime (p. 1058) ec2:VolumeSize (p. 1058)	
DeleteSpotDatafeedSubscription	스팟 인스턴스에 대한 데이터 피드를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteSubnet	서브넷을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteTags	Amazon EC2 리소스에서 하나 이상의 태그를 삭제할 수 있는 권한을 부여합니다.	태그 지정	capacity-reservation (p. 1043)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			client-vpn-endpoint (p. 1043)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			dedicated-host (p. 1043)		
			dhcp-options (p. 1044)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			fpga-image (p. 1044)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			image (p. 1045)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			instance (p. 1045)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			internet-gateway (p. 1046)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			local-gateway (p. 1046)		
			local-gateway-route-table (p. 1046)		
			local-gateway-route-table-virtual-interface-group-association (p. 1046)		
			local-gateway-route-table-vpc-association (p. 1047)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			local-gateway-virtual-interface (p. 1047)		
			local-gateway-virtual-interface-group (p. 1047)		
			network-acl (p. 1047)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			network-interface (p. 1048)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			reserved-instances (p. 1048)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			route-table (p. 1049)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			security-group (p. 1049)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			snapshot (p. 1049)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			spot-instance-request (p. 1049)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			subnet (p. 1050)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-attachment (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			transit-gateway-route-table (p. 1051)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			volume (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpc (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpc-endpoint (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			vpc-endpoint-service (p. 1053)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpc-flow-log (p. 1053)		
			vpn-connection (p. 1054)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			vpn-gateway (p. 1055)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteTrafficMirrorFilter	트래픽 미러 필터를 삭제할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-filter* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteTrafficMirrorFilterRule	트래픽 미러 필터 규칙을 삭제할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-filter* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			traffic-mirror-filter-rule* (p. 1050)	ec2:Region (p. 1057)	
DeleteTrafficMirrorSession	트래픽 미러 세션을 삭제할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-session* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteTrafficMirrorTarget	트래픽 미러 대상을 삭제할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-target* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteTransitGateway	전송 게이트웨이를 삭제할 수 있는 권한을 부여합니다.	쓰기	transit-gateway* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteTransitGatewayMulticastDomain	전송 게이트웨이 멀티캐스트 도메인을 삭제할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-multicast-domain* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteTransitGatewayPeeringAttachment	전송 게이트웨이에서 피어링 연결을 삭제할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteTransitGatewayRoute	전송 게이트웨이 라우팅 테이블에서 라우팅을 삭제할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-route-table* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteTransitGatewayRouteTable	전송 게이트웨이 라우팅 테이블을 삭제할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-route-table* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteTransitGatewayVpcAttachment	전송 게이트웨이에서 VPC 연결을 삭제할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteVolume	EBS 볼륨을 삭제할 수 있는 권한을 부여합니다.	쓰기	volume* (p. 1052)	ec2:AvailabilityZone (p. 1055) ec2:Encrypted (p. 1056) ec2:ParentSnapshot (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)	
DeleteVpc	VPC를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVpcEndpointConnectionNotifications	하나 이상의 VPC 엔드포인트 연결 알림을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVpcEndpointServiceConfigurations	하나 이상의 VPC 엔드포인트 서비스 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기	vpc-endpoint-service* (p. 1053)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteVpcEndpoints	하나 이상의 VPC 엔드포인트를 삭제할 수 있는 권한을 부여합니다.	쓰기	vpc-endpoint* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteVpcPeeringConnection	VPC 피어링 연결을 삭제할 수 있는 권한을 부여합니다.	쓰기	vpc-peering-connection* (p. 1053)	ec2:AccepterVpc (p. 1055) ec2:Region (p. 1057) ec2:RequesterVpc (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DeleteVpnConnection	VPN 연결을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVpnConnectionRoute	가상 프라이빗 게이트웨이와 고객 게이트웨이 간의 VPN 연결에 대한 고정 라우팅을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteVpnGateway	가상 프라이빗 게이트웨이를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeprovisionByoipCidr	고유 IP 주소 가져오기(BYOIP)를 통해 프로비저닝된 IP 주소 범위를 해제하고 해당 주소 풀을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeregisterImage	Amazon Machine Image(AMI) 등록을 취소할 수 있는 권한을 부여합니다.	쓰기			
DeregisterTransitGatewayMulticastGroupMembers	전송 게이트웨이 멀티캐스트 도메인의 그룹 IP 주소에서 하나 이상의 네트워크 인터페이스 멤버의 등록을 취소할 수 있는 권한을 부여합니다.	쓰기	network-interface* (p. 1048)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeregisterTransitGatewayMulticastGroupSources	전송 게이트웨이 멀티캐스트 도메인 그룹 IP 주소에서 하나 이상의 네트워크 인터페이스 소스의 등록을 취소할 수 있는 권한을 부여합니다.	쓰기	network-interface* (p. 1048)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DescribeAccountAttributes	AWS 계정의 속성을 설명할 수 있는 권한을 부여합니다.	List			
DescribeAddresses	하나 이상의 탄력적 IP 주소를 설명할 수 있는 권한을 부여합니다.	List			
DescribeAggregateIdFormat	모든 리소스 유형에 대해 더 긴 ID 형식 설정을 설명할 수 있는 권한을 부여합니다.	List			
DescribeAvailabilityZones	사용 가능한 하나 이상의 가용 영역을 설명할 수 있는 권한을 부여합니다.	List			
DescribeBundleTasks	하나 이상의 번들링 작업을 설명할 수 있는 권한을 부여합니다.	List			
DescribeByoipCidrs	고유 IP 주소 가져오기(BYOIP)를 통해 프로비저닝된 IP 주소 범위를 설명할 수 있는 권한을 부여합니다.	List			
DescribeCapacityReservations	하나 이상의 용량 예약을 설명할 수 있는 권한을 부여합니다.	List			
DescribeClassicLinkInstances	하나 이상의 연결된 EC2-Classic 인스턴스를 설명할 수 있는 권한을 부여합니다.	List			
DescribeClientVpnAuthorizationRules	Client VPN 엔드포인트에 대한 권한 부여 규칙을 설명할 수 있는 권한을 부여합니다.	List			
DescribeClientVpnConnections	Client VPN 엔드포인트에 대한 활성 클라이언트 연결과 직전 60분 간 종료된 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeClientVpnEndpoints	하나 이상의 Client VPN 엔드포인트를 설명할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeClientVpnRoutes	Client VPN 엔드포인트에 대한 라우팅을 설명할 수 있는 권한을 부여합니다.	List			
DescribeClientVpnTargetNetworks	Client VPN 엔드포인트와 연결된 대상 네트워크를 설명할 수 있는 권한을 부여합니다.	List			
DescribeConversionTasks	하나 이상의 변환 작업을 설명할 수 있는 권한을 부여합니다.	List			
DescribeCustomerGateways	하나 이상의 고객 게이트웨이를 설명할 수 있는 권한을 부여합니다.	List			
DescribeDhcpOptions	하나 이상의 DHCP 옵션 세트를 설명할 수 있는 권한을 부여합니다.	List			
DescribeEgressOnlyInternetGateways	하나 이상의 외부 전용 인터넷 게이트웨이를 설명할 수 있는 권한을 부여합니다.	List			
DescribeElasticGpus	인스턴스와 연결된 Elastic Graphics 액셀러레이터를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeExportImageTasks	하나 이상의 이미지 내보내기 작업을 설명할 수 있는 권한을 부여합니다.	List			
DescribeExportTasks	하나 이상의 인스턴스 내보내기 작업을 설명할 수 있는 권한을 부여합니다.	List			
DescribeFastSnapshotRestores	스냅샷에 대한 빠른 스냅샷 복원 상태를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeFleetHistory	지정된 시간 동안 EC2 플릿에 대한 이벤트를 설명할 수 있는 권한을 부여합니다.	List			
DescribeFleetInstances	EC2 플릿에 대해 실행 중인 인스턴스를 설명할 수 있는 권한을 부여합니다.	List			
DescribeFleets	하나 이상의 EC2 플릿을 설명할 수 있는 권한을 부여합니다.	List			
DescribeFlowLogs	하나 이상의 흐름 로그를 설명할 수 있는 권한을 부여합니다.	List			
DescribeFpgaImageAttribute	Amazon FPGA 이미지(AFI)의 속성을 설명할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeFpgaImages	하나 이상의 Amazon FPGA 이미지(AFI)를 설명할 수 있는 권한을 부여합니다.	List			
DescribeHostReservationOfferings	구입할 수 있는 전용 호스트 예약을 설명할 수 있는 권한을 부여합니다.	List			
DescribeHostReservations	AWS 계정의 전용 호스트와 연결된 전용 호스트 예약을 설명할 수 있는 권한을 부여합니다.	List			
DescribeHosts	하나 이상의 전용 호스트를 설명할 수 있는 권한을 부여합니다.	List			
DescribeIamInstanceProfileAssociations	IAM 인스턴스 프로파일 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeIdFormat	리소스에 대한 ID 형식 설정을 설명할 수 있는 권한을 부여합니다.	List			
DescribeIdentityIdFormat	IAM 사용자, IAM 역할 또는 루트 사용자의 리소스에 대한 ID 형식 설정을 설명할 수 있는 권한을 부여합니다.	List			
DescribeImageAttribute	Amazon Machine Image(AMI)의 속성을 설명할 수 있는 권한을 부여합니다.	List			
DescribeImages	하나 이상의 이미지(AMI, AKI 및 ARI)를 설명할 수 있는 권한을 부여합니다.	List			
DescribeImportImageTasks	가상 머신 가져오기 또는 스냅샷 가져오기 작업을 설명할 수 있는 권한을 부여합니다.	List			
DescribeImportSnapshotTasks	스냅샷 가져오기 작업을 설명할 수 있는 권한을 부여합니다.	List			
DescribeInstanceAttribute	인스턴스의 속성을 설명할 수 있는 권한을 부여합니다.	List			
DescribeInstanceCreditSpecifications	하나 이상의 버스트 가능 성능 인스턴스의 CPU 사용량에 대한 크레딧 옵션을 설명할 수 있는 권한을 부여합니다.	List			
DescribeInstanceStatus	하나 이상의 인스턴스 상태를 설명할 수 있는 권한을 부여합니다.	List			
DescribeInstanceTypes	AWS 리전에서 제공되는 모든 인스턴스 유형을 설명할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeInstances	하나 이상의 인스턴스를 설명할 수 있는 권한을 부여합니다.	List			
DescribeInternetGateways	하나 이상의 인터넷 게이트웨이를 설명할 수 있는 권한을 부여합니다.	List			
DescribeKeyPairs	하나 이상의 키 페어를 설명할 수 있는 권한을 부여합니다.	List			
DescribeLaunchTemplateVersions	하나 이상의 시작 템플릿 버전을 설명할 수 있는 권한을 부여합니다.	List			
DescribeLaunchTemplates	하나 이상의 시작 템플릿을 설명할 수 있는 권한을 부여합니다.	List			
DescribeLocalGatewayVirtualInterfaceGroupAssociations	가상 인터페이스 그룹과 로컬 게이트웨이 라우팅 테이블 간의 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeLocalGatewayRouteTableVpcAssociations	VPC와 로컬 게이트웨이 라우팅 테이블 간의 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeLocalGatewayRouteTables	하나 이상의 로컬 게이트웨이 라우팅 테이블을 설명할 수 있는 권한을 부여합니다.	List			
DescribeLocalGatewayVirtualInterfaceGroups	로컬 게이트웨이 가상 인터페이스 그룹을 설명할 수 있는 권한을 부여합니다.	List			
DescribeLocalGatewayVirtualInterfaces	로컬 게이트웨이 가상 인터페이스를 설명할 수 있는 권한을 부여합니다.	List			
DescribeLocalGateways	하나 이상의 로컬 게이트웨이를 설명할 수 있는 권한을 부여합니다.	List			
DescribeMovingAddresses	EC2-VPC 플랫폼으로 이동되는 탄력적 IP 주소를 설명할 수 있는 권한을 부여합니다.	List			
DescribeNatGateways	하나 이상의 NAT 게이트웨이를 설명할 수 있는 권한을 부여합니다.	List			
DescribeNetworkAcls	하나 이상의 네트워크 ACL을 설명할 수 있는 권한을 부여합니다.	List			
DescribeNetworkInterfaceAttribute	네트워크 인터페이스 속성을 설명할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeNetworkInterfacePermissions	네트워크 인터페이스와 연결된 권한을 설명할 수 있는 권한을 부여합니다.	List			
DescribeNetworkInterfaces	하나 이상의 네트워크 인터페이스를 설명할 수 있는 권한을 부여합니다.	List			
DescribePlacementGroups	하나 이상의 배치 그룹을 설명할 수 있는 권한을 부여합니다.	List			
DescribePrefixLists	사용 가능한 AWS 서비스를 접두사 목록 형식으로 설명할 수 있는 권한을 부여합니다.	List			
DescribePrincipalIdFormat	루트 사용자 및 모든 IAM 역할 그리고 더 긴 ID(17자 ID) 기본 설정을 명시적으로 지정한 IAM 사용자에 대한 ID 형식 설정을 설명할 수 있는 권한을 부여합니다.	List			
DescribePublicIpv4Pools	하나 이상의 IPv4 주소 풀을 설명할 수 있는 권한을 부여합니다.	List			
DescribeRegions	계정에서 현재 사용 가능한 하나 이상의 AWS 리전을 설명할 수 있는 권한을 부여합니다.	List			
DescribeReservedInstances	계정에서 구입한 하나 이상의 예약 인스턴스를 설명할 수 있는 권한을 부여합니다.	List			
DescribeReservedInstancesListings	예약 인스턴스 마켓플레이스에 등록된 계정의 예약 인스턴스 목록을 설명할 수 있는 권한을 부여합니다.	List			
DescribeReservedInstancesModifications	하나 이상의 예약 인스턴스에 대한 수정 사항을 설명할 수 있는 권한을 부여합니다.	List			
DescribeReservedInstancesOfferings	구매 가능한 예약 인스턴스 상품을 설명할 수 있는 권한을 부여합니다.	List			
DescribeRouteTables	하나 이상의 라우팅 테이블을 설명할 수 있는 권한을 부여합니다.	List			
DescribeScheduledInstanceAvailability	정기 인스턴스에 사용 가능한 일정을 찾을 수 있는 권한을 부여합니다.	Read			
DescribeScheduledInstances	계정에 있는 하나 이상의 정기 인스턴스를 설명할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeSecurityGroupReferences	지정된 보안 그룹을 참조하고 있는 VPC 피어링 연결의 다른 쪽에 있는 VPC를 설명할 수 있는 권한을 부여합니다.	List			
DescribeSecurityGroups	하나 이상의 보안 그룹을 설명할 수 있는 권한을 부여합니다.	List			
DescribeSnapshotAttribute	스냅샷의 속성을 설명할 수 있는 권한을 부여합니다.	List			
DescribeSnapshots	하나 이상의 EBS 스냅샷을 설명할 수 있는 권한을 부여합니다.	List			
DescribeSpotDatafeedSubscription	스팟 인스턴스에 대한 데이터 피드를 설명할 수 있는 권한을 부여합니다.	List			
DescribeSpotFleetInstances	스팟 플릿에 대해 실행 중인 인스턴스를 설명할 수 있는 권한을 부여합니다.	List			
DescribeSpotFleetRequestHistory	지정된 시간 동안 스팟 플릿 요청에 대한 이벤트를 설명할 수 있는 권한을 부여합니다.	List			
DescribeSpotFleetRequests	하나 이상의 스팟 플릿 요청을 설명할 수 있는 권한을 부여합니다.	List			
DescribeSpotInstanceRequests	하나 이상의 스팟 인스턴스 요청을 설명할 수 있는 권한을 부여합니다.	List			
DescribeSpotPriceHistory	스팟 인스턴스 가격 기록을 설명할 수 있는 권한을 부여합니다.	List			
DescribeStaleSecurityGroups	지정된 VPC의 보안 그룹에 대한 과거 참조 보안 그룹 규칙을 설명할 수 있는 권한을 부여합니다.	List			
DescribeSubnets	하나 이상의 서브넷을 설명할 수 있는 권한을 부여합니다.	List			
DescribeTags	Amazon EC2 리소스에 대한 하나 이상의 태그를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeTrafficMirrorFilters	하나 이상의 트래픽 미러 필터를 설명할 수 있는 권한을 부여합니다.	List			
DescribeTrafficMirrorSessions	하나 이상의 트래픽 미러 세션을 설명할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeTrafficMirrorTargets	하나 이상의 트래픽 미러 대상을 설명할 수 있는 권한을 부여합니다.	List			
DescribeTransitGatewayAttachments	리소스와 전송 게이트웨이 간 하나 이상의 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeTransitGatewayMulticastDomains	하나 이상의 전송 게이트웨이 멀티캐스트 도메인을 설명할 수 있는 권한을 부여합니다.	List			
DescribeTransitGatewayPeeringAttachments	하나 이상의 전송 게이트웨이 피어링 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeTransitGatewayRouteTables	하나 이상의 전송 게이트웨이 라우팅 테이블을 설명할 수 있는 권한을 부여합니다.	List			
DescribeTransitGatewayVpcAttachments	전송 게이트웨이에서 하나 이상의 VPC 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeTransitGateways	하나 이상의 전송 게이트웨이를 설명할 수 있는 권한을 부여합니다.	List			
DescribeVolumeAttribute	EBS 볼륨의 속성을 설명할 수 있는 권한을 부여합니다.	List			
DescribeVolumeStatus	하나 이상의 EBS 볼륨 상태를 설명할 수 있는 권한을 부여합니다.	List			
DescribeVolumes	하나 이상의 EBS 볼륨을 설명할 수 있는 권한을 부여합니다.	List			
DescribeVolumesModifications	하나 이상의 EBS 볼륨의 현재 수정 상태를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeVpcAttribute	VPC의 속성을 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcClassicLink	하나 이상 VPC의 ClassicLink 상태를 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcClassicLinkDnsSupport	하나 이상 VPC의 ClassicLink DNS 지원 상태를 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcEndpointConnectionNotifications	VPC 엔드포인트 및 VPC 엔드포인트 서비스에 대한 연결 알림을 설명할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeVpcEndpointConnections	VPC 엔드포인트 서비스에 대한 VPC 엔드포인트 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcEndpointServiceConfigurations	VPC 엔드포인트 서비스 구성(사용자 서비스)을 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcEndpointServicePermissions	VPC 엔드포인트 서비스를 검색하도록 허용되는 보안 주체(서비스 소비자)를 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcEndpointServices	VPC 엔드포인트를 생성할 때 지정할 수 있는 모든 지원되는 AWS 서비스를 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcEndpoints	하나 이상의 VPC 엔드포인트를 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcPeeringConnections	하나 이상의 VPC 피어링 연결을 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpcs	하나 이상의 VPC를 설명할 수 있는 권한을 부여합니다.	List			
DescribeVpnConnections	하나 이상의 VPN 연결을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeVpnGateways	하나 이상의 가상 프라이빗 게이트웨이를 설명할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DetachClassicLinkVpc	연결된 EC2-Classic 인스턴스를 VPC에서 연결 해제(분리)할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
			vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	
DetachInternetGateway	VPC에서 인터넷 게이트웨이를 분리할 수 있는 권한을 부여합니다.	쓰기			
DetachNetworkInterface	인스턴스에서 네트워크 인터페이스를 분리할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DetachVolume	인스턴스에서 EBS 볼륨을 분리할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
			volume* (p. 1052)	ec2:AvailabilityZone (p. 1055) ec2:Encrypted (p. 1056) ec2:ParentSnapshot (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)	
DetachVpnGateway	VPC에서 가상 프라이빗 게이트웨이를 분리할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DisableEbsEncryptionByDefault	계정에 기본적으로 EBS 암호화를 비활성화할 수 있는 권한을 부여합니다.	쓰기			
DisableFastSnapshotRestores	지정된 가용 영역에 있는 하나 이상의 스냅샷에 대한 빠른 스냅샷 복원을 비활성화할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1049)	ec2:Owner (p. 1056) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057) ec2:AvailabilityZone (p. 1055) ec2:SnapshotTime (p. 1058) ec2:Encrypted (p. 1056) ec2:VolumeSize (p. 1058) ec2:ResourceTag/${TagKey} (p. 1057)	
DisableTransitGatewayRouteTablePropagation	지정된 전파 라우팅 테이블로 라우팅을 전파하지 않도록 리소스 연결을 비활성화할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-route-table* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DisableVgwRoutePropagation	VPC의 지정된 라우팅 테이블로 라우팅을 전파하지 않도록 가상 프라이빗 게이트웨이를 비활성화할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DisableVpcClassicLink	VPC에 대한 ClassicLink를 비활성화할 수 있는 권한을 부여합니다.	쓰기	vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	
DisableVpcClassicLinkDnsSupport	VPC에 대한 ClassicLink DNS 지원을 비활성화할 수 있는 권한을 부여합니다.	쓰기			
DisassociateAddress	인스턴스 또는 네트워크 인터페이스에서 탄력적 IP 주소의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기			
DisassociateClientVpnTargetNetwork	Client VPN 엔드포인트에서 대상 네트워크의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DisassociateIamInstanceProfile	실행 중이거나 중지된 인스턴스에서 IAM 인스턴스 프로파일의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DisassociateRouteTable	라우팅 테이블에서 서브넷의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기			
DisassociateSubnetCidrBlock	서브넷에서 CIDR 블록의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기			
DisassociateTransitGatewayMulticastDomain	전송 게이트웨이 멀티캐스트 도메인에서 하나 이상의 서브넷의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기	subnet* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DisassociateTransitGatewayRouteTable	전송 게이트웨이 라우팅 테이블에서 리소스 연결을 연결 해제할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-route-table* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
DisassociateVpcCidrBlock	VPC에서 CIDR 블록의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기			
EnableEbsEncryptionByDefault	계정에 기본적으로 EBS 암호화를 활성화할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
EnableFastSnapshotRestores	지정된 가용 영역에 있는 하나 이상의 스냅샷에 대한 빠른 스냅샷 복원을 활성화할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1049)	ec2:Owner (p. 1056) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057) ec2:AvailabilityZone (p. 1055) ec2:SnapshotTime (p. 1058) ec2:Encrypted (p. 1056) ec2:VolumeSize (p. 1058) ec2:ResourceTag/${TagKey} (p. 1057)	
EnableTransitGatewayRouteTablePropagation	전파 라우팅 테이블에 라우팅을 전파하도록 연결을 활성화할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-route-table* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
EnableVgwRoutePropagation	VPC 라우팅 테이블에 라우팅을 전파하도록 가상 프라이빗 게이트웨이를 활성화할 수 있는 권한을 부여합니다.	쓰기			
EnableVolumeIO	I/O 작업이 비활성화된 볼륨에 I/O 작업을 활성화할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
EnableVpcClassicLink	VPC에 ClassicLink를 활성화할 수 있는 권한을 부여합니다.	쓰기	vpc* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)	
EnableVpcClassicLinkDnsSupport	VPC가 ClassicLink에 대한 DNS 호스트 이름 확인을 지원하도록 설정할 수 있는 권한을 부여합니다.	쓰기			
ExportClientVpnClientCertificateRevocationList	지정된 Client VPN 엔드포인트에 대한 클라이언트 인증서 취소 목록을 다운로드할 수 있는 권한을 부여합니다.	List			
ExportClientVpnClientConfiguration	Client VPN 엔드포인트에 대한 Client VPN 엔드포인트 구성 파일의 내용을 다운로드할 수 있는 권한을 부여합니다.	List			
ExportImage	Amazon Machine Image(AMI)를 VM 파일로 내보낼 수 있는 권한을 부여합니다.	쓰기			
ExportTransitGatewayRoutes	전송 게이트웨이 라우팅 테이블에서 Amazon S3 버킷으로 라우팅을 내보낼 수 있는 권한을 부여합니다.	쓰기			
GetCapacityReservationUsage	용량 예약에 대한 사용량 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetConsoleOutput	인스턴스에 대한 콘솔 출력을 가져올 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetConsoleScreenshot	실행 중인 인스턴스의 JPG 형식 스크린샷을 검색할 수 있는 권한을 부여합니다.	Read	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
GetDefaultCreditSpecification	버스트 가능 성능 인스턴스 패밀리의 CPU 사용량에 대한 기본 크레딧 옵션을 가져올 수 있는 권한을 부여합니다.	Read			
GetEbsDefaultKmsKeyId	기본적으로 EBS 암호화를 위한 기본 고객 마스터 키(CMK)의 ID를 가져올 수 있는 권한을 부여합니다.	Read			
GetEbsEncryptionByDefault	계정에 기본적으로 EBS 암호화가 활성화되어 있는지 여부를 설명할 수 있는 권한을 부여합니다.	Read			
GetHostReservationPurchasePreview	전용 호스트의 구성과 일치하는 구성의 예약 구매를 미리 볼 수 있는 권한을 부여합니다.	Read			
GetLaunchTemplateData	새 시작 템플릿 또는 시작 템플릿 버전에 사용하도록 지정된 인스턴스의 구성 데이터를 가져올 수 있는 권한을 부여합니다.	Read			
GetPasswordData	실행 중인 Windows 인스턴스에 대해 암호화된 관리자 암호를 검색할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetReservedInstancesExchangeQuote	하나 이상의 컨버터블 예약 인스턴스를 새 컨버터블 예약 인스턴스로 교환하기 위한 교환 정보 및 견적서를 반환할 수 있는 권한을 부여합니다.	Read			
GetTransitGatewayAttachmentPropagations	리소스 연결이 라우팅을 전파하는 라우팅 테이블을 나열할 수 있는 권한을 부여합니다.	List			
GetTransitGatewayMulticastDomainAssociations	전송 게이트웨이 멀티캐스트 도메인에 대한 연결 정보를 가져올 수 있는 권한을 부여합니다.	List			
GetTransitGatewayRouteTableAssociations	전송 게이트웨이 라우팅 테이블에 대한 연결 정보를 가져올 수 있는 권한을 부여합니다.	List			
GetTransitGatewayRouteTablePropagations	전송 게이트웨이 라우팅 테이블에 대한 라우팅 테이블 전파 정보를 가져올 수 있는 권한을 부여합니다.	List			
ImportClientVpnClientCertificateRevocationList	Client VPN 엔드포인트에 클라이언트 인증서 취소 목록을 업로드할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ImportImage	단일 또는 다중 볼륨 디스크 이미지 또는 EBS 스냅샷을 Amazon Machine 이미지(AMI)로 가져올 수 있는 권한을 부여합니다.	쓰기			
ImportInstance	디스크 이미지의 메타데이터를 사용하여 인스턴스 가져오기 작업을 생성할 수 있는 권한을 부여합니다.	쓰기			
ImportKeyPair	타사 도구를 사용하여 생성한 RSA 키 페어에서 퍼블릭 키를 가져올 수 있는 권한을 부여합니다.	쓰기			
ImportSnapshot	디스크를 EBS 스냅샷으로 가져올 수 있는 권한을 부여합니다.	쓰기			
ImportVolume	디스크 이미지의 메타데이터를 사용하여 볼륨 가져오기 작업을 생성할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyCapacityReservation	용량 예약의 용량 및 해제 조건을 수정할 수 있는 권한을 부여합니다.	쓰기	capacity-reservation* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ModifyClientVpnEndpoint	Client VPN 엔드포인트를 수정할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ModifyDefaultCreditSpecification	버스트 가능 성능 인스턴스의 CPU 사용량에 대한 계정 수준 기본 크레딧 옵션을 변경할 수 있는 권한을 부여합니다.	쓰기			
ModifyEbsDefaultKmsKeyId	계정에서 기본적으로 EBS 암호화를 위한 기본 고객 마스터 키(CMK)를 변경할 수 있는 권한을 부여합니다.	쓰기			
ModifyFleet	EC2 플릿을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyFpgaImageAttribute	Amazon FPGA 이미지(AFI)의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyHosts	전용 호스트를 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyIdFormat	리소스의 ID 형식을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyIdentityIdFormat	계정의 특정 보안 주체의 리소스 ID 형식을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyImageAttribute	Amazon Machine Image(AMI)의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyInstanceAttribute	인스턴스의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyInstanceCapacityReservationAttributes	중지된 인스턴스에 대한 용량 예약 설정을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyInstanceCreditSpecification	인스턴스의 CPU 사용량에 대한 크레딧 옵션을 수정할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyInstanceEventStartTime	예약된 EC2 인스턴스 이벤트의 시작 시간을 수정할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:Region (p. 1057)	
ModifyInstanceMetadataOptions	인스턴스에 대한 메타데이터 옵션을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyInstancePlacement	인스턴스의 배치 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyLaunchTemplate	시작 템플릿을 수정할 수 있는 권한을 부여합니다.	쓰기	launch-template* (p. 1046)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ModifyNetworkInterfaceAttribute	네트워크 인터페이스의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyReservedInstances	하나 이상의 예약 인스턴스의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifySnapshotAttribute	스냅샷에 대한 권한 설정을 추가하거나 제거할 수 있는 권한을 부여합니다.	권한 관리	snapshot* (p. 1049)	ec2:Owner (p. 1056) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:SnapshotTime (p. 1058) ec2:VolumeSize (p. 1058)	
ModifySpotFleetRequest	스팟 플릿 요청을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifySubnetAttribute	서브넷의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyTrafficMirrorFilterNetworkServices	미러링 네트워크 서비스를 허용하거나 제한할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-filter* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyTrafficMirrorFilterRule	트래픽 미러 규칙을 수정할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-filter* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			traffic-mirror-filter-rule* (p. 1050)	ec2:Region (p. 1057)	
ModifyTrafficMirrorSession	트래픽 미러 세션을 수정할 수 있는 권한을 부여합니다.	쓰기	traffic-mirror-session* (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			traffic-mirror-filter (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			traffic-mirror-target (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ModifyTransitGatewayPrefixListReference	전송 게이트웨이에서 VPC 연결을 수정할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			subnet (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ModifyVolume	EBS 볼륨의 파라미터를 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyVolumeAttribute	볼륨의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyVpcAttribute	VPC의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyVpcEndpoint	VPC 엔드포인트의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기	vpc-endpoint* (p. 1052)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			route-table (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			security-group (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			subnet (p. 1050)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ModifyVpcEndpointConnectionNotification	VPC 엔드포인트 또는 VPC 엔드포인트 서비스에 대한 연결 알림을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyVpcEndpointServiceConfiguration	VPC 엔드포인트 서비스 구성의 속성을 수정할 수 있는 권한을 부여합니다.	쓰기	vpc-endpoint-service* (p. 1053)	ec2:Region (p. 1057) ec2:VpceServicePrivateDnsName (p. 1058) ec2:ResourceTag/${TagKey} (p. 1057)	
ModifyVpcEndpointServicePermissions	VPC 엔드포인트 서비스에 대한 권한을 수정할 수 있는 권한을 부여합니다.	권한 관리	vpc-endpoint-service* (p. 1053)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ModifyVpcPeeringConnectionOptions	VPC 피어링 연결의 한 쪽에서 VPC 피어링 연결 옵션을 수정할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyVpcTenancy	VPC의 인스턴스 테넌시 속성을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyVpnConnection	사이트 간 VPN 연결의 대상 게이트웨이를 수정할 수 있는 권한을 부여합니다.	쓰기	vpn-connection* (p. 1054)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:GatewayType (p. 1056)	
ModifyVpnTunnelCertificate	사이트 간 VPN 연결에 대한 인증서를 수정할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyVpnTunnelOptions	사이트 간 VPN 연결에 대한 옵션을 수정할 수 있는 권한을 부여합니다.	쓰기	vpn-connection* (p. 1054)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:AuthenticationType (p. 1055) ec2:DPDTimeoutSeconds (p. 1055) ec2:IKEVersions (p. 1056) ec2:InsideTunnelCidr (p. 1056) ec2:Phase1DHGroupNumbers (p. 1056) ec2:Phase2DHGroupNumbers (p. 1057) ec2:Phase1EncryptionAlgorithms (p. 1056) ec2:Phase2EncryptionAlgorithms (p. 1057) ec2:Phase1IntegrityAlgorithms (p. 1057) ec2:Phase2IntegrityAlgorithms (p. 1057) ec2:Phase1LifetimeSeconds (p. 1057) ec2:Phase2LifetimeSeconds (p. 1057) ec2:PresharedKeys (p. 1057) ec2:RekeyFuzzPercentage (p. 1057) ec2:RekeyMarginTimeSeconds (p. 1057) ec2:RoutingType (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
MonitorInstances	실행 중인 인스턴스에 대한 세부 모니터링을 활성화할 수 있는 권한을 부여합니다.	쓰기			
MoveAddressToVpc	EC2-Classic 플랫폼에서 EC2-VPC 플랫폼으로 탄력적 IP 주소를 이동할 수 있는 권한을 부여합니다.	쓰기			
ProvisionByoipCidr	고유 IP 주소 가져오기(BYOIP)를 통해 AWS에서 사용할 주소 범위를 프로비저닝하고 해당 주소 풀을 생성할 수 있는 권한을 부여합니다.	쓰기			
PurchaseHostReservation	전용 호스트의 구성과 일치하는 구성을 사용하여 예약을 구매할 수 있는 권한을 부여합니다.	쓰기			
PurchaseReservedInstancesOffering	예약 인스턴스 상품을 구매할 수 있는 권한을 부여합니다.	쓰기			
PurchaseScheduledInstances	지정된 일정으로 하나 이상의 정기 인스턴스를 구매할 수 있는 권한을 부여합니다.	쓰기			
RebootInstances	하나 이상의 인스턴스 재부팅을 요청할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RegisterImage	Amazon Machine Image(AMI)를 등록할 수 있는 권한을 부여합니다.	쓰기			
RegisterTransitGatewayMulticastGroupMembers	전송 게이트웨이 멀티캐스트 도메인에서 하나 이상의 네트워크 인터페이스를 그룹 IP 주소의 멤버로 등록할 수 있는 권한을 부여합니다.	쓰기	network-interface* (p. 1048)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
RegisterTransitGatewayMulticastGroupSources	전송 게이트웨이 멀티캐스트 도메인에서 하나 이상의 네트워크 인터페이스를 그룹 IP 주소의 소스로 등록할 수 있는 권한을 부여합니다.	쓰기	network-interface* (p. 1048)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-multicast-domain* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
RejectTransitGatewayPeeringAttachment	전송 게이트웨이 피어링 연결 요청을 거부할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
RejectTransitGatewayVpcAttachment	VPC를 전송 게이트웨이에 연결하라는 요청을 거부할 수 있는 권한을 부여합니다.	쓰기	transit-gateway-attachment* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
RejectVpcEndpointConnections	VPC 엔드포인트 서비스에 대한 VPC 엔드포인트 연결 요청을 하나 이상 거부할 수 있는 권한을 부여합니다.	쓰기	vpc-endpoint-service* (p. 1053)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RejectVpcPeeringConnection	VPC 피어링 연결 요청을 거부할 수 있는 권한을 부여합니다.	쓰기	vpc-peering-connection* (p. 1053)	ec2:AccepterVpc (p. 1055) ec2:Region (p. 1057) ec2:RequesterVpc (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ReleaseAddress	탄력적 IP 주소를 해제할 수 있는 권한을 부여합니다.	쓰기			
ReleaseHosts	하나 이상의 온디맨드 전용 호스트를 해제할 수 있는 권한을 부여합니다.	쓰기			
ReplaceIamInstanceProfileAssociation	인스턴스에 대한 IAM 인스턴스 프로파일을 교체할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	iam:PassRole
ReplaceNetworkAclAssociation	서브넷이 연결되는 네트워크 ACL을 변경할 수 있는 권한을 부여합니다.	쓰기			
ReplaceNetworkAclEntry	네트워크 ACL의 항목(규칙)을 바꿀 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ReplaceRoute	VPC의 라우팅 테이블에서 라우팅을 바꿀 수 있는 권한을 부여합니다.	쓰기	route-table* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
ReplaceRouteTableAssociation	서브넷과 연결된 라우팅 테이블을 변경할 수 있는 권한을 부여합니다.	쓰기			
ReplaceTransitGatewayRoute	전송 게이트웨이 라우팅 테이블에서 라우팅을 바꿀 수 있는 권한을 부여합니다.	쓰기	transit-gateway-route-table* (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
			transit-gateway-attachment (p. 1051)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
ReportInstanceStatus	인스턴스 상태에 대한 피드백을 제출할 수 있는 권한을 부여합니다.	쓰기			
RequestSpotFleet	스팟 플릿 요청을 생성할 수 있는 권한을 부여합니다.	쓰기			
RequestSpotInstances	스팟 인스턴스 요청을 생성할 수 있는 권한을 부여합니다.	쓰기			
ResetEbsDefaultKmsKeyId	EBS용 AWS 관리형 고객 마스터 키(CMK)를 사용하도록 계정의 EBS 암호화를 위한 기본 CMK를 재설정할 수 있는 권한을 부여합니다.	쓰기			
ResetFpgaImageAttribute	Amazon FPGA 이미지(AFI)의 속성을 기본값으로 재설정할 수 있는 권한을 부여합니다.	쓰기			
ResetImageAttribute	Amazon Machine Image(AMI)의 속성을 기본값으로 재설정할 수 있는 권한을 부여합니다.	쓰기			
ResetInstanceAttribute	인스턴스의 속성을 기본값으로 재설정할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ResetNetworkInterfaceAttribute	네트워크 인터페이스의 속성을 재설정할 수 있는 권한을 부여합니다.	쓰기			
ResetSnapshotAttribute	스냅샷에 대한 권한 설정을 재설정할 수 있는 권한을 부여합니다.	권한 관리			
RestoreAddressToClassic	EC2-VPC 플랫폼으로 이미 이동한 탄력적 IP 주소를 EC2-Classic 플랫폼으로 다시 복원할 수 있는 권한을 부여합니다.	쓰기			
RevokeClientVpnIngress	Client VPN 엔드포인트에서 인바운드 권한 부여 규칙을 제거할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	
RevokeSecurityGroupEgress	VPC 보안 그룹에서 하나 이상의 아웃바운드 규칙을 제거할 수 있는 권한을 부여합니다.	쓰기	security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
RevokeSecurityGroupIngress	보안 그룹에서 하나 이상의 인바운드 규칙을 제거할 수 있는 권한을 부여합니다.	쓰기	security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RunInstances	하나 이상의 인스턴스를 시작할 수 있는 권한을 부여합니다.	쓰기	image* (p. 1045)	ec2:ImageType (p. 1056) ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:Owner (p. 1056) ec2:Public (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			instance* (p. 1045)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058) ec2:MetadataHttpEndpoint (p. 1056) ec2:MetadataHttpTokens (p. 1056) ec2:MetadataHttpPutResponseHopLim (p. 1056)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			network-interface* (p. 1048)	ec2:AvailabilityZone (p. 1055) ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/ (p. 1057) ec2:Subnet (p. 1058) ec2:Vpc (p. 1058) ec2:AssociatePublicIpAddress (p. 1055)	
			security-group* (p. 1049)	ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			subnet* (p. 1050)	ec2:AvailabilityZone (p. 1055) ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
			volume* (p. 1052)	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Encrypted (p. 1056) ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:ParentSnapshot (p. 1056) ec2:Region (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)	
			elastic-gpu (p. 1044)	ec2:ElasticGpuType (p. 1055)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			key-pair (p. 1046)	ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:Region (p. 1057)	
			launch-template (p. 1046)	ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:Region (p. 1057)	
			placement-group (p. 1048)	ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:PlacementGroupStrategy (p. 1057) ec2:Region (p. 1057)	
			snapshot (p. 1049)	ec2:IsLaunchTemplateResource (p. 1056) ec2:LaunchTemplate (p. 1056) ec2:Owner (p. 1056) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:SnapshotTime (p. 1058) ec2:VolumeSize (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	시나리오: EC2-Classic-EBS		image* (p. 1045) instance* (p. 1045) security-group* (p. 1049) volume* (p. 1052) key-pair (p. 1046) placement-group (p. 1048) snapshot (p. 1049)		
	시나리오: EC2-Classic-InstanceStore		image* (p. 1045) instance* (p. 1045) security-group* (p. 1049) key-pair (p. 1046) placement-group (p. 1048) snapshot (p. 1049)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	시나리오: EC2-VPC-EBS		image* (p. 1045) instance* (p. 1045) network-interface* (p. 1048) security-group* (p. 1049) volume* (p. 1052) key-pair (p. 1046) placement-group (p. 1048) snapshot (p. 1049)		
	시나리오: EC2-VPC-EBS-Subnet		image* (p. 1045) instance* (p. 1045) network-interface* (p. 1048) security-group* (p. 1049) subnet* (p. 1050) volume* (p. 1052) key-pair (p. 1046) placement-group (p. 1048) snapshot (p. 1049)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	시나리오: EC2-VPC-InstanceStore		image* (p. 1045) instance* (p. 1045) network-interface* (p. 1048) security-group* (p. 1049) key-pair (p. 1046) placement-group (p. 1048) snapshot (p. 1049)		
	시나리오: EC2-VPC-InstanceStore-Subnet		image* (p. 1045) instance* (p. 1045) network-interface* (p. 1048) security-group* (p. 1049) subnet* (p. 1050) key-pair (p. 1046) placement-group (p. 1048) snapshot (p. 1049)		
RunScheduledInstances	하나 이상의 정기 인스턴스를 시작할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SearchLocalGatewayRoutes	로컬 게이트웨이 라우팅 테이블에서 라우팅을 검색할 수 있는 권한을 부여합니다.	List			
SearchTransitGatewayMulticastGroups	전송 게이트웨이 멀티캐스트 도메인의 그룹 소스 및 멤버를 검색할 수 있는 권한을 부여합니다.	List			
SearchTransitGatewayRoutes	전송 게이트웨이 라우팅 테이블에서 라우팅을 검색할 수 있는 권한을 부여합니다.	List			
SendDiagnosticInterrupt	Amazon EC2 인스턴스에 진단 인터럽트를 보낼 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartInstances	중지된 인스턴스를 시작할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
StartVpcEndpointServicePrivateDnsVerification	VPC 엔드포인트 서비스에 대한 프라이빗 DNS 확인 프로세스를 시작할 수 있는 권한을 부여합니다.	쓰기	vpc-endpoint-service* (p. 1053)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StopInstances	Amazon EBS 지원 인스턴스를 중지할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
TerminateClientVpnConnections	활성 Client VPN 엔드포인트 연결을 종료할 수 있는 권한을 부여합니다.	쓰기	client-vpn-endpoint* (p. 1043)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
TerminateInstances	하나 이상의 인스턴스를 종료할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1045)	ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)	
UnassignIpv6Addresses	네트워크 인터페이스에서 하나 이상의 IPv6 주소 할당을 취소할 수 있는 권한을 부여합니다.	쓰기			
UnassignPrivateIpAddresses	네트워크 인터페이스에서 하나 이상의 보조 프라이빗 IP 주소 할당을 취소할 수 있는 권한을 부여합니다.	쓰기			
UnmonitorInstances	실행 중인 인스턴스에 대한 세부 모니터링을 비활성화할 수 있는 권한을 부여합니다.	쓰기			
UpdateSecurityGroupRuleDescriptionsEgress	VPC 보안 그룹에서 하나 이상의 아웃바운드 규칙에 대한 설명을 업데이트할 수 있는 권한을 부여합니다.	쓰기	security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateSecurityGroupRuleDescriptionsEgress	보안 그룹에서 하나 이상의 인바운드 규칙에 대한 설명을 업데이트할 수 있는 권한을 부여합니다.	쓰기	security-group* (p. 1049)	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)	
WithdrawByoipCidr	고유 IP 주소 가져오기(BYOIP)를 통해 AWS에서 사용하도록 프로비저닝된 IP 주소 범위의 공급을 중지할 수 있는 권한을 부여합니다.	쓰기			

Amazon EC2에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 955)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
capacity-reservation	`arn:${Partition}:ec2:${Region}:${Account}:capacity-reservation/${CapacityReservationId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
client-vpn-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:client-vpn-endpoint/${ClientVpnEndpointId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
customer-gateway	`arn:${Partition}:ec2:${Region}:${Account}:customer-gateway/${CustomerGatewayId}`	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
dedicated-host	`arn:${Partition}:ec2:${Region}:${Account}:dedicated-host/${HostId}`	aws:RequestTag/${TagKey} (p. 1055)

리소스 유형	ARN	조건 키
		aws:TagKeys (p. 1055) ec2:AutoPlacement (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:HostRecovery (p. 1056) ec2:InstanceType (p. 1056) ec2:Quantity (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
dhcp-options	`arn:${Partition}:ec2:${Region}:${Account}:dhcp-options/${DhcpOptionsId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
elastic-gpu	`arn:${Partition}:ec2:${Region}:${Account}:elasticGpu/${ElasticGpuId}`	
fpga-image	`arn:${Partition}:ec2:${Region}::fpga-image/${FpgaImageId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Owner (p. 1056) ec2:Public (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)

리소스 유형	ARN	조건 키
image	`arn:${Partition}:ec2:${Region}::image/${ImageId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:ImageType (p. 1056) ec2:Owner (p. 1056) ec2:Public (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058)
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:EbsOptimized (p. 1055) ec2:InstanceProfile (p. 1056) ec2:InstanceType (p. 1056) ec2:PlacementGroup (p. 1057) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:RootDeviceType (p. 1058) ec2:Tenancy (p. 1058)

리소스 유형	ARN	조건 키
internet-gateway	`arn:${Partition}:ec2:${Region}:${Account}:internet-gateway/${InternetGatewayId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
key-pair	`arn:${Partition}:ec2:${Region}:${Account}:key-pair/${KeyPairName}`	ec2:Region (p. 1057)
launch-template	`arn:${Partition}:ec2:${Region}:${Account}:launch-template/${LaunchTemplateId}`	ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
local-gateway	`arn:${Partition}:ec2:${Region}:${Account}:local-gateway/${LocalGatewayId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
local-gateway-route-table	`arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table/${LocalGatewayRouteTableId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
local-gateway-route-table-virtual-interface-group-association	`arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table-virtual-interface-group-association/${LocalGatewayRouteTableVirtualInterfaceGroupAssociationId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)

리소스 유형	ARN	조건 키
local-gateway-route-table-vpc-association	`arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table-vpc-association/${LocalGatewayRouteTableVpcAssociationId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
local-gateway-virtual-interface	`arn:${Partition}:ec2:${Region}:${Account}:local-gateway-virtual-interface/${LocalGatewayVirtualInterfaceId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
local-gateway-virtual-interface-group	`arn:${Partition}:ec2:${Region}:${Account}:local-gateway-virtual-interface-group/${LocalGatewayVirtualInterfaceGroupId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
network-acl	`arn:${Partition}:ec2:${Region}:${Account}:network-acl/${NaclId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)

리소스 유형	ARN	조건 키
network-interface	`arn:${Partition}:ec2:${Region}:${Account}:network-interface/${NetworkInterfaceId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AssociatePublicIpAddress (p. 1055) ec2:AuthorizedService (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Subnet (p. 1058) ec2:Vpc (p. 1058)
placement-group	`arn:${Partition}:ec2:${Region}:${Account}:placement-group/${PlacementGroupName}`	ec2:PlacementGroupStrategy (p. 1057) ec2:Region (p. 1057)
reserved-instances	`arn:${Partition}:ec2:${Region}:${Account}:reserved-instances/${ReservationId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:InstanceType (p. 1056) ec2:Region (p. 1057) ec2:ReservedInstancesOfferingType (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)

리소스 유형	ARN	조건 키
route-table	`arn:${Partition}:ec2:${Region}:${Account}:route-table/${RouteTableId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)
security-group	`arn:${Partition}:ec2:${Region}:${Account}:security-group/${SecurityGroupId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Owner (p. 1056) ec2:ParentVolume (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:SnapshotTime (p. 1058) ec2:VolumeSize (p. 1058)
spot-instance-request	`arn:${Partition}:ec2:${Region}::spot-instances-request/${SpotInstanceRequestId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)

리소스 유형	ARN	조건 키
subnet	`arn:${Partition}:ec2:${Region}:${Account}:subnet/${SubnetId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Vpc (p. 1058)
traffic-mirror-session	`arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-session/${TrafficMirrorSessionId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
traffic-mirror-target	`arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-target/${TrafficMirrorTargetId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
traffic-mirror-filter	`arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-filter/${TrafficMirrorFilterId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
traffic-mirror-filter-rule	`arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-filter-rule/${TrafficMirrorFilterRuleId}`	ec2:Region (p. 1057)

리소스 유형	ARN	조건 키
transit-gateway-attachment	`arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-attachment/${TransitGatewayAttachmentId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
transit-gateway-multicast-domain	`arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-multicast-domain/${TransitGatewayMulticastDomainId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
transit-gateway-route-table	`arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-route-table/${TransitGatewayRouteTableId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
transit-gateway	`arn:${Partition}:ec2:${Region}:${Account}:transit-gateway/${TransitGatewayId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)

리소스 유형	ARN	조건 키
volume	`arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AvailabilityZone (p. 1055) ec2:Encrypted (p. 1056) ec2:ParentSnapshot (p. 1056) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VolumeIops (p. 1058) ec2:VolumeSize (p. 1058) ec2:VolumeType (p. 1058)
vpc	`arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:Tenancy (p. 1058)
vpc-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint/${VpceId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VpceServiceName (p. 1058) ec2:VpceServiceOwner (p. 1058)

리소스 유형	ARN	조건 키
vpc-endpoint-service	`arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service/${VpceServiceId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057) ec2:VpceServicePrivateDnsName (p. 1058)
vpc-flow-log	`arn:${Partition}:ec2:${Region}:${Account}:vpc-flow-log/${VpcFlowLogId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:Region (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)
vpc-peering-connection	`arn:${Partition}:ec2:${Region}:${Account}:vpc-peering-connection/${VpcPeeringConnectionId}`	ec2:AccepterVpc (p. 1055) ec2:Region (p. 1057) ec2:RequesterVpc (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)

리소스 유형	ARN	조건 키
vpn-connection	`arn:${Partition}:ec2:${Region}:${Account}:vpn-connection/${VpnConnectionId}`	aws:RequestTag/${TagKey} (p. 1055) aws:TagKeys (p. 1055) ec2:AuthenticationType (p. 1055) ec2:DPDTimeoutSeconds (p. 1055) ec2:GatewayType (p. 1056) ec2:IKEVersions (p. 1056) ec2:InsideTunnelCidr (p. 1056) ec2:Phase1DHGroupNumbers (p. 1056) ec2:Phase1EncryptionAlgorithms (p. 1056) ec2:Phase1IntegrityAlgorithms (p. 1057) ec2:Phase1LifetimeSeconds (p. 1057) ec2:Phase2DHGroupNumbers (p. 1057) ec2:Phase2EncryptionAlgorithms (p. 1057) ec2:Phase2IntegrityAlgorithms (p. 1057) ec2:Phase2LifetimeSeconds (p. 1057) ec2:PresharedKeys (p. 1057) ec2:Region (p. 1057) ec2:RekeyFuzzPercentage (p. 1057) ec2:RekeyMarginTimeSeconds (p. 1057) ec2:ResourceTag/${TagKey} (p. 1057)

리소스 유형	ARN	조건 키
		ec2:RoutingType (p. 1058)
vpn-gateway	`arn:${Partition}:ec2:${Region}:${Account}:vpn-gateway/${VpnGatewayId}`	

Amazon EC2에 사용되는 조건 키

Amazon EC2는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 허용되는 태그 키 및 값 페어를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	요청에 허용되는 태그 키 목록을 기준으로 액세스를 필터링합니다.	문자열
ec2:AccepterVpc	VPC 피어링 연결에서 수락자 VPC의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:AssociatePublicIpAddress	사용자가 퍼블릭 IP 주소를 인스턴스와 연결하기를 원하는지 여부를 기준으로 액세스를 필터링	Bool
ec2:AuthenticationType	VPN 터널 엔드포인트의 인증 유형을 기준으로 액세스를 필터링합니다.	문자열
ec2:AuthorizedService	리소스를 사용할 수 있는 권한이 있는 AWS 서비스를 기준으로 액세스를 필터링합니다.	문자열
ec2:AuthorizedUser	리소스를 사용할 수 있는 권한이 있는 IAM 보안 주체를 기준으로 액세스를 필터링합니다.	문자열
ec2:AutoPlacement	전용 호스트의 자동 배치 속성을 기준으로 액세스를 필터링합니다.	문자열
ec2:AvailabilityZone	AWS 리전의 가용 영역 이름을 기준으로 액세스를 필터링합니다.	문자열
ec2:CreateAction	리소스 생성 API 작업의 이름을 기준으로 액세스를 필터링합니다.	문자열
ec2:DPDTimeoutSeconds	VPN 터널에서 DPD 시간 초과가 발생하는 기간을 기준으로 액세스를 필터링합니다.	숫자
ec2:EbsOptimized	인스턴스에 EBS 최적화가 활성화되었는지 여부를 기준으로 액세스를 필터링합니다.	Bool
ec2:ElasticGpuType	Elastic Graphics 액셀러레이터의 유형을 기준으로 액세스를 필터링합니다.	문자열

조건 키	설명	유형
ec2:Encrypted	EBS 볼륨이 암호화되었는지 여부를 기준으로 액세스를 필터링합니다.	Bool
ec2:GatewayType	VPN 연결의 AWS 측에 있는 VPN 엔드포인트의 게이트웨이 유형을 기준으로 액세스를 필터링합니다.	문자열
ec2:HostRecovery	전용 호스트에 호스트 복구가 활성화되었는지 여부를 기준으로 액세스를 필터링합니다.	문자열
ec2:IKEVersions	VPN 터널에 허용되는 IKE(Internet Key Exchange) 버전을 기준으로 액세스를 필터링합니다.	문자열
ec2:ImageType	이미지 유형(머신, aki 또는 ari)을 기준으로 액세스를 필터링합니다.	문자열
ec2:InsideTunnelCidr	VPN 터널의 내부 IP 주소 범위를 기준으로 액세스를 필터링합니다.	문자열
ec2:InstanceMarketType	인스턴스의 마켓 또는 구매 옵션(온디맨드 또는 스팟)을 기준으로 액세스를 필터링합니다.	문자열
ec2:InstanceProfile	인스턴스 프로파일의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:InstanceType	인스턴스 유형을 기준으로 액세스를 필터링합니다.	문자열
ec2:IsLaunchTemplateResource	사용자가 시작 템플릿에 지정된 리소스를 재정의할 수 있는지 여부를 기준으로 액세스를 필터링합니다.	Bool
ec2:LaunchTemplate	시작 템플릿의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:MetadataHttpEndpoint	HTTP 엔드포인트가 인스턴스 메타데이터 서비스에서 활성화되어 있는지 여부를 기준으로 액세스를 필터링합니다.	문자열
ec2:MetadataHttpPutResponseHopLimit	인스턴스 메타데이터 서비스를 호출할 때 허용되는 홉 수를 기준으로 액세스를 필터링합니다.	숫자
ec2:MetadataHttpTokens	인스턴스 메타데이터 서비스를 호출할 때 토큰이 필요한지 여부(선택 사항 또는 필수)를 기준으로 액세스를 필터링합니다.	문자열
ec2:Owner	리소스 소유자(amazon, aws-marketplace 또는 AWS 계정 ID)를 기준으로 액세스를 필터링합니다.	문자열
ec2:ParentSnapshot	상위 스냅샷의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:ParentVolume	스냅샷이 생성된 상위 볼륨의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:Permission	리소스에 대한 권한 유형(INSTANCE-ATTACH 또는 EIP-ASSOCIATE)을 기준으로 액세스를 필터링합니다.	문자열
ec2:Phase1DHGroupNumbers	1단계 IKE 협상에 대해 VPN 터널에 허용되는 Diffie-Hellman 그룹 번호를 기준으로 액세스를 필터링합니다.	숫자
ec2:Phase1EncryptionAlgorithms	1단계 IKE 협상에 대해 VPN 터널에 허용되는 암호화 알고리즘을 기준으로 액세스를 필터링합니다.	문자열

조건 키	설명	유형
ec2:Phase1IntegrityAlgorithms	1단계 IKE 협상에 대해 VPN 터널에 허용되는 무결성 알고리즘을 기준으로 액세스를 필터링합니다.	문자열
ec2:Phase1LifetimeSeconds	VPN 터널에 대한 1단계 IKE 협상의 수명(초)을 기준으로 액세스를 필터링합니다.	숫자
ec2:Phase2DHGroupNumbers	2단계 IKE 협상에 대해 VPN 터널에 허용되는 Diffie-Hellman 그룹 번호를 기준으로 액세스를 필터링합니다.	숫자
ec2:Phase2EncryptionAlgorithms	2단계 IKE 협상에 대해 VPN 터널에 허용되는 암호화 알고리즘을 기준으로 액세스를 필터링합니다.	문자열
ec2:Phase2IntegrityAlgorithms	2단계 IKE 협상에 대해 VPN 터널에 허용되는 무결성 알고리즘을 기준으로 액세스를 필터링합니다.	문자열
ec2:Phase2LifetimeSeconds	VPN 터널에 대한 2단계 IKE 협상의 수명(초)을 기준으로 액세스를 필터링합니다.	숫자
ec2:PlacementGroup	배치 그룹의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:PlacementGroupStrategy	배치 그룹에 사용되는 인스턴스 배치 전략(클러스터, 분산 또는 파티션)을 기준으로 액세스를 필터링합니다.	문자열
ec2:PresharedKeys	가상 프라이빗 게이트웨이와 고객 게이트웨이 사이의 초기 IKE 보안 연결을 설정하는 데 사용되는 사전 공유 키(PSK)를 기준으로 액세스를 필터링합니다.	문자열
ec2:ProductCode	AMI와 연결된 제품 코드를 기준으로 액세스를 필터링합니다.	문자열
ec2:Public	이미지에 퍼블릭 시작 권한이 있는지 여부를 기준으로 액세스를 필터링합니다.	Bool
ec2:Quantity	요청의 전용 호스트 수를 기준으로 액세스를 필터링합니다.	숫자
ec2:Region	AWS 리전의 이름을 기준으로 액세스를 필터링합니다.	문자열
ec2:RekeyFuzzPercentage	VPN 터널에 대해 키 재지정 시간이 임의로 선택되는 키 재지정 시간의 백분율(키 재지정 마진 시간에 의해 결정됨)을 기준으로 액세스를 필터링합니다.	숫자
ec2:RekeyMarginTimeSeconds	VPN 터널에 대해 2단계 수명이 만료되기 전 마진 시간을 기준으로 액세스를 필터링합니다.	숫자
ec2:RequesterVpc	VPC 피어링 연결에서 요청자 VPC의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:ReservedInstancesOfferingType	예약 인스턴스 상품의 결제 옵션(선결제 없음, 부분 선결제 또는 전체 선결제)을 기준으로 액세스를 필터링합니다.	문자열
ec2:ResourceTag/	리소스에 연결된 태그 키 및 값 페어의 서문 문자열을 기준으로 액세스를 필터링합니다.	문자열
ec2:ResourceTag/${TagKey}	리소스의 태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열
ec2:RoleDelivery	EC2에 대한 IAM 역할 자격 증명을 검색하기 위한 인스턴스 메타데이터 서비스의 버전을 기준으로 액세스를 필터링합니다.	숫자

조건 키	설명	유형
ec2:RootDeviceType	인스턴스의 루트 디바이스 유형(ebs 또는 인스턴스 스토어)을 기준으로 액세스를 필터링합니다.	문자열
ec2:RoutingType	VPN 연결에 대한 라우팅 유형을 기준으로 액세스를 필터링합니다.	문자열
ec2:SnapshotTime	스냅샷의 시작 시간을 기준으로 액세스를 필터링합니다.	문자열
ec2:SourceInstanceARN	요청이 시작된 인스턴스의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:Subnet	서브넷의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:Tenancy	VPC 또는 인스턴스의 테넌시(기본, 전용 또는 호스트)를 기준으로 액세스를 필터링합니다.	문자열
ec2:VolumeIops	볼륨에 대해 프로비저닝된 초당 입력/출력 작업 수(IOPS)를 기준으로 액세스를 필터링합니다.	숫자
ec2:VolumeSize	GiB 단위의 볼륨 크기를 기준으로 액세스를 필터링합니다.	숫자
ec2:VolumeType	볼륨 유형(gp2, io1, st1, sc1 또는 표준)을 기준으로 액세스를 필터링합니다.	문자열
ec2:Vpc	VPC의 ARN을 기준으로 액세스를 필터링합니다.	ARN
ec2:VpceServiceName	VPC 엔드포인트 서비스의 이름을 기준으로 액세스를 필터링합니다.	문자열
ec2:VpceServiceOwner	VPC 엔드포인트 서비스(아마존, AWS Marketplace 또는 AWS 계정 ID)의 서비스 소유자에 의한 액세스를 필터링합니다.	문자열
ec2:VpceServicePrivateDnsName	VPC 엔드포인트 서비스의 프라이빗 DNS 이름을 기준으로 액세스를 필터링합니다.	문자열

Amazon EC2 Auto Scaling에 사용되는 작업, 리소스 및 조건 키

Amazon EC2 Auto Scaling(서비스 접두사: `autoscaling`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon EC2 Auto Scaling에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AttachInstances	지정된 Auto Scaling 그룹에 하나 이상의 EC2 인스턴스를 연결합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
AttachLoadBalancerTargetGroups	지정된 Auto Scaling 그룹에 하나 이상의 대상 그룹을 연결합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
				autoscaling:TargetGroupARNs (p. 1068)	
AttachLoadBalancers	지정된 Auto Scaling 그룹에 하나 이상의 로드 밸런서를 연결합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
				autoscaling:LoadBalancerNames (p. 1068)	
BatchDeleteScheduledAction	지정된 예약된 작업을 삭제합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchPutScheduledUpdateGroupAction	Auto Scaling 그룹에 대한 여러 예약된 조정 작업을 생성하거나 업데이트합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
CompleteLifecycleAction	지정된 결과로 지정된 토큰 또는 인스턴스를 위한 수명 주기 작업을 완료합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
CreateAutoScalingGroup	지정된 이름 및 속성으로 Auto Scaling 그룹을 생성합니다.	태그 지정	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
				autoscaling:InstanceTypes (p. 1068) autoscaling:LaunchConfigurationName (p. 1068) autoscaling:LoadBalancerNames (p. 1068) autoscaling:MaxSize (p. 1068) autoscaling:MinSize (p. 1068) autoscaling:TargetGroupARNs (p. 1068) autoscaling:VPCZoneIdentifiers (p. 1068) aws:RequestTag/${TagKey} (p. 1068) aws:TagKeys (p. 1068)	
CreateLaunchConfiguration	시작 구성을 생성합니다.	쓰기	launchConfiguration* (p. 1067)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				autoscaling:ImageId (p. 1067) autoscaling:InstanceType (p. 1067) autoscaling:SpotPrice (p. 1068)	
CreateOrUpdateTags	지정된 Auto Scaling 그룹에 대한 태그를 생성하거나 업데이트합니다.	태그 지정	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
				aws:RequestTag/${TagKey} (p. 1068) aws:TagKeys (p. 1068)	
DeleteAutoScalingGroup	지정된 Auto Scaling 그룹을 삭제합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
DeleteLaunchConfiguration	지정된 시작 구성을 삭제합니다.	쓰기	launchConfiguration* (p. 1067)		
DeleteLifecycleHook	지정된 수명 주기 후크를 삭제합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
DeleteNotificationConfiguration	지정된 알림을 삭제합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeletePolicy	지정된 Auto Scaling 정책을 삭제합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
DeleteScheduledAction	지정된 예약된 작업을 삭제합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
DeleteTags	지정된 태그를 삭제합니다.	태그 지정	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
				aws:RequestTag/${TagKey} (p. 1068) aws:TagKeys (p. 1068)	
DescribeAccountLimits	AWS 계정에 대한 현재의 Auto Scaling 리소스 제한을 설명합니다.	List			
DescribeAdjustmentTypes	PutScalingPolicy에서 사용할 정책 조정유형을 설명합니다.	List			
DescribeAutoScalingGroups	하나 이상의 Auto Scaling 그룹을 설명합니다. 이름의 목록이 제공되지 않은 경우, 호출이 모든 Auto Scaling 그룹을 설명합니다.	List			
DescribeAutoScalingInstances	하나 이상의 Auto Scaling 인스턴스를 설명합니다. 목록이 제공되지 않은 경우, 호출이 모든 인스턴스를 설명합니다.	List			
DescribeAutoScalingNotificationTypes	Auto Scaling이 지원하는 알림 유형을 설명합니다.	List			
DescribeLaunchConfigurations	하나 이상의 시작 구성을 설명합니다. 이름의 목록을 생략한 경우에는 호출이 모든 시작 구성을 설명합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeLifecycleHookTypes	사용 가능한 수명 주기 후크의 유형을 설명합니다.	List			
DescribeLifecycleHooks	지정된 Auto Scaling 그룹에 대한 수명 주기 후크를 설명합니다.	List			
DescribeLoadBalancerTargetGroups	지정된 Auto Scaling 그룹에 대한 대상 그룹을 설명합니다.	List			
DescribeLoadBalancers	지정된 Auto Scaling 그룹에 대한 로드 밸런서를 설명합니다.	List			
DescribeMetricCollectionTypes	Auto Scaling에 사용할 수 있는 CloudWatch 지표를 설명합니다.	List			
DescribeNotificationConfigurations	지정된 Auto Scaling 그룹과 연결된 알림 작업을 설명합니다.	List			
DescribePolicies	지정된 Auto Scaling 그룹에 대한 정책을 설명합니다.	List			
DescribeScalingActivities	지정된 Auto Scaling 그룹에 대한 하나 이상의 조정 작업을 설명합니다.	List			
DescribeScalingProcessTypes	ResumeProcesses 및 SuspendProcesses에서 사용할 조정 프로세스 유형을 설명합니다.	List			
DescribeScheduledActions	실행하지 않은 Auto Scaling 그룹에 대해 예약된 작업을 설명합니다.	List			
DescribeTags	지정된 태그를 설명합니다.	Read			
DescribeTerminationPolicyTypes	Auto Scaling이 지원하는 종료 정책을 설명합니다.	List			
DetachInstances	지정된 Auto Scaling 그룹에서 하나 이상의 인스턴스를 삭제합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
DetachLoadBalancerTargetGroups	지정된 Auto Scaling 그룹에서 하나 이상의 대상 그룹을 분리합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
				autoscaling:TargetGroupARNs (p. 1068)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DetachLoadBalancers	지정된 Auto Scaling 그룹에서 하나 이상의 로드 밸런서를 제거합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
				autoscaling:LoadBalancerNames (p. 1068)	
DisableMetricsCollection	지정된 Auto Scaling 그룹에 대한 지정된 지표의 모니터링을 비활성화합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
EnableMetricsCollection	지정된 Auto Scaling 그룹에 대한 지정된 지표의 모니터링을 활성화합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
EnterStandby	지정된 인스턴스를 스탠바이 모드로 전환합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
ExecutePolicy	지정된 정책을 실행합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
ExitStandby	지정된 인스턴스에서 스탠바이 모드를 해제합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutLifecycleHook	지정된 Auto Scaling 그룹에 대한 수명 주기 후크를 생성하거나 업데이트합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
PutNotificationConfiguration	지정된 이벤트가 발생하면 알림을 보내도록 Auto Scaling 그룹을 구성합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
PutScalingPolicy	Auto Scaling 그룹에 대한 정책을 생성하거나 업데이트합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
PutScheduledUpdateGroupAction	Auto Scaling 그룹에 대한 예약된 조정 작업을 생성하거나 업데이트합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
				autoscaling:MaxSize (p. 1068) autoscaling:MinSize (p. 1068)	
RecordLifecycleActionHeartbeat	지정된 토큰 또는 인스턴스와 연결된 수명 주기 작업에 대한 하트비트(heartbeat)를 기록합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
ResumeProcesses	지정된 Auto Scaling 그룹에 대하여, 지정된 일시 중지된 Auto Scaling 프로세스 또는 모든 일시 중지된 프로세스를 다시 시작합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SetDesiredCapacity	지정된 Auto Scaling 그룹의 크기를 설정합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
SetInstanceHealth	지정된 인스턴스의 상태를 설정합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
SetInstanceProtection	지정된 인스턴스의 인스턴스 보호 설정을 업데이트합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
SuspendProcesses	지정된 Auto Scaling 그룹에 대하여, 지정된 Auto Scaling 프로세스 또는 모든 프로세스를 일시 중지합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
TerminateInstanceInAutoScalingGroup	지정된 인스턴스를 종료하고 원하는 그룹 크기를 선택적으로 조정합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	
UpdateAutoScalingGroup	지정된 Auto Scaling 그룹에 대한 구성을 업데이트합니다.	쓰기	autoScalingGroup* (p. 1067)	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				autoscaling:InstanceTypes (p. 1068) autoscaling:LaunchConfigurationName (p. 1068) autoscaling:MaxSize (p. 1068) autoscaling:MinSize (p. 1068) autoscaling:VPCZoneIdentifiers (p. 1068)	

Amazon EC2 Auto Scaling에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1059)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
autoScalingGroup	`arn:${Partition}:autoscaling:${Region}:${Account}:autoScalingGroup:${GroupId}:autoScalingGroupName/${GroupFriendlyName}`	autoscaling:ResourceTag/${TagKey} (p. 1068) aws:ResourceTag/${TagKey} (p. 1068)
launchConfiguration	`arn:${Partition}:autoscaling:${Region}:${Account}:launchConfiguration:${Id}:launchConfigurationName/${LaunchConfigurationName}`	

Amazon EC2 Auto Scaling에 사용되는 조건 키

Amazon EC2 Auto Scaling은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
autoscaling:ImageId	인스턴스를 생성하는 데 사용되는 AMI.	문자열
autoscaling:InstanceType	사용 가능한 하드웨어 리소스의 측면에서 인스턴스 유형.	문자열

조건 키	설명	유형
autoscaling:InstanceTypes	사용 가능한 하드웨어 리소스의 측면에서 인스턴스 유형.	문자열
autoscaling:LaunchConfigurationName	시작 구성의 이름.	문자열
autoscaling:LaunchTemplateVersionSpecified	사용자가 시작 템플릿의 모든 버전을 지정할 수 있는지 또는 최신 버전이나 기본 버전만 지정할 수 있는지 여부를 기준으로 액세스를 필터링합니다.	Bool
autoscaling:LoadBalancerNames	로드 밸런서의 이름입니다.	문자열
autoscaling:MaxSize	최대 조정 크기.	숫자
autoscaling:MinSize	최소 조정 크기.	숫자
autoscaling:ResourceTag/${TagKey}	리소스에 연결된 태그의 값.	문자열
autoscaling:SpotPrice	인스턴스와 연결된 스팟 가격.	숫자
autoscaling:TargetGroupARNs	대상 그룹의 ARN.	ARN
autoscaling:VPCZoneIdentifiers	VPC 영역의 식별자.	문자열
aws:RequestTag/${TagKey}	요청과 연결된 태그의 값.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열

Amazon EC2 Image Builder에 사용되는 작업, 리소스 및 조건 키

Amazon EC2 Image Builder(서비스 접두사: `imagebuilder`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon EC2 Image Builder에서 정의한 작업 (p. 1069)

- Amazon EC2 Image Builder에서 정의한 리소스 유형 (p. 1073)
- Amazon EC2 Image Builder의 조건 키 (p. 1074)

Amazon EC2 Image Builder에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelImageCreation	이미지 생성을 취소합니다.	쓰기	image* (p. 1074)		
CreateComponent	새 구성 요소를 생성합니다.	쓰기	component* (p. 1073)		
			kmsKey (p. 1074)		
				aws:RequestTag/${TagKey} (p. 1074) aws:TagKeys (p. 1074)	
CreateDistributionConfiguration	새 배포 구성을 생성합니다.	쓰기	distributionConfiguration* (p. 1073)		
				aws:RequestTag/${TagKey} (p. 1074) aws:TagKeys (p. 1074)	
CreateImage	새 이미지를 생성합니다.	쓰기	image* (p. 1074)		imagebuilder:GetImageRe imagebuilder:GetInfrastru
				aws:RequestTag/${TagKey} (p. 1074) aws:TagKeys (p. 1074)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateImagePipeline	새 이미지 파이프라인을 생성합니다.	쓰기	imagePipeline* (p. 1074)		imagebuilder:GetImageRe
				aws:RequestTag/${TagKey} (p. 1074) aws:TagKeys (p. 1074)	
CreateImageRecipe	새 이미지 레시피를 생성합니다.	쓰기	imageRecipe* (p. 1074)		imagebuilder:GetCompon
				aws:RequestTag/${TagKey} (p. 1074) aws:TagKeys (p. 1074)	
CreateInfrastructureConfiguration	새 인프라 구성을 생성합니다.	쓰기	infrastructureConfiguration* (p. 1074)		iam:PassRole
				aws:RequestTag/${TagKey} (p. 1074) aws:TagKeys (p. 1074)	
DeleteComponent	구성 요소를 삭제합니다.	쓰기	component* (p. 1073)		
DeleteDistributionConfiguration	배포 구성을 삭제합니다.	쓰기	distributionConfiguration* (p. 1073)		
DeleteImage	이미지 삭제	쓰기	image* (p. 1074)		
DeleteImagePipeline	이미지 파이프라인을 삭제합니다.	쓰기	imagePipeline* (p. 1074)		
DeleteImageRecipe	이미지 레시피를 삭제할 수 있는 권한을 부여합니다.	쓰기	imageRecipe* (p. 1074)		
DeleteInfrastructureConfiguration	인프라 구성을 삭제합니다.	쓰기	infrastructureConfiguration* (p. 1074)		
GetComponent	구성 요소에 대한 세부 정보를 봅니다.	Read	component* (p. 1073)		
GetComponentPolicy	구성 요소와 연결된 리소스 정책을 봅니다.	권한 관리	component* (p. 1073)		
GetDistributionConfiguration	배포 구성에 대한 세부 정보를 봅니다.	Read	distributionConfiguration* (p. 1073)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetImage	이미지에 대한 세부 정보를 봅니다.	Read	image* (p. 1074)		
				aws:ResourceTag/${TagKey} (p. 1074)	
GetImagePipeline	이미지 파이프라인에 대한 세부 정보를 봅니다.	Read	imagePipeline* (p. 1074)		
GetImagePolicy	이미지와 연결된 리소스 정책을 봅니다.	권한 관리	image* (p. 1074)		
GetImageRecipe	이미지 레시피에 대한 세부 정보를 봅니다.	Read	imageRecipe* (p. 1074)		
GetImageRecipePolicy	이미지 레시피에 연결된 리소스 정책을 봅니다.	권한 관리	imageRecipe* (p. 1074)		
GetInfrastructureConfiguration	인프라 구성에 대한 세부 정보를 봅니다.	Read	infrastructureConfiguration* (p. 1074)		
ListComponentBuildVersions	계정의 구성 요소 빌드 버전을 나열합니다.	List	componentVersion* (p. 1073)		
ListComponents	계정에서 소유하거나 계정과 공유하는 구성 요소 버전을 나열합니다.	List			
ListDistributionConfigurations	계정의 배포 구성을 나열합니다.	List			
ListImageBuildVersions	계정의 이미지 빌드 버전을 나열합니다.	List	imageVersion* (p. 1074)		
ListImagePipelines	계정의 이미지 파이프라인을 나열합니다.	List			
ListImageRecipes	계정에서 소유하거나 계정과 공유하는 이미지 레시피를 나열합니다.	List			
ListImages	계정에서 소유하거나 계정과 공유하는 이미지 버전을 나열합니다.	List			
ListInfrastructureConfigurations	계정의 인프라 구성을 나열합니다.	List			
ListTagsForResource	Image Builder 리소스에 대한 태그를 나열합니다.	Read	component (p. 1073)		
			distributionConfiguration (p. 1073)		
			image (p. 1074)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			imagePipeline (p. 1074)		
			imageRecipe (p. 1074)		
			infrastructureConfiguration (p. 1074)		
				aws:ResourceTag/${TagKey} (p. 1074)	
PutComponentPolicy	구성 요소와 연결된 리소스 정책을 설정합니다.	권한 관리	component* (p. 1073)		
PutImagePolicy	이미지와 연결된 리소스 정책을 설정합니다.	권한 관리	image* (p. 1074)		
PutImageRecipePolicy	이미지 레시피와 연결된 리소스 정책을 설정합니다.	권한 관리	imageRecipe* (p. 1074)		
StartImagePipelineExecution	파이프라인에서 새 이미지를 생성합니다.	쓰기	imagePipeline* (p. 1074)		imagebuilder:GetImagePi
TagResource	Image Builder 리소스에 태그를 지정합니다.	태그 지정	component (p. 1073)		
			distributionConfiguration (p. 1073)		
			image (p. 1074)		
			imagePipeline (p. 1074)		
			imageRecipe (p. 1074)		
			infrastructureConfiguration (p. 1074)		
				aws:TagKeys (p. 1074) aws:RequestTag/${TagKey} (p. 1074) aws:ResourceTag/${TagKey} (p. 1074)	
UntagResource	Image Builder 리소스에 대한 태그를 해제합니다.	태그 지정	component (p. 1073)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			distributionConfiguration (p. 1073)		
			image (p. 1074)		
			imagePipeline (p. 1074)		
			imageRecipe (p. 1074)		
			infrastructureConfiguration (p. 1074)		
				aws:ResourceTag/${TagKey} (p. 1074) aws:TagKeys (p. 1074)	
UpdateDistributionConfiguration	기존 배포 구성을 업데이트합니다.	쓰기	distributionConfiguration* (p. 1073)		
UpdateImagePipelines	기존 이미지 파이프라인을 업데이트합니다.	쓰기	imagePipeline* (p. 1074)		
UpdateInfrastructureConfiguration	기존 인프라 구성을 업데이트합니다.	쓰기	infrastructureConfiguration* (p. 1074)	iam:PassRole	
				aws:ResourceTag/${TagKey} (p. 1074)	

Amazon EC2 Image Builder에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1069)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
component	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}`	aws:ResourceTag/${TagKey} (p. 1074)
componentVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}`	aws:ResourceTag/${TagKey} (p. 1074)
distributionConfiguration	`arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}`	aws:ResourceTag/${TagKey} (p. 1074)

리소스 유형	ARN	조건 키
image	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}`	aws:ResourceTag/${TagKey} (p. 1074)
imageVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}`	aws:ResourceTag/${TagKey} (p. 1074)
imageRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}`	aws:ResourceTag/${TagKey} (p. 1074)
imagePipeline	`arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}`	aws:ResourceTag/${TagKey} (p. 1074)
infrastructureConfiguration	`arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1074)
kmsKey	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	

Amazon EC2 Image Builder의 조건 키

Amazon EC2 Image Builder는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon EC2 Instance Connect에 사용되는 작업, 리소스 및 조건 키

Amazon EC2 Instance Connect(서비스 접두사: `ec2-instance-connect`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon EC2 Instance Connect에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SendSSHPublicKey	60초 동안 남아 있는 인스턴스 메타데이터에 SSH 퍼블릭 키를 푸시할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1075)		
				ec2:osuser (p. 1076)	

Amazon EC2 Instance Connect에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1075)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	

Amazon EC2 Instance Connect에 사용되는 조건 키

Amazon EC2 Instance Connect는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
ec2:osuser	인스턴스를 시작하는 데 사용한 AMI의 기본 사용자 이름을 지정하여 액세스 필터링	문자열

AWS Elastic Beanstalk에 사용되는 작업 리소스 및 조건 키

AWS Elastic Beanstalk(서비스 접두사: `elasticbeanstalk`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS Elastic Beanstalk에서 정의한 작업 (p. 1076)
- AWS Elastic Beanstalk에서 정의한 리소스 유형 (p. 1082)
- AWS Elastic Beanstalk에 사용되는 조건 키 (p. 1083)

AWS Elastic Beanstalk에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AbortEnvironmentUpdate	진행 중인 환경 구성 업데이트 또는 애플리케이션 버전 배포를 취소할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
AddTags	Elastic Beanstalk 리소스에 태그를 추가하고 태그 값을 업데이트할 수 있는 권한을 부여합니다.	태그 지정	application (p. 1082)		
			applicationversion (p. 1082)		
			configurationtemplate (p. 1083)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			environment (p. 1083)		
			platform (p. 1083)		
				aws:RequestTag/${TagKey} (p. 1083) aws:TagKeys (p. 1083)	
ApplyEnvironmentManagedAction	예약된 관리형 작업을 즉시 적용할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
CheckDNSAvailability	CNAME 가용성을 확인할 수 있는 권한을 부여합니다.	Read			
ComposeEnvironments	각각 단일 애플리케이션의 개별 구성요소를 실행하는 환경의 그룹을 생성 또는 업데이트할 수 있는 권한을 부여합니다.	쓰기	application* (p. 1082)		
			applicationversion* (p. 1082)	elasticbeanstalk:InApplication (p. 1084)	
CreateApplication	새 애플리케이션을 생성할 수 있는 권한을 부여합니다.	쓰기	application* (p. 1082)		
				aws:RequestTag/${TagKey} (p. 1083) aws:TagKeys (p. 1083)	
CreateApplicationVersion	애플리케이션의 애플리케이션 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	application* (p. 1082)		
			applicationversion* (p. 1082)	elasticbeanstalk:InApplication (p. 1084)	
				aws:RequestTag/${TagKey} (p. 1083) aws:TagKeys (p. 1083)	
CreateConfigurationTemplate	구성 템플릿을 생성할 수 있는 권한을 부여합니다.	쓰기	configurationtemplate* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				elasticbeanstalk:FromApplication (p. 1083) elasticbeanstalk:FromApplicationVersio (p. 1083) elasticbeanstalk:FromConfigurationTem (p. 1083) elasticbeanstalk:FromEnvironment (p. 1083) elasticbeanstalk:FromSolutionStack (p. 1084) elasticbeanstalk:FromPlatform (p. 1084) aws:RequestTag/ ${TagKey} (p. 1083) aws:TagKeys (p. 1083)	
CreateEnvironment	애플리케이션의 환경을 시작할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
				elasticbeanstalk:FromApplicationVersio (p. 1083) elasticbeanstalk:FromConfigurationTem (p. 1083) elasticbeanstalk:FromSolutionStack (p. 1084) elasticbeanstalk:FromPlatform (p. 1084) aws:RequestTag/ ${TagKey} (p. 1083) aws:TagKeys (p. 1083)	
CreatePlatformVersion	사용자 지정 플랫폼의 새 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	platform* (p. 1083)		
				aws:RequestTag/ ${TagKey} (p. 1083) aws:TagKeys (p. 1083)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateStorageLocation	계정의 Amazon S3 스토리지 위치를 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteApplication	애플리케이션을 모든 연결된 버전 및 구성과 함께 삭제할 수 있는 권한을 부여합니다.	쓰기	application* (p. 1082)		
DeleteApplicationVersion	애플리케이션에서 애플리케이션 버전을 삭제할 수 있는 권한을 부여합니다.	쓰기	applicationversion* (p. 1082)	elasticbeanstalk:InApplication (p. 1084)	
DeleteConfigurationTemplate	구성 템플릿을 삭제할 수 있는 권한을 부여합니다.	쓰기	configurationtemplate* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
DeleteEnvironmentConfiguration	실행 환경과 연결된 초안 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
DeletePlatformVersion	사용자 지정 플랫폼의 버전을 삭제할 수 있는 권한을 부여합니다.	쓰기	platform* (p. 1083)		
DescribeAccountAttributes	리소스 할당량 등 계정 속성의 목록을 검색할 수 있는 권한을 부여합니다.	Read			
DescribeApplicationVersions	AWS Elastic Beanstalk 스토리지 버킷에 저장된 애플리케이션 버전의 목록을 검색할 수 있는 권한을 부여합니다.	List	applicationversion* (p. 1082)	elasticbeanstalk:InApplication (p. 1084)	
DescribeApplications	기존 애플리케이션에 대한 설명을 검색할 수 있는 권한을 부여합니다.	List	application (p. 1082)		
DescribeConfigurationOptions	환경 구성 옵션에 대한 설명을 검색할 수 있는 권한을 부여합니다.	Read	configurationtemplate (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
			environment (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
			solutionstack (p. 1083)		
DescribeConfigurationSettings	구성 세트의 설정에 대한 설명을 검색할 수 있는 권한을 부여합니다.	Read	configurationtemplate (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
			environment (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
DescribeEnvironmentHealth	환경의 전반적 상태에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	environment (p. 1083)		
DescribeEnvironmentManagedActionHistory	환경의 완료 및 실패한 관리형 작업의 목록을 검색할 수 있는 권한을 부여합니다.	Read	environment (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeEnvironmentManagedActions	환경의 예정 및 진행 중 관리형 작업의 목록을 검색할 수 있는 권한을 부여합니다.	Read	environment (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
DescribeEnvironmentResources	환경을 위한 AWS 리소스의 목록을 검색할 수 있는 권한을 부여합니다.	Read	environment (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
DescribeEnvironments	기존 환경에 대한 설명을 검색할 수 있는 권한을 부여합니다.	List	environment (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
DescribeEvents	일련의 기준과 일치하는 이벤트 설명의 목록을 검색할 수 있는 권한을 부여합니다.	Read	application (p. 1082)		
			applicationversion (p. 1082)	elasticbeanstalk:InApplication (p. 1084)	
			configurationtemplate (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
			environment (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
DescribeInstancesHealth	환경 인스턴스의 상태에 대한 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read	environment (p. 1083)		
DescribePlatformVersion	플랫폼 버전에 대한 설명을 검색할 수 있는 권한을 부여합니다.	Read	platform (p. 1083)		
ListAvailableSolutionStacks	사용 가능한 솔루션 스택 이름의 목록을 검색할 수 있는 권한을 부여합니다.	List	solutionstack (p. 1083)		
ListPlatformVersions	사용 가능한 플랫폼의 목록을 검색할 수 있는 권한을 부여합니다.	List	platform (p. 1083)		
ListTagsForResource	Elastic Beanstalk 리소스의 태그 목록을 검색할 수 있는 권한을 부여합니다.	Read	application (p. 1082)		
			applicationversion (p. 1082)		
			configurationtemplate (p. 1083)		
			environment (p. 1083)		
			platform (p. 1083)		
RebuildEnvironment	환경의 모든 AWS 리소스를 삭제 및 재생성하고 강제로 다시 시작할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RemoveTags	Elastic Beanstalk 리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	application (p. 1082)		
			applicationversion (p. 1082)		
			configurationtemplate (p. 1083)		
			environment (p. 1083)		
			platform (p. 1083)		
				aws:TagKeys (p. 1083)	
RequestEnvironmentInfo	배포된 환경에 대한 정보를 컴파일하는 요청을 시작할 수 있는 권한을 부여합니다.	Read	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
RestartAppServer	환경이 각 Amazon EC2 인스턴스에서 실행 중인 애플리케이션 컨테이너 서버를 다시 시작하도록 요청할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
RetrieveEnvironmentInfo	RequestEnvironmentInfo 요청에서 컴파일된 정보를 가져올 수 있는 권한을 부여합니다.	Read	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
SwapEnvironmentCNAMEs	두 환경의 CNAME를 스왑할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
				elasticbeanstalk:FromEnvironment (p. 1083)	
TerminateEnvironment	환경을 종료할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
UpdateApplication	지정된 속성으로 애플리케이션을 업데이트할 수 있는 권한을 부여합니다.	쓰기	application* (p. 1082)		
UpdateApplicationResourceLifecycle	애플리케이션과 연결된 애플리케이션 버전 수명 주기 정책을 업데이트할 수 있는 권한을 부여합니다.	쓰기	application* (p. 1082)		
UpdateApplicationVersion	애플리케이션 속성으로 애플리케이션 버전을 업데이트할 수 있는 권한을 부여합니다.	쓰기	applicationversion* (p. 1082)	elasticbeanstalk:InApplication (p. 1084)	
UpdateConfigurationTemplate	지정된 속성 도는 구성 옵션 값으로 구성 템플릿을 업데이트할 수 있는 권한을 부여합니다.	쓰기	configurationtemplate* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				elasticbeanstalk:FromApplication (p. 1083) elasticbeanstalk:FromApplicationVersio (p. 1083) elasticbeanstalk:FromConfigurationTem (p. 1083) elasticbeanstalk:FromEnvironment (p. 1083) elasticbeanstalk:FromSolutionStack (p. 1084) elasticbeanstalk:FromPlatform (p. 1084)	
UpdateEnvironment	환경을 업데이트할 수 있는 권한을 부여합니다.	쓰기	environment* (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
				elasticbeanstalk:FromApplicationVersio (p. 1083) elasticbeanstalk:FromConfigurationTem (p. 1083) elasticbeanstalk:FromSolutionStack (p. 1084) elasticbeanstalk:FromPlatform (p. 1084)	
ValidateConfigurationSettings	구성 템플릿 또는 환경에 대한 구성 설정 세트의 유효성을 확인할 수 있는 권한을 부여합니다.	Read	configurationtemplate (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	
			environment (p. 1083)	elasticbeanstalk:InApplication (p. 1084)	

AWS Elastic Beanstalk에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1076)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
application	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey} (p. 1083)
applicationversion	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:applicationversion/${ApplicationName}/${VersionLabel}`	aws:ResourceTag/${TagKey} (p. 1083)

리소스 유형	ARN	조건 키
		elasticbeanstalk:InApplication (p. 1084)
configurationtemplate	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:configurationtemplate/${ApplicationName}/${TemplateName}`	aws:ResourceTag/${TagKey} (p. 1083) elasticbeanstalk:InApplication (p. 1084)
environment	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:environment/${ApplicationName}/${EnvironmentName}`	aws:ResourceTag/${TagKey} (p. 1083) elasticbeanstalk:InApplication (p. 1084)
solutionstack	`arn:${Partition}:elasticbeanstalk:${Region}::solutionstack/${SolutionStackName}`	
platform	`arn:${Partition}:elasticbeanstalk:${Region}::platform/${PlatformNameWithVersion}`	

AWS Elastic Beanstalk에 사용되는 조건 키

AWS Elastic Beanstalk는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
elasticbeanstalk:FromApplication	애플리케이션을 종속성 또는 입력 파라미터 제약 조건으로 사용하여 액세스를 필터링합니다.	ARN
elasticbeanstalk:FromApplicationVersion	애플리케이션 버전을 종속성 또는 입력 파라미터 제약 조건으로 사용하여 액세스를 필터링합니다.	ARN
elasticbeanstalk:FromConfigurationTemplate	구성 템플릿을 종속성 또는 입력 파라미터 제약 조건으로 사용하여 액세스를 필터링합니다.	ARN
elasticbeanstalk:FromEnvironment	환경을 종속성 또는 입력 파라미터 제약 조건으로 사용하여 액세스를 필터링합니다.	ARN

조건 키	설명	유형
elasticbeanstalk:FromPlatform	플랫폼을 종속성 또는 입력 파라미터 제약 조건으로 사용하여 액세스를 필터링합니다.	ARN
elasticbeanstalk:FromSolutionStack	솔루션 스택을 종속성 또는 입력 파라미터 제약 조건으로 사용하여 액세스를 필터링합니다.	ARN
elasticbeanstalk:InApplication	작업이 작동하는 리소스가 포함된 애플리케이션을 기준으로 액세스를 필터링합니다.	ARN

Amazon Elastic Block Store에 사용되는 작업, 리소스 및 조건 키

Amazon Elastic Block Store(서비스 접두사: `ebs`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Elastic Block Store에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetSnapshotBlock	Amazon Elastic Block Store(EBS) 스냅샷에서 블록의 데이터를 반환할 수 있는 권한을 부여합니다.	Read	snapshot* (p. 1085)		
ListChangedBlocks	동일한 볼륨/스냅샷 계보에 대한 두 Amazon Elastic Block Store(EBS) 스냅샷 간에 서로 다른 블록에 대한 블록 인덱스 및 블	Read	snapshot* (p. 1085)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	록 토큰을 나열할 수 있는 권한을 부여합니다.				
ListSnapshotBlocks	Amazon Elastic Block Store(EBS) 스냅샷의 블록에 대한 블록 인덱스 및 블록 토큰을 나열할 권한을 부여합니다.	Read	snapshot* (p. 1085)		

Amazon Elastic Block Store에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1084)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:ResourceTag/${TagKey} (p. 1085)

Amazon Elastic Block Store의 조건 키

Amazon Elastic Block Store는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:ResourceTag/${TagKey}	AWS 리소스에 할당된 태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열

Amazon Elastic Container Registry에 사용되는 작업, 리소스 및 조건 키

Amazon Elastic Container Registry(서비스 접두사: `ecr`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Elastic Container Registry에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchCheckLayerAvailability	지정된 레지스트리 및 리포지토리에서 하나 이상 이미지 계층의 가용성을 확인할 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
BatchDeleteImage	지정된 리포지토리 내의 지정된 이미지 목록을 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
BatchGetImage	지정된 리포지토리 내의 지정된 이미지에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
CompleteLayerUpload	지정된 레지스트리, 리포지토리 이름 및 업로드 ID에 대한 이미지 계층 업로드가 완료되었음을 Amazon ECR에 알릴 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
CreateRepository	이미지 리포지토리를 생성할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
				aws:RequestTag/${TagKey} (p. 1089) aws:TagKeys (p. 1089)	
DeleteLifecyclePolicy	지정된 수명 주기 정책을 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
DeleteRepository	기존 이미지 리포지토리를 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteRepositoryPolicy	지정된 리포지토리에서 리포지토리 정책을 삭제할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
DescribeImageScanFindings	지정된 이미지에 대한 이미지 스캔 결과를 설명할 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
DescribeImages	이미지 크기, 이미지 태그, 생성 날짜를 포함하여 리포지토리의 이미지에 대한 메타데이터를 가져올 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
DescribeRepositories	레지스트리의 이미지 리포지토리를 설명할 수 있는 권한을 부여합니다.	List	repository (p. 1088)		
GetAuthorizationToken	12시간 동안 지정된 레지스트리에 유효한 토큰을 검색할 수 있는 권한을 부여합니다.	Read			
GetDownloadUrlForLayer	이미지 계층에 해당하는 다운로드 URL을 검색할 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
GetLifecyclePolicy	지정된 수명 주기 정책을 검색할 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
GetLifecyclePolicyPreview	지정된 수명 주기 정책 미리 보기 요청의 결과를 검색할 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
GetRepositoryPolicy	지정된 리포지토리에 대한 리포지토리 정책을 검색할 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
InitiateLayerUpload	이미지 계층을 업로드할 예정임을 Amazon ECR에 알릴 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
ListImages	지정된 리포지토리에 대한 모든 이미지 ID를 나열할 수 있는 권한을 부여합니다.	List	repository* (p. 1088)		
ListTagsForResource	Amazon ECR 리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	repository* (p. 1088)		
PutImage	이미지와 관련된 이미지 매니페스트를 생성하거나 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
PutImageScanningConfiguration	리포지토리에 대한 이미지 스캔 구성을 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutImageTagMutability	리포지토리에 대한 이미지 태그 변경 가능성 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
PutLifecyclePolicy	수명 주기 정책을 생성하거나 업데이트할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
SetRepositoryPolicy	지정된 리포지토리에 리포지토리 정책을 적용하여 액세스 권한을 제어할 수 있는 권한을 부여합니다.	권한 관리	repository* (p. 1088)		
StartImageScan	이미지 스캔을 시작할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
StartLifecyclePolicyPreview	지정된 수명 주기 정책의 미리 보기를 시작할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		
TagResource	Amazon ECR 리소스에 태그를 지정할 수 있는 권한을 부여합니다.	태그 지정	repository* (p. 1088)		
				aws:RequestTag/${TagKey} (p. 1089) aws:TagKeys (p. 1089)	
UntagResource	Amazon ECR 리소스의 태그를 해제할 수 있는 권한을 부여합니다.	태그 지정	repository* (p. 1088)		
UploadLayerPart	Amazon ECR에 이미지 계층 부분을 업로드할 수 있는 권한을 부여합니다.	쓰기	repository* (p. 1088)		

Amazon Elastic Container Registry에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1086)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
repository	`arn:${Partition}:ecr:${Region}:${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} (p. 1089) ecr:ResourceTag/${TagKey} (p. 1089)

Amazon Elastic Container Registry에 사용되는 조건 키

Amazon Elastic Container Registry는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열
ecr:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열

Amazon Elastic Container Service에 사용되는 작업, 리소스 및 조건 키

Amazon Elastic Container Service(서비스 접두사: `ecs`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Elastic Container Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCluster	새 Amazon ECS 클러스터를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1097) aws:TagKeys (p. 1097)	
CreateService	지정된 작업 정의에서 원하는 수의 작업을 실행하고 유지합니다.	쓰기	service* (p. 1096)		
				ecs:cluster (p. 1097) ecs:task-definition (p. 1097) aws:RequestTag/${TagKey} (p. 1097) aws:TagKeys (p. 1097)	
CreateTaskSet	새 Amazon ECS 작업 집합을 생성합니다.	쓰기		ecs:cluster (p. 1097) ecs:service (p. 1097) ecs:task-definition (p. 1097)	
DeleteAccountSetting	계정의 지정된 IAM 사용자, IAM 역할 또는 루트 사용자에 대해 리소스의 ARN 및 리소스 ID 형식을 수정합니다. 새 ARN 및 리소스 ID 형식이 새로 생성되는 리소스에서 비활성화되는지 여부를 지정할 수 있습니다.	쓰기			
DeleteAttributes	Amazon ECS 리소스에서 하나 이상의 사용자 지정 속성을 삭제합니다.	쓰기	container-instance* (p. 1096)		
				ecs:cluster (p. 1097)	
DeleteCluster	지정된 클러스터를 삭제합니다.	쓰기	cluster* (p. 1096)		
DeleteService	클러스터 내에서 지정된 서비스를 삭제합니다.	쓰기	service* (p. 1096)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				ecs:cluster (p. 1097)	
DeleteTaskSet	지정된 작업 집합을 삭제합니다.	쓰기	task-set* (p. 1096)		
				ecs:cluster (p. 1097) ecs:service (p. 1097)	
DeregisterContainerInstance	지정된 클러스터에서 Amazon ECS 컨테이너 인스턴스를 등록 취소합니다.	쓰기	cluster* (p. 1096)		
DeregisterTaskDefinition	패밀리 및 개정에 의한 지정된 작업 정의를 등록 취소합니다.	쓰기			
DescribeClusters	클러스터를 하나 이상 설명합니다.	Read	cluster* (p. 1096)		
DescribeContainerInstances	Amazon ECS 컨테이너 인스턴스를 설명합니다.	Read	container-instance* (p. 1096)		
				ecs:cluster (p. 1097)	
DescribeServices	클러스터에서 실행 중인 지정된 서비스를 설명합니다.	Read	service* (p. 1096)		
				ecs:cluster (p. 1097)	
DescribeTaskDefinition	작업 정의를 설명합니다. 패밀리 및 개정을 지정하여 특정 작업 정의에 대한 정보를 찾을 수 있습니다. 또는 간단하게 패밀리만 지정하여 해당 패밀리에서 최신 ACTIVE 개정을 찾을 수도 있습니다.	Read			
DescribeTaskSets	Amazon ECS 작업 집합을 설명합니다.	Read	task-set* (p. 1096)		
				ecs:cluster (p. 1097) ecs:service (p. 1097)	
DescribeTasks	지정된 태그를 설명합니다.	Read	task* (p. 1096)		
				ecs:cluster (p. 1097)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DiscoverPollEndpoint	업데이트를 위해 폴링할 Amazon ECS 에이전트의 엔드포인트를 반환합니다.	쓰기			
ListAccountSettings	지정된 보안 주체에 대한 Amazon ECS 리소스의 계정 설정을 나열합니다.	List			
ListAttributes	지정된 대상 유형 및 클러스터 내의 Amazon ECS 리소스에 대한 속성을 나열합니다.	List	cluster* (p. 1096)		
ListClusters	기존 클러스터의 목록을 반환합니다.	List			
ListContainerInstances	지정된 클러스터의 컨테이너 인스턴스 목록을 반환합니다.	List	cluster* (p. 1096)		
ListServices	지정된 클러스터에서 실행 중인 서비스를 나열합니다.	List		ecs:cluster (p. 1097)	
ListTagsForResource	지정된 리소스의 태그를 나열합니다.	List	cluster (p. 1096)		
			container-instance (p. 1096)		
			task (p. 1096)		
			task-definition (p. 1096)		
ListTaskDefinitionFamilies	계정에 등록된 작업 정의 패밀리의 목록을 반환합니다(더 이상 어떤 ACTIVE 작업 정의도 없는 작업 정의 패밀리를 포함할 수 있음).	List			
ListTaskDefinitions	계정에 등록된 작업 정의 목록을 반환합니다.	List			
ListTasks	지정된 클러스터에 대한 작업 목록을 반환합니다.	List	container-instance* (p. 1096)		
				ecs:cluster (p. 1097)	
Poll [권한만 해당]	Amazon ECS 서비스와 연결하여 상태를 보고하고 명령을 가져올 수 있는 권한을 에이전트에 부여합니다.	쓰기	container-instance* (p. 1096)		
				ecs:cluster (p. 1097)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutAccountSetting	계정의 지정된 IAM 사용자, IAM 역할 또는 루트 사용자에 대해 리소스의 ARN 및 리소스 ID 형식을 수정합니다. 새 ARN 및 리소스 ID 형식이 새로 생성되는 리소스에서 활성화되는지 여부를 지정할 수 있습니다. 리소스 태그 지정과 같은 새로운 Amazon ECS 기능을 사용하려면 이 설정을 활성화해야 합니다.	쓰기			
PutAccountSettingDefault	개별 계정 설정이 없는 계정의 모든 IAM 사용자에 대해 리소스 유형의 ARN 및 리소스 ID 형식을 수정합니다. 리소스 태그 지정과 같은 새로운 Amazon ECS 기능을 사용하려면 이 설정을 활성화해야 합니다.	쓰기			
PutAttributes	Amazon ECS 리소스에 대한 속성을 생성하거나 업데이트합니다.	쓰기	container-instance* (p. 1096)		
				ecs:cluster (p. 1097)	
RegisterContainerInstance	EC2 인스턴스를 지정된 클러스터에 등록합니다.	쓰기	cluster* (p. 1096)		
				aws:RequestTag/${TagKey} (p. 1097) aws:TagKeys (p. 1097)	
RegisterTaskDefinition	제공된 패밀리 및 containerDefinitions로부터 새 작업 정의를 등록합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1097) aws:TagKeys (p. 1097)	
RunTask	임의의 배치 및 기본 Amazon ECS 스케줄러를 사용하여 작업을 시작합니다.	쓰기	task-definition* (p. 1096)		
				ecs:cluster (p. 1097) aws:RequestTag/${TagKey} (p. 1097) aws:TagKeys (p. 1097)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartTask	지정된 컨테이너 인스턴스에서 지정된 작업 정의로부터 새 작업을 시작합니다.	쓰기	task-definition* (p. 1096)		
				ecs:cluster (p. 1097) ecs:container-instances (p. 1097) aws:RequestTag/${TagKey} (p. 1097) aws:TagKeys (p. 1097)	
StartTelemetrySession	원격 측정 세션을 시작할 수 있는 권한을 부여합니다.	쓰기	container-instance* (p. 1096)		
				ecs:cluster (p. 1097)	
StopTask	작업 실행을 중지합니다.	쓰기	task* (p. 1096)		
				ecs:cluster (p. 1097)	
SubmitAttachmentStateChanges	연결 상태가 변경되었음을 확인하기 위해 전송됩니다.	쓰기	cluster* (p. 1096)		
SubmitContainerStateChange	컨테이너가 상태를 변경했음을 승인하기 위해 전송됨.	쓰기	cluster* (p. 1096)		
SubmitTaskStateChange	작업이 상태를 변경했음을 승인하기 위해 전송됨.	쓰기	cluster* (p. 1096)		
TagResource	지정된 리소스에 태그를 지정합니다.	태그 지정	cluster (p. 1096)		
			container-instance (p. 1096)		
			service (p. 1096)		
			task (p. 1096)		
			task-definition (p. 1096)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1097) aws:RequestTag/${TagKey} (p. 1097)	
UntagResource	지정된 리소스에서 태그를 제거합니다.	태그 지정	cluster (p. 1096)		
			container-instance (p. 1096)		
			service (p. 1096)		
			task (p. 1096)		
			task-definition (p. 1096)		
				aws:TagKeys (p. 1097)	
UpdateContainerAgent	지정된 컨테이너 인스턴스에서 Amazon ECS 컨테이너 에이전트를 업데이트합니다.	쓰기	container-instance* (p. 1096)		
				ecs:cluster (p. 1097)	
UpdateContainerInstancesState	사용자가 Amazon ECS 컨테이너 인스턴스의 상태를 수정할 수 있습니다.	쓰기	container-instance* (p. 1096)		
				ecs:cluster (p. 1097)	
UpdateService	서비스에 사용되는 원하는 개수, 배포 구성 또는 작업 정의를 수정합니다.	쓰기	service* (p. 1096)		
				ecs:cluster (p. 1097) ecs:task-definition (p. 1097)	
UpdateServicePrimaryTaskSet	서비스에 사용된 기본 작업 집합을 수정합니다.	쓰기	service* (p. 1096)		
				ecs:cluster (p. 1097)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateTaskSet	지정된 작업 집합을 업데이트합니다.	쓰기	task-set* (p. 1096)		
				ecs:cluster (p. 1097) ecs:service (p. 1097)	

Amazon Elastic Container Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1089)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
cluster	`arn:${Partition}:ecs:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey} (p. 1097) ecs:ResourceTag/${TagKey} (p. 1097)
container-instance	`arn:${Partition}:ecs:${Region}:${Account}:container-instance/${ContainerInstanceId}`	aws:ResourceTag/${TagKey} (p. 1097) ecs:ResourceTag/${TagKey} (p. 1097)
service	`arn:${Partition}:ecs:${Region}:${Account}:service/${ServiceName}`	aws:ResourceTag/${TagKey} (p. 1097) ecs:ResourceTag/${TagKey} (p. 1097)
task	`arn:${Partition}:ecs:${Region}:${Account}:task/${TaskId}`	aws:ResourceTag/${TagKey} (p. 1097) ecs:ResourceTag/${TagKey} (p. 1097)
task-definition	`arn:${Partition}:ecs:${Region}:${Account}:task-definition/${TaskDefinitionFamilyName}:${TaskDefinitionRevisionNumber}`	aws:ResourceTag/${TagKey} (p. 1097) ecs:ResourceTag/${TagKey} (p. 1097)
task-set	`arn:${Partition}:ecs:${region}:${Account}:task-set/${ClusterName}/${ServiceName}/${TaskSetId}`	aws:ResourceTag/${TagKey} (p. 1097) ecs:ResourceTag/${TagKey} (p. 1097)

Amazon Elastic Container Service에 사용되는 조건 키

Amazon Elastic Container Service는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}		문자열
aws:ResourceTag/${TagKey}		문자열
aws:TagKeys		문자열
ecs:ResourceTag/${TagKey}		문자열
ecs:cluster	ECS 클러스터의 ARN.	ARN
ecs:container-instances	ECS 컨테이너 인스턴스의 ARN.	ARN
ecs:service	ECS 서비스의 ARN.	ARN
ecs:task-definition	ECS 작업 정의의 ARN.	ARN

Amazon Elastic Container Service for Kubernetes에 사용되는 작업, 리소스 및 조건 키

Amazon Elastic Container Service for Kubernetes(서비스 접두사: `eks`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Elastic Container Service for Kubernetes에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCluster	Amazon EKS 클러스터를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1101) aws:TagKeys (p. 1101)	
CreateFargateProfile	AWS Fargate 프로필을 생성합니다.	쓰기	cluster* (p. 1100)		
				aws:RequestTag/${TagKey} (p. 1101) aws:TagKeys (p. 1101)	
CreateNodegroup	Amazon EKS 노드 그룹을 생성합니다.	쓰기	cluster* (p. 1100)		
				aws:RequestTag/${TagKey} (p. 1101) aws:TagKeys (p. 1101)	
DeleteCluster	Amazon EKS 클러스터를 삭제합니다.	쓰기	cluster* (p. 1100)		
DeleteFargateProfile	AWS Fargate 프로필을 삭제합니다.	쓰기	fargateprofile* (p. 1100)		
DeleteNodegroup	Amazon EKS 노드 그룹을 삭제합니다.	쓰기	nodegroup* (p. 1100)		
DescribeCluster	Amazon EKS 클러스터에 대한 설명이 포함된 정보를 반환합니다.	Read	cluster* (p. 1100)		
DescribeFargateProfile	클러스터와 연결된 AWS Fargate 프로필에 대한 설명 정보를 반환합니다.	Read	fargateprofile* (p. 1100)		
DescribeNodegroup	Amazon EKS 노드 그룹에 대한 설명이 포함된 정보를 반환합니다.	Read	nodegroup* (p. 1100)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeUpdate	지정된 리전 또는 기본 리전에서 지정된 Amazon EKS 클러스터/노드 그룹에 대한 지정된 업데이트를 설명합니다.	Read	cluster* (p. 1100)		
			nodegroup (p. 1100)		
ListClusters	지정된 리전 또는 기본 리전에 있는 AWS 계정의 Amazon EKS 클러스터를 나열합니다.	List			
ListFargateProfiles	주어진 클러스터와 연결된 AWS 계정(지정된 리전 또는 기본 리전)의 AWS Fargate 프로필을 나열합니다.	List	cluster* (p. 1100)		
ListNodegroups	지정된 리전 또는 기본 리전에서 지정된 클러스터에 연결된 AWS 계정의 Amazon EKS 노드 그룹을 나열합니다.	List	cluster* (p. 1100)		
ListTagsForResource	지정된 리소스의 태그를 나열합니다.	List	cluster (p. 1100)		
			fargateprofile (p. 1100)		
			nodegroup (p. 1100)		
ListUpdates	지정된 리전 또는 기본 리전에서 지정된 Amazon EKS 클러스터/노드 그룹에 대한 업데이트를 나열합니다.	List	cluster* (p. 1100)		
			nodegroup (p. 1100)		
TagResource	지정된 리소스에 태그를 지정합니다.	태그 지정	cluster (p. 1100)		
			fargateprofile (p. 1100)		
			nodegroup (p. 1100)		
				aws:RequestTag/${TagKey} (p. 1101) aws:TagKeys (p. 1101)	
UntagResource	지정된 리소스에서 태그를 제거합니다.	태그 지정	cluster (p. 1100)		
			fargateprofile (p. 1100)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			nodegroup (p. 1100)		
				aws:TagKeys (p. 1101)	
UpdateClusterConfig	Amazon EKS 클러스터 구성(예: API 서버 엔드포인트 액세스)을 업데이트합니다.	쓰기	cluster* (p. 1100)		
UpdateClusterVersion	Amazon EKS 클러스터의 Kubernetes 버전을 업데이트합니다.	쓰기	cluster* (p. 1100)		
UpdateNodegroupConfig	Amazon EKS 노드 그룹 구성(예: 최소/최대/원하는 용량 또는 레이블)을 업데이트합니다.	쓰기	nodegroup* (p. 1100)		
UpdateNodegroupVersion	Amazon EKS 노드 그룹의 Kubernetes 버전을 업데이트합니다.	쓰기	nodegroup* (p. 1100)		

Amazon Elastic Container Service for Kubernetes에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1097)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey} (p. 1101)
nodegroup	`arn:${Partition}:eks:${Region}:${Account}:nodegroup/${ClusterName}/${NodegroupName}/${UUID}`	aws:ResourceTag/${TagKey} (p. 1101)
fargateprofile	`arn:${Partition}:eks:${Region}:${Account}:fargateprofile/${ClusterName}/${FargateProfileName}/${UUID}`	aws:ResourceTag/${TagKey} (p. 1101)

Amazon Elastic Container Service for Kubernetes의 조건 키

Amazon Elastic Container Service for Kubernetes는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	EKS 서비스에 대한 사용자의 요청에 있는 키를 기준으로 액세스를 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	EKS 서비스에 대한 사용자의 요청에 있는 모든 태그 키 이름의 목록을 기준으로 액세스를 필터링합니다.	문자열

Amazon Elastic File System에 사용되는 작업, 리소스 및 조건 키

Amazon Elastic File System(서비스 접두사: `elasticfilesystem`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Elastic File System에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Backup [권한만 해당]	기존 파일 시스템에 대한 백업 작업을 시작합니다.	쓰기	file-system* (p. 1104)		
ClientMount [권한만 해당]	파일 시스템에 대한 읽기 액세스를 허용하는 권한입니다.	Read		elasticfilesystem:AccessPointArn (p. 1105)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ClientRootAccess [권한만 해당]	파일 시스템에 대한 루트 액세스를 허용하는 권한입니다.	쓰기	file-system* (p. 1104)		
				elasticfilesystem:AccessPointArn (p. 1105)	
ClientWrite [권한만 해당]	파일 시스템에 대한 쓰기 액세스를 허용하는 권한입니다.	쓰기	file-system* (p. 1104)		
				elasticfilesystem:AccessPointArn (p. 1105)	
CreateAccessPoint	지정된 파일 시스템에 대한 액세스 포인트를 생성합니다.	쓰기	file-system* (p. 1104)		
CreateFileSystem	빈 파일 시스템을 새로 생성합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 1104) aws:TagKeys (p. 1105)	
CreateMountTarget	파일 시스템의 탑재 대상을 생성합니다.	쓰기	file-system* (p. 1104)		
CreateTags	파일 시스템과 연결된 태그를 생성하거나 덮어씁니다.	태그 지정	file-system* (p. 1104)		
				aws:RequestTag/${TagKey} (p. 1104) aws:TagKeys (p. 1105)	
DeleteAccessPoint	지정된 액세스 포인트를 삭제합니다.	쓰기	access-point* (p. 1104)		
DeleteFileSystem	파일 시스템을 삭제하여 해당 콘텐츠에 대한 액세스를 영구적으로 차단합니다.	쓰기	file-system* (p. 1104)		
DeleteFileSystemPolicy	지정된 파일 시스템에 대한 리소스 수준 정책을 지웁니다.	쓰기	file-system* (p. 1104)		
DeleteMountTarget	지정된 탑재 대상을 삭제합니다.	쓰기	file-system* (p. 1104)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteTags	파일 시스템에서 지정된 태그를 삭제합니다.	태그 지정	file-system* (p. 1104)		
				aws:TagKeys (p. 1105)	
DescribeAccessPoints	Amazon EFS 액세스 포인트에 대한 설명을 반환합니다.	List	file-system* (p. 1104)		
DescribeFileSystemPolicy	지정된 파일 시스템에 대한 현재 리소스 수준 정책을 반환합니다.	Read	file-system (p. 1104)		
DescribeFileSystems	파일 시스템 CreationToken 또는 FileSystemId가 제공된 경우 특정 Amazon EFS 파일 시스템의 설명을 반환합니다. 그렇지 않으면 호출 중인 엔드포인트의 AWS 리전에서 호출자의 AWS 계정이 소유한 모든 파일 시스템의 설명을 반환합니다.	List	file-system (p. 1104)		
DescribeLifecycleConfiguration	지정된 Amazon EFS 파일 시스템에 대한 현재 LifecycleConfiguration 객체를 반환합니다.	Read	file-system* (p. 1104)		
DescribeMountTargetSecurityGroups	현재 탑재 대상에 대해 유효한 보안 그룹을 반환합니다.	Read	file-system* (p. 1104)		
DescribeMountTargets	파일 시스템에 대한 모든 현재 탑재 대상 또는 특정 탑재 대상의 설명을 반환합니다.	Read	file-system* (p. 1104)		
DescribeTags	파일 시스템과 연결된 태그를 반환합니다.	Read	file-system* (p. 1104)		
ListTagsForResource	지정된 Amazon EFS 리소스와 연결된 태그를 반환합니다.	Read	file-system* (p. 1104)		
ModifyMountTargetSecurityGroups	탑재 대상에 대해 유효한 보안 그룹 세트를 수정합니다.	쓰기	file-system* (p. 1104)		
PutFileSystemPolicy	지정된 파일 시스템에 대해 지정된 액터의 작업을 부여하거나 제한하는 리소스 수준 정책을 적용합니다.	쓰기	file-system* (p. 1104)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutLifecycleConfiguration	새 LifecycleConfiguration 객체를 생성하여 수명 주기 관리를 활성화합니다.	쓰기	file-system* (p. 1104)		
Restore [권한만 해당]	기존 파일 시스템에 대한 복원 작업을 시작합니다.	쓰기	file-system* (p. 1104)		
TagResource	지정된 Amazon EFS 리소스와 연결된 태그를 생성하거나 덮어씁니다.	태그 지정			
UntagResource	지정된 Amazon EFS 리소스에서 지정된 태그를 삭제합니다.	태그 지정			
UpdateFileSystem	기존 파일 시스템의 처리량 모드 또는 프로비저닝된 처리량을 업데이트합니다.	쓰기	file-system* (p. 1104)		

Amazon Elastic File System에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1101)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
file-system	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey} (p. 1104)
access-point	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:access-point/${AccessPointId}`	aws:ResourceTag/${TagKey} (p. 1104)

Amazon Elastic File System의 조건 키

Amazon Elastic File System은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
elasticfilesystem:AccessPointArn	파일 시스템을 마운트하는 데 사용되는 액세스 포인트의 ARN	문자열

Amazon Elastic Inference에 사용되는 작업, 리소스 및 조건 키

Amazon Elastic Inference(서비스 접두사: `elastic-inference`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Elastic Inference에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Connect	고객을 Elastic Inference 액셀러레이터에 연결합니다.	쓰기	accelerator* (p. 1106)		

Amazon Elastic Inference에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1105)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
accelerator	`arn:${Partition}:elastic-inference:${Region}:${Account}:elastic-inference-accelerator/${AcceleratorId}`	

Amazon Elastic Inference에 사용되는 조건 키

EI에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Elastic Load Balancing에 사용되는 작업, 리소스 및 조건 키

Elastic Load Balancing(서비스 접두사: `elasticloadbalancing`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Elastic Load Balancing에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTags	지정된 로드 밸런서에 지정된 태그를 추가합니다. 각 로드 밸런서는 최대 10개의 태그를 보유할 수 있습니다.	태그 지정	loadbalancer* (p. 1108)		
ApplySecurityGroupsToLoadBalancer	가상 사설 클라우드(VPC)에서 하나 이상의 보안 그룹을 로드 밸런서와 연결합니다.	쓰기	loadbalancer* (p. 1108)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AttachLoadBalancerToSubnets	지정된 로드 밸런서에 대해 구성된 VPC 세트에 하나 이상의 서브넷을 추가합니다.	쓰기	loadbalancer* (p. 1108)		
ConfigureHealthCheck	백엔드 인스턴스의 상태를 평가할 때 사용할 상태 확인 설정을 지정합니다.	쓰기	loadbalancer* (p. 1108)		
CreateAppCookieStickinessPolicy	애플리케이션 생성 쿠키의 수명을 따르는 고정 세션 수명으로 고정성 정책을 생성합니다.	쓰기	loadbalancer* (p. 1108)		
CreateLBCookieStickinessPolicy	브라우저(사용자 에이전트)의 수명 또는 지정된 만료 기간에 따라 제어되는 고정 세션 수명으로 고정성 정책을 생성합니다.	쓰기	loadbalancer* (p. 1108)		
CreateLoadBalancer	로드 밸런서를 생성합니다.	쓰기	loadbalancer (p. 1108)		
CreateLoadBalancerListeners	지정된 로드 밸런서에 대한 리스너를 하나 이상 생성합니다.	쓰기	loadbalancer* (p. 1108)		
CreateLoadBalancerPolicy	지정된 로드 밸런서에 대해 지정된 속성으로 정책을 생성합니다.	쓰기	loadbalancer* (p. 1108)		
DeleteLoadBalancer	지정된 로드 밸런서를 삭제합니다.	쓰기	loadbalancer* (p. 1108)		
DeleteLoadBalancerListeners	지정된 로드 밸런서에서 지정된 리스너를 삭제합니다.	쓰기	loadbalancer* (p. 1108)		
DeleteLoadBalancerPolicy	지정된 로드 밸런서에서 지정된 정책을 삭제합니다. 이 정책은 모든 리스너에 대해 활성화되어서는 안됩니다.	쓰기	loadbalancer* (p. 1108)		
DeregisterInstancesFromLoadBalancer	지정된 로드 밸런서에서 지정된 인스턴스를 등록 취소합니다.	쓰기	loadbalancer* (p. 1108)		
DescribeInstanceHealth	지정된 로드 밸런서와 관련하여 지정된 인스턴스의 상태를 설명합니다.	Read			
DescribeLoadBalancerAttributes	지정된 로드 밸런서에 대한 속성을 설명합니다.	Read			
DescribeLoadBalancerPolicies	지정된 정책을 설명합니다.	Read			
DescribeLoadBalancerPolicyTypes	지정된 로드 밸런서 정책 유형을 설명합니다.	Read			
DescribeLoadBalancers	지정된 로드 밸런서를 설명합니다. 로드 밸런서가 지정되지 않은 경우 호출을 통해 모든 로드 밸런서를 설명합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeTags	지정된 로드 밸런서와 연결된 태그를 설명합니다.	Read			
DetachLoadBalancerFromSubnets	로드 밸런서에 대해 구성된 서브넷 세트에서 지정된 서브넷을 제거합니다.	쓰기	loadbalancer* (p. 1108)		
DisableAvailabilityZonesForLoadBalancer	지정된 로드 밸런서에 대한 가용 영역 세트에서 지정된 가용 영역을 제거합니다.	쓰기	loadbalancer* (p. 1108)		
EnableAvailabilityZonesForLoadBalancer	지정된 로드 밸런서에 대한 가용 영역 세트에 지정된 가용 영역을 추가합니다.	쓰기	loadbalancer* (p. 1108)		
ModifyLoadBalancerAttributes	지정된 로드 밸런서의 속성을 수정합니다.	쓰기	loadbalancer* (p. 1108)		
RegisterInstancesWithLoadBalancer	지정된 로드 밸런서에 지정된 인스턴스를 추가합니다.	쓰기	loadbalancer* (p. 1108)		
RemoveTags	지정된 로드 밸런서에서 하나 이상의 태그를 제거합니다.	태그 지정	loadbalancer* (p. 1108)		
SetLoadBalancerListenerSSLCertificate	지정된 리스너의 SSL 연결을 종료하는 인증서를 설정합니다.	쓰기	loadbalancer* (p. 1108)		
SetLoadBalancerPoliciesForBackendServer	백엔드 서버가 수신 대기하는 지정된 포트와 연결된 정책 세트를 새로운 정책 세트로 바꿉니다.	쓰기	loadbalancer* (p. 1108)		
SetLoadBalancerPoliciesOfListener	지정된 로드 밸런서 포트에 대한 현재 정책 세트를 지정된 정책 세트로 바꿉니다.	쓰기	loadbalancer* (p. 1108)		

Elastic Load Balancing에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1106)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
listener	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}`	
loadbalancer	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}`	aws:RequestTag/tag-key (p. 1109) aws:TagKeys (p. 1109)

리소스 유형	ARN	조건 키
		elasticloadbalancing:ResourceTag/tag-key (p. 1109)

Elastic Load Balancing의 조건 키

Elastic Load Balancing은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/tag-key	ELB 서비스에 대한 사용자의 요청에 있는 키입니다.	문자열
aws:TagKeys	요청의 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열
elasticloadbalancing:ResourceTag/	리소스에 연결된 태그 키 및 값 페어의 서문 문자열입니다.	문자열
elasticloadbalancing:ResourceTag/tag-key	태그 키 및 값 페어입니다.	문자열

Elastic Load Balancing V2에 사용되는 작업, 리소스 및 조건 키

Elastic Load Balancing(서비스 접두사: `elasticloadbalancing`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Elastic Load Balancing V2에서 정의한 작업 (p. 1109)
- Elastic Load Balancing V2에서 정의한 리소스 유형 (p. 1113)
- Elastic Load Balancing V2의 조건 키 (p. 1114)

Elastic Load Balancing V2에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있

으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddListenerCertificates	지정된 보안 리스너에 지정된 인증서를 추가합니다.	쓰기	listener/app* (p. 1113)		
			listener/net* (p. 1114)		
AddTags	지정된 로드 밸런서에 지정된 태그를 추가합니다. 각 로드 밸런서는 최대 10개의 태그를 보유할 수 있습니다.	태그 지정	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		
			targetgroup (p. 1114)		
CreateListener	지정된 Application Load Balancer에 대한 리스너를 생성합니다.	쓰기	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		
CreateLoadBalancer	로드 밸런서를 생성합니다.	쓰기	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		
CreateRule	지정된 리스너에 대한 규칙을 생성합니다.	쓰기	listener/app* (p. 1113)		
			listener/net* (p. 1114)		
CreateTargetGroup	대상 그룹을 생성합니다.	쓰기	targetgroup* (p. 1114)		
DeleteListener	지정된 리스너를 삭제합니다.	쓰기	listener/app* (p. 1113)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			listener/net* (p. 1114)		
DeleteLoadBalancer	지정된 로드 밸런서를 삭제합니다.	쓰기	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		
DeleteRule	지정된 규칙을 삭제합니다.	쓰기	listener-rule/app* (p. 1113)		
			listener-rule/net* (p. 1114)		
DeleteTargetGroup	지정된 대상 그룹을 삭제합니다.	쓰기	targetgroup* (p. 1114)		
DeregisterTargets	지정된 대상 그룹에서 지정된 대상을 등록 취소합니다.	쓰기	targetgroup* (p. 1114)		
DescribeAccountLimits	AWS 계정에 대한 Elastic Load Balancing 리소스 제한을 설명합니다.	Read			
DescribeListenerCertificates	지정된 보안 리스너에 대한 인증서를 설명합니다.	Read			
DescribeListeners	지정된 Application Load Balancer에 대한 리스너 또는 지정된 리스너를 설명합니다.	Read			
DescribeLoadBalancerAttributes	지정된 로드 밸런서에 대한 속성을 설명합니다.	Read			
DescribeLoadBalancers	지정된 로드 밸런서를 설명합니다. 로드 밸런서가 지정되지 않은 경우 호출을 통해 모든 로드 밸런서를 설명합니다.	Read			
DescribeRules	지정된 리스너에 대한 규칙 또는 지정된 규칙을 설명합니다.	Read			
DescribeSSLPolicies	SSL 협상에 사용되는 지정된 정책 또는 모든 정책을 설명합니다.	Read			
DescribeTags	지정된 로드 밸런서와 연결된 태그를 설명합니다.	Read			
DescribeTargetGroupAttributes	지정된 대상 그룹에 대한 속성을 설명합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeTargetGroups	지정된 대상 그룹 또는 모든 대상 그룹을 설명합니다.	Read			
DescribeTargetHealth	지정된 대상 또는 모든 대상의 상태를 설명합니다.	Read			
ModifyListener	지정된 리스너의 지정된 속성을 수정합니다.	쓰기	listener/app* (p. 1113)		
			listener/net* (p. 1114)		
ModifyLoadBalancerAttributes	지정된 로드 밸런서의 속성을 수정합니다.	쓰기	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		
ModifyRule	지정된 규칙을 수정합니다.	쓰기	listener-rule/app* (p. 1113)		
			listener-rule/net* (p. 1114)		
ModifyTargetGroup	지정된 대상 그룹의 대상 상태를 평가할 때 사용되는 상태 확인을 수정합니다.	쓰기	targetgroup* (p. 1114)		
ModifyTargetGroupAttributes	지정된 대상 그룹의 지정된 속성을 수정합니다.	쓰기	targetgroup* (p. 1114)		
RegisterTargets	지정된 대상 그룹에 지정된 대상을 등록합니다.	쓰기	targetgroup* (p. 1114)		
RemoveListenerCertificates	지정된 보안 리스너의 지정된 인증서를 제거합니다.	쓰기	listener/app* (p. 1113)		
			listener/net* (p. 1114)		
RemoveTags	지정된 로드 밸런서에서 하나 이상의 태그를 제거합니다.	태그 지정	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			targetgroup (p. 1114)		
SetIpAddressType	찾을 수 없음	쓰기	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		
SetRulePriorities	지정된 규칙의 우선 순위를 설정합니다.	쓰기	listener-rule/app* (p. 1113)		
			listener-rule/net* (p. 1114)		
SetSecurityGroups	지정된 보안 그룹을 지정된 로드 밸런서와 연결합니다.	쓰기	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		
SetSubnets	지정된 로드 밸런서에 대해 지정된 서브넷의 가용 영역을 활성화합니다.	쓰기	loadbalancer/app/ (p. 1114)		
			loadbalancer/net/ (p. 1114)		
SetWebAcl [권한만 해당]	WAF에 WebAcl 권한을 부여합니다.	쓰기			

Elastic Load Balancing V2에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1109)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
listener/app	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}`	
listener-rule/app	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/app/`	

리소스 유형	ARN	조건 키
	`${LoadBalancerName}/${LoadBalancerId}/ ${ListenerId}/${ListenerRuleId}`	
listener/net	`arn:${Partition}:elasticloadbalancing: ${Region}:${Account}:listener/net/ ${LoadBalancerName}/${LoadBalancerId}/ ${ListenerId}`	
listener-rule/ net	`arn:${Partition}:elasticloadbalancing: ${Region}:${Account}:listener-rule/net/ ${LoadBalancerName}/${LoadBalancerId}/ ${ListenerId}/${ListenerRuleId}`	
loadbalancer/ app/	`arn:${Partition}:elasticloadbalancing: ${Region}:${Account}:loadbalancer/app/ ${LoadBalancerName}/${LoadBalancerId}`	aws:RequestTag/tag-key (p. 1114) aws:TagKeys (p. 1114) elasticloadbalancing:ResourceTag/ tag-key (p. 1115)
loadbalancer/ net/	`arn:${Partition}:elasticloadbalancing: ${Region}:${Account}:loadbalancer/net/ ${LoadBalancerName}/${LoadBalancerId}`	aws:RequestTag/tag-key (p. 1114) aws:TagKeys (p. 1114) elasticloadbalancing:ResourceTag/ tag-key (p. 1115)
targetgroup	`arn:${Partition}:elasticloadbalancing: ${Region}:${Account}:targetgroup/ ${TargetGroupName}/${TargetGroupId}`	aws:RequestTag/tag-key (p. 1114) aws:TagKeys (p. 1114) elasticloadbalancing:ResourceTag/ tag-key (p. 1115)

Elastic Load Balancing V2의 조건 키

Elastic Load Balancing V2는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/ tag-key	ELB 서비스에 대한 사용자의 요청에 있는 키입니다.	문자열
aws:TagKeys	요청의 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열

조건 키	설명	유형
elasticloadbalancing:ResourceTag/tag-key	태그 키 및 값 페어입니다.	문자열

Amazon Elastic MapReduce에 사용되는 작업, 리소스 및 조건 키

Amazon Elastic MapReduce(서비스 접두사: `elasticmapreduce`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Elastic MapReduce에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

> **Note**
>
> DescribeJobFlows API는 더 이상 사용되지 않으며 결국 제거됩니다. ListClusters, DescribeCluster, ListSteps, ListInstanceGroups 및 ListBootstrapActions를 대신 사용하는 것이 좋습니다.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddInstanceFleet	실행 중인 클러스터에 인스턴스 집합을 추가할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
AddInstanceGroups	실행 중인 클러스터에 인스턴스 그룹을 추가할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddJobFlowSteps	실행 중인 클러스터에 새 단계를 추가할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
AddTags	Amazon EMR 리소스에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	cluster (p. 1119)		
			editor (p. 1119)		
				aws:RequestTag/${TagKey} (p. 1119) aws:TagKeys (p. 1119) elasticmapreduce:RequestTag/${TagKey} (p. 1120)	
CancelSteps	실행 중인 클러스터에서 대기 중 단계를 취소할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
CreateEditor [권한만 해당]	EMR 노트북을 생성할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
				aws:RequestTag/${TagKey} (p. 1119) aws:TagKeys (p. 1119) elasticmapreduce:RequestTag/${TagKey} (p. 1120)	
CreateSecurityConfiguration	보안 구성을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteEditor [권한만 해당]	EMR 노트북을 삭제할 수 있는 권한을 부여합니다.	쓰기	editor* (p. 1119)		
DeleteSecurityConfiguration	보안 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DescribeCluster	상태, 하드웨어 및 소프트웨어 구성, VPC 설정 등 클러스터에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	cluster* (p. 1119)		
DescribeEditor [권한만 해당]	상태, 사용자, 역할, 태그, 위치 등 노트북에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read	editor* (p. 1119)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeJobFlows	이 API는 더 이상 사용되지 않으며 결국 제거됩니다. ListClusters, DescribeCluster, ListSteps, ListInstanceGroups 및 ListBootstrapActions를 대신 사용하는 것이 좋습니다.	Read	cluster* (p. 1119)		
DescribeSecurityConfiguration	보안 구성에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
DescribeStep	클러스터 단계에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	cluster* (p. 1119)		
GetBlockPublicAccessConfiguration	리전의 AWS 계정에 대한 EMR 블록 퍼블릭 액세스 구성을 검색할 수 있는 권한을 부여합니다.	Read			
ListBootstrapActions	클러스터와 연결된 부트스트랩 작업에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	cluster* (p. 1119)		
ListClusters	액세스 가능한 클러스터의 상태를 가져올 수 있는 권한을 부여합니다.	List			
ListEditors [권한만 해당]	액세스 가능한 EMR 노트북에 대한 요약 정보를 나열할 수 있는 권한을 부여합니다.	List			
ListInstanceFleets	클러스터의 인스턴스 집합에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	cluster* (p. 1119)		
ListInstanceGroups	클러스터의 인스턴스 그룹에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	cluster* (p. 1119)		
ListInstances	클러스터의 Amazon EC2 인스턴스에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	cluster* (p. 1119)		
ListSecurityConfigurations	이 계정에서 사용 가능한 보안 구성을 생성 날짜 및 시간과 함께 이름 기준으로 나열할 수 있는 권한을 부여합니다.	List			
ListSteps	클러스터와 연결된 단계를 나열할 수 있는 권한을 부여합니다.	Read	cluster* (p. 1119)		
ModifyCluster	클러스터에 대해 동시에 실행할 수 있는 단계 수와 같은 클러스터 설정을 변경할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyInstanceFleet	인스턴스 집합의 목표 온디맨드 및 목표 스팟 용량을 변경할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
ModifyInstanceGroups	인스턴스 그룹의 EC2 인스턴스 수 및 구성을 변경할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
OpenEditorInConsole [권한만 해당]	콘솔에서 EMR 노트북에 대해 Jupyter 노트북 편집기를 시작할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
			editor* (p. 1119)		
PutAutoScalingPolicy	코어 인스턴스 그룹 또는 작업 인스턴스 그룹에 대한 자동 조정 정책을 생성하거나 업데이트할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
PutBlockPublicAccessConfiguration	리전의 AWS 계정에 대한 EMR 블록 퍼블릭 액세스 구성을 생성하거나 업데이트할 수 있는 권한을 부여합니다.	권한 관리			
RemoveAutoScalingPolicy	인스턴스 그룹에서 자동 조정 정책을 제거할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
RemoveTags	Amazon EMR 리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	cluster (p. 1119)		
			editor (p. 1119)		
				aws:TagKeys (p. 1119)	
RunJobFlow	클러스터(작업 흐름)를 생성하고 시작할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1119) aws:TagKeys (p. 1119) elasticmapreduce:RequestTag/${TagKey} (p. 1120)	
SetTerminationProtection	클러스터에 대한 종료 보호를 추가하고 제거할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
StartEditor [권한만 해당]	EMR 노트북을 시작할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
			editor* (p. 1119)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StopEditor [권한만 해당]	EMR 노트북을 종료할 수 있는 권한을 부여합니다.	쓰기	editor* (p. 1119)		
TerminateJobFlows	클러스터(작업 흐름)를 종료할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1119)		
ViewEventsFromAllClustersInConsole [권한만 해당]	EMR 관리 콘솔을 사용하여 모든 클러스터의 이벤트를 볼 수 있는 권한을 부여합니다.	List			

Amazon Elastic MapReduce에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1115)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
cluster	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:cluster/${ClusterId}`	aws:ResourceTag/${TagKey} (p. 1119) elasticmapreduce:ResourceTag/${TagKey} (p. 1120)
editor	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:editor/${EditorId}`	aws:ResourceTag/${TagKey} (p. 1119) elasticmapreduce:ResourceTag/${TagKey} (p. 1120)

Amazon Elastic MapReduce에 사용되는 조건 키

Amazon Elastic MapReduce는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	태그와 값 페어가 작업과 함께 제공되는지 여부에 따라 액세스를 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	Amazon EMR 리소스와 연결된 태그와 값 페어를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	태그 키가 태그 값에 상관없이 작업과 함께 제공되는지 여부에 따라 액세스를 필터링합니다.	문자열

조건 키	설명	유형
elasticmapreduce:RequestTag/${TagKey}	태그와 값 페어가 작업과 함께 제공되는지 여부에 따라 작업을 필터링합니다.	문자열
elasticmapreduce:ResourceTag/${TagKey}	Amazon EMR 리소스와 연결된 태그와 값 페어를 기준으로 작업을 필터링합니다.	문자열

Amazon Elastic Transcoder에 사용되는 작업, 리소스 및 조건 키

Amazon Elastic Transcoder(서비스 접두사: `elastictranscoder`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Elastic Transcoder에서 정의한 작업 (p. 1120)
- Amazon Elastic Transcoder에서 정의한 리소스 유형 (p. 1121)
- Amazon Elastic Transcoder의 조건 키 (p. 1122)

Amazon Elastic Transcoder에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelJob	Elastic Transcoder가 처리를 시작하지 않은 작업 취소	쓰기	job* (p. 1122)		
CreateJob	작업 만들기	쓰기	pipeline* (p. 1122)		
			preset* (p. 1122)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreatePipeline	파이프라인 생성	쓰기	pipeline* (p. 1122)		
CreatePreset	사전 설정 생성.	쓰기	preset* (p. 1122)		
DeletePipeline	파이프라인 삭제	쓰기	pipeline* (p. 1122)		
DeletePreset	사전 설정 삭제	쓰기	preset* (p. 1122)		
ListJobsByPipeline	파이프라인에 할당된 작업 목록 가져오기	List	pipeline* (p. 1122)		
ListJobsByStatus	현재 AWS 계정에 연결되었으며 지정된 상태의 모든 작업에 대한 정보 가져오기	List			
ListPipelines	현재 AWS 계정과 연결된 파이프라인 목록 가져오기	List			
ListPresets	현재 AWS 계정과 연결된 모든 사전 설정 목록 가져오기.	List			
ReadJob	작업에 관한 세부 정보 가져오기	Read	job* (p. 1122)		
ReadPipeline	파이프라인에 관한 세부 정보 가져오기	Read	pipeline* (p. 1122)		
ReadPreset	사전 설정에 관한 세부 정보 가져오기.	Read	preset* (p. 1122)		
TestRole	Elastic Transcoder가 작업을 생성 및 처리할 수 있는지 확인하기 위해 파이프라인의 설정 테스트	쓰기			
UpdatePipeline	파이프라인의 설정 업데이트	쓰기	pipeline* (p. 1122)		
UpdatePipelineNotifications	파이프라인의 Amazon Simple Notification Service(Amazon SNS) 알림만 업데이트	쓰기	pipeline* (p. 1122)		
UpdatePipelineStatus	파이프라인 일시 중지 또는 다시 활성화(따라서 파이프라인은 작업 처리를 중지하거나 다시 시작함), 파이프라인의 상태 업데이트.	쓰기	pipeline* (p. 1122)		

Amazon Elastic Transcoder에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1120)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
job	`arn:${Partition}:elastictranscoder:${Region}:${Account}:job/${JobId}`	
pipeline	`arn:${Partition}:elastictranscoder:${Region}:${Account}:pipeline/${PipelineId}`	
preset	`arn:${Partition}:elastictranscoder:${Region}:${Account}:preset/${PresetId}`	

Amazon Elastic Transcoder의 조건 키

Elastic Transcoder에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon ElastiCache에 사용되는 작업, 리소스 및 조건 키

Amazon ElastiCache(서비스 접두사: `elasticache`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon ElastiCache에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

> **Note**
>
> IAM에서 ElastiCache 정책을 생성할 때는 리소스 블록에 "*" 와일드카드 문자를 사용해야 합니다. IAM 정책에서 다음 ElastiCache API 작업 사용에 대한 자세한 내용은 Amazon ElastiCache 사용 설명서의 ElastiCache 작업 및 IAM 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTagsToResource	AddTagsToResource 작업은 최대 10개의 비용 할당 태그를 이름이 지정된 리소스에 추가합니다.	태그 지정			
AuthorizeCacheSecurityGroupIngress	AuthorizeCacheSecurityGroupIngress 작업은 캐시 보안 그룹에 대한 네트워크 수신을 허용합니다.	쓰기			ec2:AuthorizeSecurityGro
CopySnapshot	CopySnapshot 작업은 기존 스냅샷을 복사합니다.	쓰기			s3:DeleteObject s3:GetBucketAcl s3:PutObject
CreateCacheCluster	CreateCacheCluster 작업은 캐시 클러스터를 생성합니다.	쓰기			ec2:CreateNetworkInterfa ec2:DeleteNetworkInterfa ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
CreateCacheParameterGroup	CreateCacheParameterGroup 작업은 새 캐시 파라미터 그룹을 생성합니다.	쓰기			
CreateCacheSecurityGroup	CreateCacheSecurityGroup 작업은 새 캐시 보안 그룹을 생성합니다.	쓰기			
CreateCacheSubnetGroup	CreateCacheSubnetGroup 작업은 새 캐시 서브넷 그룹을 생성합니다.	쓰기			
CreateReplicationGroup	CreateReplicationGroup 작업은 복제 그룹을 생성합니다.	쓰기			ec2:CreateNetworkInterfa ec2:DeleteNetworkInterfa ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
CreateSnapshot	CreateSnapshot 작업은 시간상 특정 순간에 전체 캐시 클러스터의 복사본을 생성합니다.	쓰기			
DecreaseReplicaCount	DecreaseReplicaCount 작업은 Redis 복제 그룹의 복제본 수를 줄입니다.	쓰기			ec2:CreateNetworkInterfa ec2:DeleteNetworkInterfa

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
					ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs
DeleteCacheCluster	DeleteCacheCluster 작업은 이전에 프로비저닝된 캐시 클러스터를 삭제합니다.	쓰기			
DeleteCacheParameterGroup	DeleteCacheParameterGroup 작업은 지정된 캐시 파라미터 그룹을 삭제합니다.	쓰기			
DeleteCacheSecurityGroup	DeleteCacheSecurityGroup 작업은 캐시 보안 그룹을 삭제합니다.	쓰기			
DeleteCacheSubnetGroup	DeleteCacheSubnetGroup 작업은 캐시 서브넷 그룹을 삭제합니다.	쓰기			
DeleteReplicationGroup	DeleteReplicationGroup 작업은 기존 복제 그룹을 삭제합니다.	쓰기			
DeleteSnapshot	DeleteSnapshot 작업은 기존 스냅샷을 삭제합니다.	쓰기			
DescribeCacheClusters	DescribeCacheClusters 작업은 캐시 클러스터 식별자가 지정되지 않은 경우 프로비저닝된 모든 캐시 클러스터 또는 캐시 클러스터 식별자가 제공된 경우 특정 캐시 클러스터에 대한 정보를 반환합니다.	List			
DescribeCacheEngineVersions	DescribeCacheEngineVersions 작업은 사용 가능한 캐시 엔진 및 버전의 목록을 반환합니다.	List			
DescribeCacheParameterGroups	DescribeCacheParameterGroups 작업은 캐시 파라미터 그룹 설명의 목록을 반환합니다.	List			
DescribeCacheParameters	DescribeCacheParameters 작업은 특정 캐시 파라미터 그룹에 대한 세부 파라미터 목록을 반환합니다.	List			
DescribeCacheSecurityGroups	DescribeCacheSecurityGroups 작업은 캐시 보안 그룹 설명의 목록을 반환합니다.	List			
DescribeCacheSubnetGroups	DescribeCacheSubnetGroups 작업은 캐시 서브넷 그룹 설명의 목록을 반환합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeEngineDefaultParameters	DescribeEngineDefaultParameters 작업은 지정된 캐시 엔진에 대한 기본 엔진 및 시스템 파라미터 정보를 반환합니다.	List			
DescribeEvents	DescribeEvents 작업은 캐시 클러스터, 캐시 보안 그룹 및 캐시 파라미터 그룹과 관련된 이벤트를 반환합니다.	List			
DescribeReplicationGroups	DescribeReplicationGroups 작업은 특정 복제 그룹에 대한 정보를 반환합니다.	List			
DescribeReservedCacheNodes	DescribeReservedCacheNodes 작업은 이 계정에 대한 예약 캐시 노드 또는 지정된 예약 캐시 노드에 대한 정보를 반환합니다.	List			
DescribeReservedCacheNodesOfferings	DescribeReservedCacheNodesOfferings 작업은 사용 가능한 예약 캐시 노드 제공을 나열합니다.	List			
DescribeSnapshots	DescribeSnapshots 작업은 캐시 클러스터 스냅샷에 대한 정보를 반환합니다.	List			
IncreaseReplicaCount	IncreaseReplicaCount 작업은 Redis 복제 그룹의 복제본 수를 늘립니다.	쓰기			ec2:CreateNetworkInterfa ec2:DeleteNetworkInterfa ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs
ListAllowedNodeTypeModifications	허용된 노드 유형 수정을 나열합니다.	List			
ListTagsForResource	ListTagsForResource 작업은 현재 이름이 지정된 리소스에 있는 모든 비용 할당 태그를 나열합니다.	Read			
ModifyCacheCluster	ModifyCacheCluster 작업은 캐시 클러스터에 대한 설정을 수정합니다.	쓰기			
ModifyCacheParameterGroup	ModifyCacheParameterGroup 작업은 캐시 파라미터 그룹의 파라미터를 수정합니다.	쓰기			
ModifyCacheSubnetGroup	ModifyCacheSubnetGroup 작업은 기존 캐시 서브넷 그룹을 수정합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyReplicationGroup	ModifyReplicationGroup 작업은 복제 그룹에 대한 설정을 수정합니다.	쓰기			
ModifyReplicationGroupShardConfiguration	ModifyReplicationGroupShardConfiguration 작업은 샤드를 추가하거나, 샤드를 제거하거나, 기존 샤드 간에 키스페이스를 재분배하도록 허용합니다.	쓰기			ec2:CreateNetworkInterfa ec2:DeleteNetworkInterfa ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs
PurchaseReservedCacheNodesOffering	PurchaseReservedCacheNodesOffering 작업을 예약 캐시 노드 제공을 구입하도록 허용합니다.	쓰기			
RebootCacheCluster	RebootCacheCluster 작업은 프로비저닝된 캐시 클러스터 내의 일부 또는 모든 캐시 노드를 재부팅합니다.	쓰기			
RemoveTagsFromResource	RemoveTagsFromResource 작업은 이름이 지정된 리소스에서 TagKeys 목록으로 식별된 태그를 제거합니다.	태그 지정			
ResetCacheParameterGroup	ResetCacheParameterGroup 작업은 캐시 파라미터 그룹의 파라미터를 엔진 또는 시스템 기본값으로 수정합니다.	쓰기			
RevokeCacheSecurityGroupIngress	RevokeCacheSecurityGroupIngress 작업은 캐시 보안 그룹의 수신을 취소합니다.	쓰기			
TestFailover	TestFailover 작업은 복제 그룹 내의 지정된 노드 그룹에 대해 자동 장애 조치를 테스트하도록 허용합니다.	쓰기			ec2:CreateNetworkInterfa ec2:DeleteNetworkInterfa ec2:DescribeNetworkInter ec2:DescribeSubnets ec2:DescribeVpcs

Amazon ElastiCache에서 정의한 리소스 유형

Amazon ElastiCache는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon ElastiCache에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon ElastiCache의 조건 키

ElastiCache에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Note

IAM 정책에서 조건을 사용하여 ElastiCache에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 Amazon ElastiCache 사용 설명서의 ElastiCache 키를 참조하십시오.

Amazon Elasticsearch Service에 사용되는 작업, 리소스 및 조건 키

Amazon Elasticsearch Service(서비스 접두사: `es`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

Amazon Elasticsearch Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTags	Amazon ES 도메인에 리소스 태그를 연결할 권한을 부여합니다.	태그 지정	domain* (p. 1130)		
CreateElasticsearchDomain	Amazon ES 도메인을 생성할 권한을 부여합니다.	쓰기	domain (p. 1130)		
CreateElasticsearchServiceRole	VPC 액세스를 사용하는 Amazon ES 도메인에 필요한 서비스 연결 역할을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteElasticsearchDomain	Amazon ES 도메인 및 모든 데이터를 삭제할 권한을 부여합니다.	쓰기	domain* (p. 1130)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteElasticsearchServiceRole	VPC 액세스를 사용하는 Amazon ES 도메인에 필요한 서비스 연결 역할을 삭제할 권한을 부여합니다.	쓰기			
DescribeElasticsearchDomain	도메인 ID, 도메인 서비스 엔드포인트 및 도메인 ARN을 비롯하여 지정된 Amazon ES 도메인에 대한 도메인 구성의 설명을 볼 권한을 부여합니다.	Read	domain* (p. 1130)		
DescribeElasticsearchDomainConfig	Amazon ES 도메인의 구성 옵션 및 상태에 대한 설명을 볼 권한을 부여합니다.	Read	domain* (p. 1130)		
DescribeElasticsearchDomains	지정된 최대 5개의 Amazon ES 도메인에 대한 도메인 구성의 설명을 볼 권한을 부여합니다.	List	domain* (p. 1130)		
DescribeElasticsearchInstanceTypeLimits	지정된 Elasticsearch 버전 및 인스턴스 유형에 대한 인스턴스 개수, 스토리지 및 마스터 노드 제한을 볼 권한을 부여합니다.	List			
DescribeReservedElasticsearchInstanceOfferings	ES에 대한 예약 인스턴스 상품을 가져올 수 있는 권한을 부여합니다.	List			
DescribeReservedElasticsearchInstances	고객이 이미 구매한 ES 예약 인스턴스를 가져올 수 있는 권한을 부여합니다.	List			
ESHttpDelete	HTTP DELETE 요청을 Elasticsearch API로 전송할 권한을 부여합니다.	쓰기	domain (p. 1130)		
ESHttpGet	HTTP GET 요청을 Elasticsearch API로 전송할 권한을 부여합니다.	Read	domain (p. 1130)		
ESHttpHead	HTTP HEAD 요청을 Elasticsearch API로 전송할 권한을 부여합니다.	Read	domain (p. 1130)		
ESHttpPatch	HTTP PATCH 요청을 Elasticsearch API로 전송할 권한을 부여합니다.	쓰기	domain (p. 1130)		
ESHttpPost	HTTP POST 요청을 Elasticsearch API로 전송할 권한을 부여합니다.	쓰기	domain (p. 1130)		
ESHttpPut	HTTP PUT 요청을 Elasticsearch API로 전송할 권한을 부여합니다.	쓰기	domain (p. 1130)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetCompatibleElasticsearchVersions	Amazon ES 도메인을 업그레이드할 수 있는 호환되는 Elasticsearch 버전의 목록을 가져올 수 있는 권한을 부여합니다.	List	domain* (p. 1130)		
GetUpgradeHistory	지정된 ES 도메인의 업그레이드 기록을 가져올 수 있는 권한을 부여합니다.	Read	domain* (p. 1130)		
GetUpgradeStatus	지정된 ES 도메인의 업그레이드 상태를 가져올 수 있는 권한을 부여합니다.	Read	domain* (p. 1130)		
ListDomainNames	현재 사용자가 소유한 모든 Amazon ES 도메인의 이름을 표시할 권한을 부여합니다.	List			
ListElasticsearchInstanceTypeDetails	지정된 Elasticsearch 버전에서 사용 가능한 기능과 모든 인스턴스 유형을 나열할 수 있는 권한을 부여합니다.	List			
ListElasticsearchInstanceTypes	지정된 Elasticsearch 버전에서 지원되는 모든 Elasticsearch 인스턴스 유형을 나열할 권한을 부여합니다.	List			
ListElasticsearchVersions	Amazon ES에서 지원되는 모든 Elasticsearch 버전을 나열할 권한을 부여합니다.	List			
ListTags	Amazon ES 도메인에 대한 모든 태그를 표시할 권한을 부여합니다.	Read	domain* (p. 1130)		
PurchaseReservedElasticsearchInstanceOffering	ES 예약 인스턴스를 구매할 수 있는 권한을 부여합니다.	쓰기			
RemoveTags	Amazon ES 도메인에서 태그를 제거할 권한을 부여합니다.	태그 지정	domain* (p. 1130)		
UpdateElasticsearchDomainConfig	Amazon ES 도메인의 구성(예: 인스턴스 유형 또는 인스턴스 수)을 수정할 권한을 부여합니다.	쓰기	domain* (p. 1130)		
UpgradeElasticsearchDomain	지정된 버전으로 Elasticsearch 도메인 업그레이드를 시작할 수 있는 권한을 부여합니다.	쓰기	domain* (p. 1130)		

Amazon Elasticsearch Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1127)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
domain	`arn:${Partition}:es:${Region}:${Account}:domain/${DomainName}`	

Amazon Elasticsearch Service의 조건 키

Elasticsearch Service에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Elemental MediaConnect에 사용되는 작업, 리소스 및 조건 키

AWS Elemental MediaConnect(서비스 접두사: `mediaconnect`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Elemental MediaConnect에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddFlowOutputs	흐름에 출력을 추가할 수 있는 권한을 부여합니다.	쓰기			
CreateFlow	흐름을 생성할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteFlow	흐름을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DescribeFlow	흐름 ARN, 이름 및 가용성, 그리고 소스, 출력 및 권한에 대한 세부 정보를 포함한 흐름의 세부 정보를 표시할 수 있는 권한을 부여합니다.	Read			
GrantFlowEntitlements	흐름에 권한을 부여할 수 있는 권한을 부여합니다.	쓰기			
ListEntitlements	계정에 부여된 모든 권한의 목록을 표시할 수 있는 권한을 부여합니다.	List			
ListFlows	이 계정과 관련된 흐름의 목록을 표시할 수 있는 권한을 부여합니다.	List			
RemoveFlowOutput	흐름에서 출력을 제거할 수 있는 권한을 부여합니다.	쓰기			
RevokeFlowEntitlement	흐름에 권한을 부여할 수 있는 권한을 부여합니다.	쓰기			
StartFlow	흐름을 시작할 수 있는 권한을 부여합니다.	쓰기			
StopFlow	흐름을 중지할 수 있는 권한을 부여합니다.	쓰기			
UpdateFlowEntitlement	흐름에 대한 권한을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateFlowOutput	흐름에 대한 출력을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateFlowSource	흐름의 소스를 업데이트할 수 있는 권한을 부여합니다.	쓰기			

AWS Elemental MediaConnect에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1130)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Entitlement	`arn:${Partition}:mediaconnect:${Region}:${Account}:entitlement:${FlowId}:${EntitlementName}`	

리소스 유형	ARN	조건 키
Flow	`arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}`	
Output	`arn:${Partition}:mediaconnect:${Region}:${Account}:output:${OutputId}:${OutputName}`	
Source	`arn:${Partition}:mediaconnect:${Region}:${Account}:source:${SourceId}:${SourceName}`	

AWS Elemental MediaConnect에서 사용되는 조건 키

MediaConnect에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Elemental MediaConvert에 사용되는 작업, 리소스 및 조건 키

AWS Elemental MediaConvert(서비스 접두사: `mediaconvert`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Elemental MediaConvert에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateCertificate	AWS Certificate Manager(ACM) Amazon 리소스 이름(ARN)을 AWS Elemental MediaConvert와 연결할 수 있는 권한을 부여합니다.	쓰기			
CancelJob	대기열에서 대기 중인 AWS Elemental MediaConvert 작업을 취소할 수 있는 권한을 부여합니다.	쓰기	Job* (p. 1136)		
CreateJob	AWS Elemental MediaConvert 작업을 생성하고 제출할 수 있는 권한을 부여합니다.	쓰기	JobTemplate (p. 1136)		
			Preset (p. 1136)		
			Queue (p. 1136)		
CreateJobTemplate	AWS Elemental MediaConvert 사용자 지정 작업 템플릿을 생성할 수 있는 권한을 부여합니다.	쓰기	Preset (p. 1136)		
			Queue (p. 1136)		
				aws:RequestTag/${TagKey} (p. 1136) aws:TagKeys (p. 1136)	
CreatePreset	AWS Elemental MediaConvert 사용자 지정 출력 사전 설정을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1136) aws:TagKeys (p. 1136)	
CreateQueue	AWS Elemental MediaConvert 작업 대기열을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1136) aws:TagKeys (p. 1136)	
DeleteJobTemplate	AWS Elemental MediaConvert 사용자 지정 작업 템플릿을 삭제할 수 있는 권한을 부여합니다.	쓰기	JobTemplate* (p. 1136)		
DeletePreset	AWS Elemental MediaConvert 사용자 지정 출력 사전 설정을 삭제할 수 있는 권한을 부여합니다.	쓰기	Preset* (p. 1136)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteQueue	AWS Elemental MediaConvert 작업 대기열을 삭제할 수 있는 권한을 부여합니다.	쓰기	Queue* (p. 1136)		
DescribeEndpoints	계정별 엔드포인트에 대한 요청을 보내 AWS Elemental MediaConvert 서비스를 구독할 수 있는 권한을 부여합니다. 모든 트랜스코딩 요청은 서비스가 반환하는 엔드포인트로 보내야 합니다.	List			
DisassociateCertificate	AWS Certificate Manager(ACM) 인증서의 Amazon 리소스 이름(ARN)과 AWS Elemental MediaConvert 리소스 간 연결을 제거할 수 있는 권한을 부여합니다.	쓰기			
GetJob	AWS Elemental MediaConvert 작업을 가져올 수 있는 권한을 부여합니다.	Read	Job* (p. 1136)		
GetJobTemplate	AWS Elemental MediaConvert 작업 템플릿을 가져올 수 있는 권한을 부여합니다.	Read	JobTemplate* (p. 1136)		
GetPreset	AWS Elemental MediaConvert 출력 사전 설정을 가져올 수 있는 권한을 부여합니다.	Read	Preset* (p. 1136)		
GetQueue	AWS Elemental MediaConvert 작업 대기열을 가져올 수 있는 권한을 부여합니다.	Read	Queue* (p. 1136)		
ListJobTemplates	AWS Elemental MediaConvert 작업 템플릿을 나열할 수 있는 권한을 부여합니다.	List			
ListJobs	AWS Elemental MediaConvert 작업을 나열할 수 있는 권한을 부여합니다.	List	Queue (p. 1136)		
ListPresets	AWS Elemental MediaConvert 출력 사전 설정을 나열할 수 있는 권한을 부여합니다.	List			
ListQueues	AWS Elemental MediaConvert 작업 대기열을 나열할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	MediaConvert 대기열, 사전 설정 또는 작업 템플릿에 대한 태그를 검색할 수 있는 권한을 부여합니다.	Read	JobTemplate (p. 1136)		
			Preset (p. 1136)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			Queue (p. 1136)		
TagResource	MediaConvert 대기열, 사전 설정 또는 작업 템플릿에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	JobTemplate (p. 1136)		
			Preset (p. 1136)		
			Queue (p. 1136)		
				aws:RequestTag/${TagKey} (p. 1136) aws:TagKeys (p. 1136)	
UntagResource	MediaConvert 대기열, 사전 설정 또는 작업 템플릿에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	JobTemplate (p. 1136)		
			Preset (p. 1136)		
			Queue (p. 1136)		
				aws:TagKeys (p. 1136)	
UpdateJobTemplate	AWS Elemental MediaConvert 사용자 지정 작업 템플릿을 업데이트할 수 있는 권한을 부여합니다.	쓰기	JobTemplate* (p. 1136)		
			Preset (p. 1136)		
			Queue (p. 1136)		
UpdatePreset	AWS Elemental MediaConvert 사용자 지정 출력 사전 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기	Preset* (p. 1136)		
UpdateQueue	AWS Elemental MediaConvert 작업 대기열을 업데이트할 수 있는 권한을 부여합니다.	쓰기	Queue* (p. 1136)		

AWS Elemental MediaConvert에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1132)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Job	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobs/${JobId}`	
Queue	`arn:${Partition}:mediaconvert:${Region}:${Account}:queues/${QueueName}`	aws:ResourceTag/${TagKey} (p. 1136)
Preset	`arn:${Partition}:mediaconvert:${Region}:${Account}:presets/${PresetName}`	aws:ResourceTag/${TagKey} (p. 1136)
JobTemplate	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobTemplates/${JobTemplateName}`	aws:ResourceTag/${TagKey} (p. 1136)
CertificateAssociation	`arn:${Partition}:mediaconvert:${Region}:${Account}:certificates/${CertificateArn}`	

AWS Elemental MediaConvert의 조건 키

AWS Elemental MediaConvert는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Elemental MediaLive에 사용되는 작업, 리소스 및 조건 키

AWS Elemental MediaLive(서비스 접두사: `medialive`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS Elemental MediaLive에서 정의한 작업 (p. 1137)
- AWS Elemental MediaLive에서 정의한 리소스 유형 (p. 1141)
- AWS Elemental MediaLive에 사용되는 조건 키 (p. 1141)

AWS Elemental MediaLive에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchUpdateSchedule	채널의 일정에서 작업을 추가 및 제거할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1141)		
CreateChannel	채널을 생성할 수 있는 권한을 부여합니다.	태그 지정	channel* (p. 1141)		
			input* (p. 1141)		
				aws:RequestTag/${TagKey} (p. 1141) aws:TagKeys (p. 1141)	
CreateInput	입력을 생성할 수 있는 권한을 부여합니다.	태그 지정	input* (p. 1141)		
			input-security-group* (p. 1141)		
				aws:RequestTag/${TagKey} (p. 1141) aws:TagKeys (p. 1141)	
CreateInputSecurityGroup	입력 보안 그룹을 생성할 수 있는 권한을 부여합니다.	태그 지정	input-security-group* (p. 1141)		
				aws:RequestTag/${TagKey} (p. 1141)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1141)	
CreateMultiplex	멀티플렉스를 생성할 수 있는 권한을 부여합니다.	태그 지정	multiplex* (p. 1141)		
				aws:RequestTag/${TagKey} (p. 1141) aws:TagKeys (p. 1141)	
CreateTags	채널, 입력, 입력 보안 그룹, 멀티플렉스 및 예약에 대한 태그를 생성할 수 있는 권한을 부여합니다.	태그 지정	channel (p. 1141)		
			input (p. 1141)		
			input-security-group (p. 1141)		
			multiplex (p. 1141)		
			reservation (p. 1141)		
				aws:TagKeys (p. 1141) aws:RequestTag/${TagKey} (p. 1141)	
DeleteChannel	채널을 삭제할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1141)		
DeleteInput	입력을 삭제할 수 있는 권한을 부여합니다.	쓰기	input* (p. 1141)		
DeleteInputSecurityGroup	입력 보안 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	input-security-group* (p. 1141)		
DeleteMultiplex	멀티플렉스를 삭제할 수 있는 권한을 부여합니다.	쓰기	multiplex* (p. 1141)		
DeleteReservation	만료된 예약을 삭제할 수 있는 권한을 부여합니다.	쓰기	reservation* (p. 1141)		
DeleteTags	채널, 입력, 입력 보안 그룹, 멀티플렉스 및 예약에서 태그를 삭제할 수 있는 권한을 부여합니다.	태그 지정	channel (p. 1141)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			input (p. 1141)		
			input-security-group (p. 1141)		
			multiplex (p. 1141)		
			reservation (p. 1141)		
				aws:TagKeys (p. 1141)	
DescribeChannel	채널에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	channel* (p. 1141)		
DescribeInput	입력을 설명할 수 있는 권한을 부여합니다.	Read	input* (p. 1141)		
DescribeInputSecurityGroup	입력 보안 그룹을 설명할 수 있는 권한을 부여합니다.	Read	input-security-group* (p. 1141)		
DescribeMultiplex	멀티플렉스를 설명할 수 있는 권한을 부여합니다.	Read	multiplex* (p. 1141)		
DescribeOffering	예약 상품에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	offering* (p. 1141)		
DescribeReservation	예약에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read	reservation* (p. 1141)		
DescribeSchedule	채널에 예약된 작업의 목록을 볼 수 있는 권한을 부여합니다.	Read	channel* (p. 1141)		
ListChannels	채널을 나열할 수 있는 권한을 부여합니다.	List			
ListInputSecurityGroups	입력 보안 그룹을 나열할 수 있는 권한을 부여합니다.	List			
ListInputs	입력을 나열할 수 있는 권한을 부여합니다.	List			
ListMultiplexes	멀티플렉스를 나열할 수 있는 권한을 부여합니다.	List			
ListOfferings	예약 상품을 나열할 수 있는 권한을 부여합니다.	List			
ListReservations	예약을 나열할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTagsForResource	채널, 입력, 입력 보안 그룹, 멀티플렉스 및 예약에 대한 태그를 나열할 수 있는 권한을 부여합니다.	List	channel (p. 1141)		
			input (p. 1141)		
			input-security-group (p. 1141)		
			multiplex (p. 1141)		
			reservation (p. 1141)		
PurchaseOffering	예약 상품을 구매할 수 있는 권한을 부여합니다.	태그 지정	offering* (p. 1141)		
			reservation* (p. 1141)		
				aws:RequestTag/${TagKey} (p. 1141) aws:TagKeys (p. 1141)	
StartChannel	채널을 시작할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1141)		
StartMultiplex	멀티플렉스를 시작할 수 있는 권한을 부여합니다.	쓰기	multiplex* (p. 1141)		
StopChannel	채널을 중지할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1141)		
StopMultiplex	멀티플렉스를 중지할 수 있는 권한을 부여합니다.	쓰기	multiplex* (p. 1141)		
UpdateChannel	채널을 업데이트할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1141)		
UpdateChannelClass	채널의 클래스를 업데이트할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1141)		
UpdateInput	입력을 업데이트할 수 있는 권한을 부여합니다.	쓰기	input* (p. 1141)		
UpdateInputSecurityGroup	입력 보안 그룹을 업데이트할 수 있는 권한을 부여합니다.	쓰기	input-security-group* (p. 1141)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateMultiplex	멀티플렉스를 업데이트할 수 있는 권한을 부여합니다.	쓰기	multiplex* (p. 1141)		
UpdateReservation	예약을 업데이트할 수 있는 권한을 부여합니다.	쓰기	reservation* (p. 1141)		

AWS Elemental MediaLive에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1137)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
channel	`arn:${Partition}:medialive:${Region}:${Account}:channel:*`	aws:ResourceTag/${TagKey} (p. 1141)
input	`arn:${Partition}:medialive:${Region}:${Account}:input:*`	aws:ResourceTag/${TagKey} (p. 1141)
input-security-group	`arn:${Partition}:medialive:${Region}:${Account}:inputSecurityGroup:*`	aws:ResourceTag/${TagKey} (p. 1141)
multiplex	`arn:${Partition}:medialive:${Region}:${Account}:multiplex:*`	aws:ResourceTag/${TagKey} (p. 1141)
reservation	`arn:${Partition}:medialive:${Region}:${Account}:reservation:*`	aws:ResourceTag/${TagKey} (p. 1141)
offering	`arn:${Partition}:medialive:${Region}:${Account}:offering:*`	

AWS Elemental MediaLive에 사용되는 조건 키

AWS Elemental MediaLive는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	MediaLive 요청에 대한 태그입니다.	문자열
aws:ResourceTag/${TagKey}	MediaLive 리소스에 대한 태그입니다.	문자열
aws:TagKeys	MediaLive 리소스 또는 요청에 대한 태그 키입니다.	문자열

AWS Elemental MediaPackage에 사용되는 작업, 리소스 및 조건 키

AWS Elemental MediaPackage(서비스 접두사: `mediapackage`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Elemental MediaPackage에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateChannel	AWS Elemental MediaPackage에서 채널을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1144) aws:TagKeys (p. 1144)	
CreateOriginEndpoint	AWS Elemental MediaPackage에서 엔드포인트를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1144) aws:TagKeys (p. 1144)	
DeleteChannel	AWS Elemental MediaPackage에서 채널을 삭제할 수 있는 권한을 부여합니다.	쓰기	channels* (p. 1144)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteOriginEndpoint	AWS Elemental MediaPackage에서 엔드포인트를 삭제할 수 있는 권한을 부여합니다.	쓰기	origin_endpoints* (p. 1144)		
DescribeChannel	AWS Elemental MediaPackage의 채널에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	channels* (p. 1144)		
DescribeOriginEndpoint	AWS Elemental MediaPackage의 엔드포인트에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	origin_endpoints* (p. 1144)		
ListChannels	AWS Elemental MediaPackage의 채널 목록을 볼 수 있는 권한을 부여합니다.	Read			
ListOriginEndpoints	AWS Elemental MediaPackage의 엔드포인트 목록을 볼 수 있는 권한을 부여합니다.	Read			
ListTagsForResource	채널 또는 OriginEndpoint에 할당된 태그를 나열할 수 있는 권한을 부여합니다.	Read	channels (p. 1144)		
			origin_endpoints (p. 1144)		
RotateIngestEndpointCredentials	AWS Elemental MediaPackage의 채널에 대한 IngestEndpoint 자격 증명을 교체할 수 있는 권한을 부여합니다.	쓰기	channels* (p. 1144)		
TagResource	채널 또는 OriginEndpoint에 태그를 할당할 수 있는 권한을 부여합니다.	쓰기	channels (p. 1144)		
			origin_endpoints (p. 1144)		
				aws:RequestTag/${TagKey} (p. 1144) aws:TagKeys (p. 1144)	
UntagResource	채널 또는 OriginEndpoint에 대한 태그를 삭제할 수 있는 권한을 부여합니다.	쓰기	channels (p. 1144)		
			origin_endpoints (p. 1144)		
				aws:TagKeys (p. 1144)	
UpdateChannel	AWS Elemental MediaPackage의 채널을 변경할 수 있는 권한을 부여합니다.	쓰기	channels* (p. 1144)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateOriginEndpoint	AWS Elemental MediaPackage의 엔드포인트를 변경할 수 있는 권한을 부여합니다.	쓰기	origin_endpoints* (p. 1144)		

AWS Elemental MediaPackage에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1142)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
channels	`arn:${Partition}:mediapackage:${Region}:${Account}:channels/${ChannelIdentifier}`	aws:ResourceTag/${TagKey} (p. 1144)
origin_endpoints	`arn:${Partition}:mediapackage:${Region}:${Account}:origin_endpoints/${OriginEndpointIdentifier}`	aws:ResourceTag/${TagKey} (p. 1144)

AWS Elemental MediaPackage의 조건 키

AWS Elemental MediaPackage는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}		문자열
aws:ResourceTag/${TagKey}		문자열
aws:TagKeys		문자열

AWS Elemental MediaPackage VOD에 사용되는 작업, 리소스 및 조건 키

AWS Elemental MediaPackage VOD(서비스 접두사: `mediapackage-vod`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Elemental MediaPackage VOD에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateAsset	AWS Elemental MediaPackage에서 자산을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreatePackagingConfiguration	AWS Elemental MediaPackage에서 패키지 구성을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreatePackagingGroup	AWS Elemental MediaPackage에서 패키지 그룹을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteAsset	AWS Elemental MediaPackage에서 자산을 삭제할 수 있는 권한을 부여합니다.	쓰기	assets* (p. 1146)		
DeletePackagingConfiguration	AWS Elemental MediaPackage에서 패키지 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기	packaging-configurations* (p. 1146)		
DeletePackagingGroup	AWS Elemental MediaPackage에서 패키지 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	packaging-groups* (p. 1146)		
DescribeAsset	AWS Elemental MediaPackage에서 자산에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	assets* (p. 1146)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribePackagingConfiguration	AWS Elemental MediaPackage에서 패키지 구성에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	packaging-configurations* (p. 1146)		
DescribePackagingGroup	AWS Elemental MediaPackage에서 패키지 그룹에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	packaging-groups* (p. 1146)		
ListAssets	AWS Elemental MediaPackage에서 자산 목록을 볼 수 있는 권한을 부여합니다.	List			
ListPackagingConfigurations	AWS Elemental MediaPackage에서 패키지구성 목록을 볼 수 있는 권한을 부여합니다.	List			
ListPackagingGroups	AWS Elemental MediaPackage에서 패키지 그룹 목록을 볼 수 있는 권한을 부여합니다.	List			

AWS Elemental MediaPackage VOD에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1145)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
assets	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:assets/${AssetIdentifier}`	
packaging-configurations	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-configurations/${PackagingConfigurationIdentifier}`	
packaging-groups	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-groups/${PackagingGroupIdentifier}`	

AWS Elemental MediaPackage VOD의 조건 키

MediaPackage VOD에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Elemental MediaStore에 사용되는 작업, 리소스 및 조건 키

AWS Elemental MediaStore(서비스 접두사: `mediastore`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Elemental MediaStore에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateContainer	컨테이너를 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteContainer	현재 계정의 컨테이너를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteContainerPolicy	현재 계정의 컨테이너에서 액세스 정책을 삭제할 수 있는 권한을 부여합니다.	권한 관리			
DeleteCorsPolicy	현재 계정의 컨테이너에서 CORS 정책을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteLifecyclePolicy	현재 계정의 컨테이너에서 수명 주기 정책을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteMetricPolicy	현재 계정의 컨테이너에서 지표 정책을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteObject	객체를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DescribeContainer	현재 계정의 컨테이너에 대한 세부 정보를 검색할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeObject	객체 메타데이터를 검색할 수 있는 권한을 부여합니다.	List			
GetContainerPolicy	현재 계정의 컨테이너에 대한 액세스 정책을 검색할 수 있는 권한을 부여합니다.	Read			
GetCorsPolicy	현재 계정의 컨테이너에 대한 CORS 정책을 검색할 수 있는 권한을 부여합니다.	Read			
GetLifecyclePolicy	현재 계정의 컨테이너에 할당된 수명 주기 정책을 검색할 수 있는 권한을 부여합니다.	Read			
GetMetricPolicy	현재 계정의 컨테이너에 할당된 지표 정책을 검색할 수 있는 권한을 부여합니다.	Read			
GetObject	객체를 검색할 수 있는 권한을 부여합니다.	Read			
ListContainers	현재 계정의 컨테이너 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListItems	현재 계정의 객체 및 폴더 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	현재 계정의 컨테이너에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read			
PutContainerPolicy	현재 계정의 컨테이너에 대한 액세스 정책을 생성 또는 교체할 수 있는 권한을 부여합니다.	권한 관리			
PutCorsPolicy	현재 계정의 컨테이너에 대한 CORS 정책을 추가 또는 수정할 수 있는 권한을 부여합니다.	쓰기			
PutLifecyclePolicy	현재 계정의 컨테이너에 할당된 수명 주기 정책을 추가 또는 수정할 수 있는 권한을 부여합니다.	쓰기			
PutMetricPolicy	현재 계정의 컨테이너에 할당된 지표 정책을 추가 또는 수정할 수 있는 권한을 부여합니다.	쓰기			
PutObject	객체를 업로드할 수 있는 권한을 부여합니다.	쓰기			
StartAccessLogging	현재 계정의 컨테이너에 대한 액세스 로깅을 활성화할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StopAccessLogging	현재 계정의 컨테이너에 대한 액세스 로깅을 비활성화할 수 있는 권한을 부여합니다.	쓰기			
TagResource	현재 계정의 컨테이너에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정			
UntagResource	현재 계정의 컨테이너에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정			

AWS Elemental MediaStore에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1147)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
container	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}`	

AWS Elemental MediaStore에 사용되는 조건 키

MediaStore에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Elemental MediaTailor에 사용되는 작업, 리소스 및 조건 키

AWS Elemental MediaTailor(서비스 접두사: `mediatailor`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Elemental MediaTailor에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeletePlaybackConfiguration	지정된 이름의 재생 구성을 삭제합니다.	쓰기	playbackConfiguration* (p. 1151)		
GetPlaybackConfiguration	지정된 이름의 구성을 검색할 수 있는 권한을 부여합니다.	Read	playbackConfiguration* (p. 1151)		
ListPlaybackConfigurations	사용 가능한 구성의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	지정된 재생 구성 리소스에 할당된 태그의 목록을 반환합니다.	Read			
PutPlaybackConfiguration	새 구성을 추가할 수 있는 권한을 부여합니다.	쓰기	playbackConfiguration* (p. 1151)		
				aws:RequestTag/${TagKey} (p. 1151) aws:TagKeys (p. 1151)	
TagResource	지정된 재생 구성 리소스에 태그를 추가합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 1151) aws:TagKeys (p. 1151)	
UntagResource	지정된 재생 구성 리소스에서 태그를 제거합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 1151) aws:TagKeys (p. 1151)	

AWS Elemental MediaTailor에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1149)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
playbackConfiguration	`arn:${Partition}:mediatailor:${Region}:${Account}:playbackConfiguration/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1151)

AWS Elemental MediaTailor에 사용되는 조건 키

AWS Elemental MediaTailor는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon EventBridge에 사용되는 작업, 리소스 및 조건 키

Amazon EventBridge(서비스 접두사: `events`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon EventBridge에서 정의한 작업 (p. 1151)
- Amazon EventBridge에서 정의한 리소스 유형 (p. 1155)
- Amazon EventBridge에 사용되는 조건 키 (p. 1155)

Amazon EventBridge에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시

됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ActivateEventSource	비활성화된 파트너 이벤트 소스를 활성화합니다. 활성화되면 일치하는 이벤트 버스가 이벤트 소스에서 이벤트를 수신하기 시작합니다.	쓰기	event-source* (p. 1155)		
CreateEventBus	계정 내에 새로운 이벤트 버스를 생성합니다. 이는 자체 사용자 지정 애플리케이션 및 서비스에서 이벤트를 수신하는 데 사용할 수 있는 사용자 지정 이벤트 버스이거나 파트너 이벤트 소스와 일치할 수 있는 파트너 이벤트 버스일 수 있습니다.	쓰기	event-bus* (p. 1155)		
				aws:RequestTag/${TagKey} (p. 1155) aws:TagKeys (p. 1155)	
CreatePartnerEventSource	AWS 파트너가 파트너 이벤트 소스를 생성하도록 호출합니다.	쓰기	event-source* (p. 1155)		
DeactivateEventSource	AWS 파트너가 파트너 이벤트 소스를 생성하도록 호출합니다.	쓰기	event-source* (p. 1155)		
DeleteEventBus	지정된 사용자 지정 이벤트 버스 또는 파트너 이벤트 버스를 삭제합니다. 이 이벤트 버스와 연결된 모든 규칙도 삭제됩니다. 계정의 기본 이벤트 버스는 삭제할 수 없습니다.	쓰기	event-bus* (p. 1155)		
DeletePartnerEventSource	AWS 파트너가 파트너 이벤트 소스를 삭제하도록 호출합니다.	쓰기	event-source* (p. 1155)		
DeleteRule	규칙을 삭제합니다. 규칙을 삭제하기 전에 먼저 RemoveTargets를 사용하여 규칙에서 모든 대상을 제거해야 합니다.	쓰기	rule* (p. 1155)		
DescribeEventBus	계정의 이벤트 버스 및 연결된 정책을 사용하여 계정에 이벤트를 기록하도록 허용된 외부 AWS 계정을 표시합니다.	Read	event-bus (p. 1155)		
DescribeEventSource	계정과 공유되는 지정된 파트너 이벤트 소스의 세부 정보를 설명합니다.	Read	event-source* (p. 1155)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribePartnerEventSource	생성한 지정된 파트너 이벤트 소스의 세부 정보를 설명하도록 AWS 파트너가 호출합니다.	Read	event-source* (p. 1155)		
DescribeRule	지정된 규칙에 대한 세부 정보를 설명합니다.	Read	rule* (p. 1155)		
DisableRule	규칙을 비활성화합니다. 비활성화된 규칙은 어떤 이벤트와도 일치하지 않으며, 일정 표현식이 있는 경우 자체 트리거되지 않습니다.	쓰기	rule* (p. 1155)		
EnableRule	규칙을 활성화합니다. 규칙이 없으면 작업이 실패합니다.	쓰기	rule* (p. 1155)		
ListEventBuses	기본 이벤트 버스, 사용자 지정 이벤트 버스, 파트너 이벤트 버스를 포함하여 계정의 모든 이벤트 버스를 나열합니다.	List	event-bus* (p. 1155)		
ListEventSources	이 계정과 공유된 이벤트 소스를 나열합니다.	List	event-source* (p. 1155)		
ListPartnerEventSourceAccounts	지정된 파트너 이벤트 소스가 연결된 AWS 계정 ID를 표시하도록 AWS 파트너가 호출합니다.	List	event-source* (p. 1155)		
ListPartnerEventSources	생성한 파트너 이벤트 소스를 모두 나열하도록 AWS 파트너가 호출합니다.	List	event-source* (p. 1155)		
ListRuleNamesByTarget	지정된 대상에 적용시킬 수 있는 규칙의 이름을 나열합니다.	List	rule* (p. 1155)		
ListRules	계정의 Amazon EventBridge 규칙을 나열합니다.	List	rule* (p. 1155)		
ListTagsForResource	이 작업은 Amazon EventBridge 리소스에 대한 태그를 나열합니다.	List	event-bus (p. 1155)		
			rule (p. 1155)		
ListTargetsByRule	규칙에 할당된 대상의 목록입니다.	List	rule* (p. 1155)		
PutEvents	규칙에 일치시킬 수 있도록 사용자 지정 이벤트를 Amazon EventBridge로 보냅니다.	쓰기			
PutPartnerEvents	규칙에 일치시킬 수 있도록 사용자 지정 이벤트를 Amazon EventBridge로 보냅니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutPermission	PutPermission을 실행하면 지정된 AWS 계정이 이벤트를 계정의 기본 이벤트 버스에 놓도록 허용합니다.	쓰기			
PutRule	규칙을 생성 또는 업데이트합니다. 규칙이 기본적으로 또는 상태 파라미터의 값을 기반으로 활성화됩니다.	태그 지정	rule* (p. 1155)		
				events:detail.userIdentity.principalId (p. 1156) events:detail-type (p. 1156) events:source (p. 1156) events:detail.service (p. 1156) events:detail.eventTypeCode (p. 1156) aws:RequestTag/${TagKey} (p. 1155) aws:TagKeys (p. 1155)	
PutTargets	대상을 규칙에 추가합니다. 대상은 규칙이 트리거될 때 호출될 수 있는 리소스입니다.	쓰기	rule* (p. 1155)		
				events:TargetArn (p. 1156)	
RemovePermission	이벤트를 기본 이벤트 버스에 놓을 수 있도록 다른 AWS 계정의 권한을 호출합니다.	쓰기			
RemoveTargets	규칙이 트리거될 때 대상이 더 이상 호출되지 않도록 규칙에서 대상을 제거합니다.	쓰기	rule* (p. 1155)		
TagResource	이 작업은 Amazon EventBridge 리소스를 태그 지정합니다.	태그 지정	event-bus (p. 1155)		
			rule (p. 1155)		
				aws:TagKeys (p. 1155) aws:RequestTag/${TagKey} (p. 1155)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
TestEventPattern	이벤트 패턴이 제공된 이벤트와 일치하는지 테스트합니다.	Read			
UntagResource	이 작업은 Amazon EventBridge 리소스에서 태그를 제거합니다.	태그 지정	event-bus (p. 1155)		
			rule (p. 1155)		
				aws:TagKeys (p. 1155)	

Amazon EventBridge에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1151)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
event-source	`arn:${Partition}:events:${Region}::event-source/${EventSourceName}`	
event-bus	`arn:${Partition}:events:${Region}:${Account}:event-bus/${EventBusName}`	aws:ResourceTag/${TagKey} (p. 1155)
rule	`arn:${Partition}:events:${Region}:${Account}:rule/[${EventBusName}/]${RuleName}`	aws:ResourceTag/${TagKey} (p. 1155)

Amazon EventBridge에 사용되는 조건 키

Amazon EventBridge는 `Condition` 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
events:TargetArn	규칙을 적용시킬 수 있는 대상의 ARN	ARN
events:detail-type	이벤트의 detail-type 필드의 리터럴 문자열에 일치시킵니다.	문자열
events:detail.eventTypeCode	이벤트의 detail.eventTypeCode 필드의 리터럴 문자열에 일치시킵니다.	문자열
events:detail.service	이벤트의 detail.service 필드의 리터럴 문자열에 일치시킵니다.	문자열
events:detail.userIdentity.principalId	이벤트의 detail.useridentity.principalid 필드의 리터럴 문자열에 일치시킵니다.	문자열
events:source	이벤트를 생성한 AWS 서비스 또는 AWS 파트너 이벤트 소스입니다. 이벤트의 소스 필드의 리터럴 문자열에 일치시킵니다.	문자열

Amazon EventBridge Schemas에 사용되는 작업, 리소스 및 조건 키

Amazon EventBridge Schemas(서비스 접두사: `schemas`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon EventBridge Schemas에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateDiscoverer	이벤트 스키마 검색자를 생성합니다. 생성된 이벤트는 해당 스키마 문서에 자동으로 매핑됩니다.	쓰기	discoverer* (p. 1159)		
CreateRegistry	계정에서 새 스키마 레지스트리를 생성합니다.	쓰기	registry* (p. 1159)		
CreateSchema	계정에서 새 스키마를 생성합니다.	쓰기	schema* (p. 1159)		
DeleteDiscoverer	계정에서 검색자를 삭제합니다.	쓰기	discoverer* (p. 1159)		
DeleteRegistry	계정에서 기존 레지스트리를 삭제합니다.	쓰기	registry* (p. 1159)		
DeleteSchema	계정에서 기존 스키마를 삭제합니다.	쓰기	schema* (p. 1159)		
DeleteSchemaVersion	계정에서 스키마의 특정 버전을 삭제합니다.	쓰기	schema* (p. 1159)		
DescribeCodeBinding	계정에서 특정 스키마에 대해 생성된 코드에 대한 메타데이터를 검색합니다.	Read	schema* (p. 1159)		
DescribeDiscoverer	계정에서 검색자 메타데이터를 검색합니다.	Read	discoverer* (p. 1159)		
DescribeRegistry	계정에서 기존 레지스트리 메타데이터를 설명합니다.	Read	registry* (p. 1159)		
DescribeSchema	계정에서 기존 스키마를 검색합니다.	Read	schema* (p. 1159)		
GetCodeBindingSource	계정에서 특정 스키마에 대해 생성된 코드에 대한 메타데이터를 검색합니다.	Read	schema* (p. 1159)		
GetDiscoveredSchema	제공된 샘플 이벤트 목록에 대한 스키마를 검색합니다.	Read			
ListDiscoverers	계정에서 모든 검색자를 나열합니다.	List	discoverer* (p. 1159)		
ListRegistries	계정에서 모든 검색자를 나열합니다.	List	registry* (p. 1159)		
ListSchemaVersions	스키마의 모든 버전을 나열합니다.	List	schema* (p. 1159)		
ListSchemas	모든 스키마를 나열합니다.	List	schema* (p. 1159)		
ListTagsForResource	이 작업은 리소스에 대한 태그를 나열합니다.	List	discoverer* (p. 1159)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			registry* (p. 1159)		
			schema* (p. 1159)		
PutCodeBinding	계정에서 특정 스키마에 대한 코드를 생성합니다.	쓰기	schema* (p. 1159)		
SearchSchemas	계정에서 지정된 키워드를 기반으로 스키마를 검색합니다.	List	schema* (p. 1159)		
StartDiscoverer	지정된 검색자를 시작합니다. 검색자가 일단 시작되면 게시된 이벤트에 대한 스키마를 계정의 구성된 소스에 자동으로 등록합니다.	쓰기	discoverer* (p. 1159)		
StopDiscoverer	지정된 검색자를 시작합니다. 검색자가 일단 시작되면 게시된 이벤트에 대한 스키마를 계정의 구성된 소스에 자동으로 등록합니다.	쓰기	discoverer* (p. 1159)		
TagResource	이 작업은 리소스에 태그를 지정합니다.	태그 지정	discoverer* (p. 1159)		
			registry* (p. 1159)		
			schema* (p. 1159)		
				aws:TagKeys (p. 1159) aws:RequestTag/${TagKey} (p. 1159)	
UntagResource	이 작업은 리소스에서 태그를 제거합니다.	태그 지정	discoverer* (p. 1159)		
			registry* (p. 1159)		
			schema* (p. 1159)		
				aws:TagKeys (p. 1159)	
UpdateDiscoverer	계정에서 기존 검색자를 업데이트합니다.	쓰기	discoverer* (p. 1159)		
UpdateRegistry	계정에서 기존 레지스트리 메타데이터를 업데이트합니다.	쓰기	registry* (p. 1159)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateSchema	계정에서 기존 스키마를 업데이트합니다.	쓰기	schema* (p. 1159)		

Amazon EventBridge Schemas에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1156)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
discoverer	`arn:${Partition}:schemas:${Region}:${Account}:discoverer/${DiscovererId}`	aws:ResourceTag/${TagKey} (p. 1159)
registry	`arn:${Partition}:schemas:${Region}:${Account}:registry/${RegistryName}`	aws:ResourceTag/${TagKey} (p. 1159)
schema	`arn:${Partition}:schemas:${Region}:${Account}:schema/${RegistryName}/${SchemaName}`	aws:ResourceTag/${TagKey} (p. 1159)

Amazon EventBridge Schemas의 조건 키

Amazon EventBridge Schemas는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Firewall Manager에 사용되는 작업, 리소스 및 조건 키

AWS Firewall Manager(서비스 접두사: `fms`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

AWS Firewall Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateAdminAccount	AWS Firewall Manager 관리자 계정을 설정하고 모든 조직 계정에서 서비스를 활성화합니다.	쓰기			
DeleteNotificationChannel	조직 전체의 주요 FM 이벤트 및 오류에 대해 FM 관리자에게 알리는 데 사용되는 IAM 역할 및 Amazon Simple Notification Service(SNS) 주제와의 AWS Firewall Manager 연결을 삭제합니다.	쓰기			
DeletePolicy	AWS Firewall Manager 정책을 영구적으로 삭제합니다.	쓰기	policy* (p. 1162)		
				aws:ResourceTag/${TagKey} (p. 1162)	
DisassociateAdminAccount	AWS Firewall Manager 관리자 계정으로 설정된 계정을 연결 해제하고 모든 조직 계정에서 서비스를 비활성화합니다.	쓰기			
GetAdminAccount	AWS Firewall Manager와 연결된 AWS Organizations 마스터 계정을 AWS Firewall Manager 관리자로 반환합니다.	Read			
GetComplianceDetail	지정된 멤버 계정에 대한 세부 규정 준수 정보를 반환합니다. 세부 정보에는 지정된 정책을 준수하거	Read	policy* (p. 1162)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	나 준수하지 않는 리소스가 포함되어 있습니다.				
GetNotificationChannel	AWS Firewall Manager SNS 로그를 기록하는 데 사용되는 Amazon Simple Notification Service(SNS) 주제에 대한 정보를 반환합니다.	Read			
GetPolicy	지정된 AWS Firewall Manager 정책에 대한 정보를 반환합니다.	Read	policy* (p. 1162)		
GetProtectionStatus	잠재적 DDoS 공격의 경우 정책 수준 공격 요약 정보를 반환합니다.	Read	policy* (p. 1162)		
ListComplianceStatus	응답에서 PolicyComplianceStatus 객체의 배열을 반환합니다. PolicyComplianceStatus를 사용하여 지정된 정책으로 보호되는 멤버 계정의 요약을 가져옵니다.	List	policy* (p. 1162)		
ListMemberAccounts	호출자가 FMS 관리자 계정일 경우 멤버 계정 ID의 배열을 반환합니다.	List			
ListPolicies	응답에서 PolicySummary 객체의 배열을 반환합니다.	List			
ListTagsForResource	지정된 리소스에 대한 태그를 나열합니다.	Read	policy* (p. 1162)		
PutNotificationChannel	AWS Firewall Manager(FM)가 조직 전체의 주요 FM 이벤트 및 오류에 대해 FM 관리자에게 알리는 데 사용할 수 있는 IAM 역할 및 Amazon Simple Notification Service(SNS) 주제를 지정합니다.	쓰기			
PutPolicy	AWS Firewall Manager 정책을 생성합니다.	쓰기	policy* (p. 1162)		
				aws:RequestTag/${TagKey} (p. 1162) aws:TagKeys (p. 1162)	
TagResource	지정된 리소스에 태그를 추가합니다.	태그 지정	policy* (p. 1162)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1162) aws:TagKeys (p. 1162)	
UntagResource	지정된 리소스에서 태그를 제거합니다.	태그 지정	policy* (p. 1162)		
				aws:TagKeys (p. 1162)	

AWS Firewall Manager에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1160)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
policy	`arn:${Partition}:fms:${Region}:${Account}:policy/${Id}`	aws:ResourceTag/${TagKey} (p. 1162)

AWS Firewall Manager의 조건 키

AWS Firewall Manager는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon Forecast에 사용되는 작업, 리소스 및 조건 키

Amazon Forecast(서비스 접두사: `forecast`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

Amazon Forecast에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateDataset	데이터 세트를 생성합니다.	쓰기	dataset* (p. 1165)		
CreateDatasetGroup	데이터 세트 그룹을 생성합니다.	쓰기	datasetGroup* (p. 1165)		
CreateDatasetImportJob	데이터 세트 가져오기 작업을 생성합니다.	쓰기	datasetImportJob* (p. 1165)		
CreateForecast	예측을 생성합니다.	쓰기	predictor* (p. 1165)		
CreateForecastExportJob	예측 내보내기 작업을 생성합니다.	쓰기	forecast* (p. 1165)		
CreatePredictor	예측기를 생성합니다.	쓰기	datasetGroup* (p. 1165)		
DeleteDataset	데이터 세트를 삭제합니다.	쓰기	dataset* (p. 1165)		
DeleteDatasetGroup	데이터 세트 그룹을 삭제합니다.	쓰기	datasetGroup* (p. 1165)		
DeleteDatasetImportJob	데이터 세트 가져오기 작업을 삭제합니다.	쓰기	datasetImportJob* (p. 1165)		
DeleteForecast	예측을 삭제합니다.	쓰기	forecast* (p. 1165)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteForecastExportJob	예측 내보내기 작업을 삭제합니다.	쓰기	forecastExport* (p. 1165)		
DeletePredictor	예측기를 삭제합니다.	쓰기	predictor* (p. 1165)		
DescribeDataset	데이터 세트를 설명합니다.	Read	dataset* (p. 1165)		
DescribeDatasetGroup	데이터 세트 그룹을 설명합니다.	Read	datasetGroup* (p. 1165)		
DescribeDatasetImportJob	데이터 세트 가져오기 작업을 설명합니다.	Read	datasetImportJob* (p. 1165)		
DescribeForecast	예측을 설명합니다.	Read	forecast* (p. 1165)		
DescribeForecastExportJob	예측 내보내기 작업을 설명합니다.	Read	forecastExport* (p. 1165)		
DescribePredictor	예측기를 설명합니다.	Read	predictor* (p. 1165)		
GetAccuracyMetrics	예측기에 대한 정확성 지표를 가져옵니다.	Read	predictor* (p. 1165)		
ListDatasetGroups	데이터 세트 그룹을 나열합니다.	List			
ListDatasetImportJobs	데이터 세트 가져오기 작업을 나열합니다.	List			
ListDatasets	데이터 세트를 나열합니다.	List			
ListForecastExportJobs	예측 내보내기 작업을 나열합니다.	List			
ListForecasts	예측을 나열합니다.	List			
ListPredictors	예측기를 나열합니다.	List			
QueryForecast	단일 항목에 대한 예측을 검색합니다.	Read	forecast* (p. 1165)		
UpdateDatasetGroup	데이터 세트 그룹을 업데이트합니다.	쓰기	dataset* (p. 1165)		
			datasetGroup* (p. 1165)		

Amazon Forecast에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1163)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
dataset	`arn:${Partition}:forecast:${Region}:${Account}:dataset/${ResourceId}`	
datasetGroup	`arn:${Partition}:forecast:${Region}:${Account}:dataset-group/${ResourceId}`	
datasetImportJob	`arn:${Partition}:forecast:${Region}:${Account}:dataset-import-job/${ResourceId}`	
algorithm	`arn:${Partition}:forecast:::algorithm/${ResourceId}`	
predictor	`arn:${Partition}:forecast:${Region}:${Account}:predictor/${ResourceId}`	
forecast	`arn:${Partition}:forecast:${Region}:${Account}:forecast/${ResourceId}`	
forecastExport	`arn:${Partition}:forecast:${Region}:${Account}:forecast-export-job/${ResourceId}`	

Amazon Forecast에 사용되는 조건 키

Forecast에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Fraud Detector에 사용되는 작업, 리소스 및 조건 키

Amazon Fraud Detector(서비스 접두사: `frauddetector`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Fraud Detector에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchCreateVariable	변수의 배치를 생성합니다.	쓰기			
BatchGetVariable	변수의 배치를 가져옵니다.	List			
CreateDetectorVersion	감지기 버전을 생성합니다. 감지기 버전이 DRAFT 상태로 시작됩니다.	쓰기			
CreateModelVersion	지정된 모델 유형을 사용하여 모델의 버전을 생성합니다.	쓰기			
CreateRule	지정된 감지기와 함께 사용할 규칙을 생성합니다.	쓰기			
CreateVariable	변수를 생성합니다.	쓰기			
DeleteDetectorVersion	감지기 버전을 삭제합니다.	쓰기			
DeleteEvent	지정된 이벤트를 삭제합니다.	쓰기			
DescribeDetector	지정된 감지기의 모든 버전을 가져옵니다.	Read			
DescribeModelVersions	지정된 모델 유형 또는 지정된 모델 유형 및 모델 ID에 대한 모든 모델 버전을 가져옵니다. 지정된 단일 모델 버전에 대한 세부 정보를 가져올 수도 있습니다.	Read			
GetDetectorVersion	특정 감지기 버전을 가져옵니다.	List			
GetDetectors	모든 감지기를 가져옵니다. 이것은 페이지 매김 API입니다. null MaxSizeperPage를 제공하는 경우, 이 작업은 페이지당 최대 10개의 레코드를 검색합니다. maxSizePerPage를 제공하는 경우에 이 값은 5와 10 사이여야 합니다. 다음 페이지 결과를 얻으려면 요청의 일부로 GetEventTypesResponse에서 나온 페이지 매김 토큰을 제공합니다. null 페이지 매김 토큰은 처음부터 레코드를 가져옵니다.	List			
GetExternalModels	서비스로 가져온 하나 이상의 Amazon SageMaker 모델에 대	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	한 세부 정보를 가져옵니다. 이것은 페이지 매김 API입니다. null MaxSizeperPage를 제공하는 경우, 이 작업은 페이지당 최대 10개의 레코드를 검색합니다. maxSizePerPage를 제공하는 경우에 이 값은 5와 10 사이여야 합니다. 다음 페이지 결과를 얻으려면 요청의 일부로 GetExternalModelsResult에서 나온 페이지 매김 토큰을 제공합니다. null 페이지 매김 토큰은 처음부터 레코드를 가져옵니다.				
GetModelVersion	모델 버전을 가져옵니다.	List			
GetModels	AWS 계정의 모든 모델 또는 지정된 모델 유형을 가져오거나 지정된 모델 유형, 모델 ID 조합에 대해 단일 모델을 가져옵니다.	List			
GetOutcomes	하나 이상의 결과를 가져옵니다. 이것은 페이지 매김 API입니다. null MaxSizeperPage를 제공하는 경우, 이 작업은 페이지당 최대 10개의 레코드를 검색합니다. maxSizePerPage를 제공하는 경우에 이 값은 50과 100 사이여야 합니다. 다음 페이지 결과를 얻으려면 요청의 일부로 GetOutcomesResult에서 나온 페이지 매김 토큰을 제공합니다. null 페이지 매김 토큰은 처음부터 레코드를 가져옵니다.	List			
GetPrediction	감지기 버전과 비교해 이벤트를 평가합니다. 버전 ID가 제공되지 않는 경우, 감지기(ACTIVE)의 버전이 사용됩니다.	Read			
GetRules	지정된 감지기에 사용할 수 있는 모든 규칙을 가져옵니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetVariables	모든 변수 또는 특정 변수를 가져옵니다. 이것은 페이지 매김 API입니다. null maxSizePerPage를 제공하면 페이지당 최대 100개의 레코드를 검색할 수 있습니다. maxSizePerPage를 제공하는 경우에 이 값은 50과 100 사이여야 합니다. 다음 페이지 결과를 얻으려면 요청의 일부로 GetVariablesResult에서 나온 페이지 매김 토큰을 제공합니다. null 페이지 매김 토큰은 처음부터 레코드를 가져옵니다.	List			
PutDetector	감지기를 생성 또는 업데이트합니다.	쓰기			
PutExternalModel	Amazon SageMaker 모델 엔드포인트를 생성 또는 업데이트합니다. 이 작업을 사용하여 IAM 역할 및/또는 매핑된 변수를 포함하여 모델 엔드포인트의 구성을 업데이트할 수도 있습니다.	쓰기			
PutModel	모델을 생성 또는 업데이트합니다.	쓰기			iam:PassRole
PutOutcome	결과를 생성 또는 업데이트합니다.	쓰기			
UpdateDetectorVersion	감지기 버전을 업데이트합니다. 업데이트할 수 있는 감지기 버전 속성으로는 모델, 외부 모델 엔드포인트, 규칙 및 설명이 있습니다. DRAFT 상태의 감지기 버전만 업데이트할 수 있습니다.	쓰기			
UpdateDetectorVersionMetadata	감지기 버전의 설명을 업데이트합니다. 모든 감지기 버전(DRAFT, ACTIVE 또는 INACTIVE)에 대한 메타데이터를 업데이트할 수 있습니다.	쓰기			
UpdateDetectorVersionStatus	감지기 버전의 상태를 업데이트합니다. UpdateDetectorVersionStatus를 사용하여 DRAFT에서 ACTIVE로, ACTIVE에서 INACTIVE로, 그리고 INACTIVE에서 ACTIVE로 상태를 승격 또는 강등할 수 있습니다.	쓰기			
UpdateModelVersion	모델 버전을 업데이트합니다. 이 작업을 사용하여 설명 및 상태 속성을 업데이트할 수 있습니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateRuleMetadata	규칙의 메타데이터를 업데이트합니다.	쓰기			
UpdateRuleVersion	규칙 버전을 업데이트하여 새 규칙 버전을 생성합니다.	쓰기			
UpdateVariable	변수를 업데이트합니다.	쓰기			

Amazon Fraud Detector에서 정의한 리소스 유형

Amazon Fraud Detector는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Fraud Detector에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Fraud Detector의 조건 키

Fraud Detector에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon FreeRTOS에 사용되는 작업, 리소스 및 조건 키

Amazon FreeRTOS(서비스 접두사: `freertos`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon FreeRTOS에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateSoftwareConfiguration	소프트웨어 구성을 생성합니다	쓰기	configuration* (p. 1170)		
				aws:RequestTag/${TagKey} (p. 1171) aws:TagKeys (p. 1171)	
DeleteSoftwareConfiguration	소프트웨어 구성을 삭제합니다.	쓰기	configuration* (p. 1170)		
DescribeHardwarePlatform	하드웨어 플랫폼을 설명합니다.	Read			
DescribeSoftwareConfiguration	소프트웨어 구성을 설명합니다.	Read	configuration* (p. 1170)		
GetSoftwareURL	Amazon FreeRTOS 소프트웨어 다운로드의 URL을 가져옵니다.	Read			
GetSoftwareURLForConfiguration	구성에 따른 Amazon FreeRTOS 소프트웨어 다운로드의 URL을 가져옵니다.	Read			
ListFreeRTOSVersions	AmazonFreeRTOS의 버전을 나열합니다.	List			
ListHardwarePlatforms	하드웨어 플랫폼을 나열합니다.	List			
ListHardwareVendors	하드웨어 공급업체를 나열합니다.	List			
ListSoftwareConfigurations	소프트웨어 구성을 나열합니다.	List			
UpdateSoftwareConfiguration	소프트웨어 구성을 업데이트합니다.	쓰기	configuration* (p. 1170)		

Amazon FreeRTOS에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1169)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
configuration	`arn:${Partition}:freertos:${Region}:${Account}:configuration/${configurationName}`	aws:ResourceTag/${TagKey} (p. 1171)

Amazon FreeRTOS에 사용되는 조건 키

Amazon FreeRTOS는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	사용자가 Amazon FreeRTOS로 보내는 요청에 존재하는 태그 키입니다.	문자열
aws:ResourceTag/${TagKey}	Amazon FreeRTOS 리소스에 연결된 태그의 태그 키 구성 요소입니다.	문자열
aws:TagKeys	요청의 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열

Amazon FSx에 사용되는 작업, 리소스 및 조건 키

Amazon FSx(서비스 접두사: `fsx`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon FSx에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelDataRepositoryTask	이 작업은 데이터 리포지토리 작업을 취소합니다.	쓰기	task* (p. 1174)		
CreateBackup	이 작업은 새 백업을 생성합니다.	태그 지정	backup* (p. 1174)		
			file-system* (p. 1174)		
				aws:RequestTag/${TagKey} (p. 1175) aws:TagKeys (p. 1175)	
CreateDataRepositoryTask	이 작업은 새 백업을 생성합니다.	태그 지정	file-system* (p. 1174)		
			task* (p. 1174)		
				aws:RequestTag/${TagKey} (p. 1175) aws:TagKeys (p. 1175)	
CreateFileSystem	이 작업은 빈 Amazon FSx 파일 시스템을 새로 생성합니다.	태그 지정	file-system* (p. 1174)		
				aws:RequestTag/${TagKey} (p. 1175) aws:TagKeys (p. 1175)	
CreateFileSystemFromBackup	이 작업은 기존 백업에서 새 Amazon FSx 파일 시스템을 생성합니다.	태그 지정	backup* (p. 1174)		
			file-system* (p. 1174)		
				aws:RequestTag/${TagKey} (p. 1175) aws:TagKeys (p. 1175)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteBackup	이 작업은 그 내용을 삭제하여 백업을 삭제합니다. 삭제 후 백업은 더 이상 존재하지 않고 데이터는 사라집니다.	쓰기	backup* (p. 1174)		
DeleteFileSystem	이 작업은 그 내용을 삭제하여 파일 시스템을 삭제합니다.	쓰기	file-system* (p. 1174)		
DescribeBackups	이 작업은 해당 백업에 대해 하나 이상의 BackupIds가 제공될 경우 특정 Amazon FSx 백업에 대한 설명을 반환합니다. 그렇지 않을 경우 사용자가 호출하는 엔드포인트의 AWS 리전에서 사용자의 AWS 계정이 소유하는 모든 백업을 반환합니다.	Read			
DescribeDataRepositoryTasks	이 작업은 해당 데이터 리포지토리 작업에 TaskId가 하나 이상 제공되는 경우 특정 Amazon FSX 데이터 리포지토리 작업에 대한 설명을 반환합니다. 그렇지 않을 경우 사용자가 호출하는 엔드포인트의 AWS 리전에서 사용자의 AWS 계정이 소유하는 모든 데이터 리포지토리 작업을 반환합니다.	Read			
DescribeFileSystems	이 작업은 파일 시스템에 대해 FileSystemIds 값이 제공될 경우 특정 Amazon FSx 파일 시스템에 대한 설명을 반환합니다. 그렇지 않을 경우 사용자가 호출하는 엔드포인트의 AWS 리전에서 사용자의 AWS 계정이 소유하는 모든 파일 시스템에 대한 설명을 반환합니다.	Read			
ListTagsForResource	이 작업은 Amazon FSx 리소스에 대한 태그를 나열합니다.	Read	backup (p. 1174)		
			file-system (p. 1174)		
			task (p. 1174)		
TagResource	이 작업은 Amazon FSx 리소스에 태그를 지정합니다.	태그 지정	backup (p. 1174)		
			file-system (p. 1174)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			task (p. 1174)		
				aws:TagKeys (p. 1175) aws:RequestTag/${TagKey} (p. 1175)	
UntagResource	이 작업은 Amazon FSx 리소스에서 태그를 제거합니다.	태그 지정	backup (p. 1174)		
			file-system (p. 1174)		
			task (p. 1174)		
				aws:TagKeys (p. 1175)	
UpdateFileSystem	이 작업은 파일 시스템 구성을 업데이트합니다.	쓰기	file-system* (p. 1174)		

Amazon FSx에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1171)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
file-system	`arn:${Partition}:fsx:${Region}:${Account}:file-system/*`	aws:ResourceTag/${TagKey} (p. 1175)
backup	`arn:${Partition}:fsx:${Region}:${Account}:backup/*`	aws:ResourceTag/${TagKey} (p. 1175)
task	`arn:${Partition}:fsx:${Region}:${Account}:task/*`	aws:ResourceTag/${TagKey} (p. 1175)

Amazon FSx에 사용되는 조건 키

Amazon FSx는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/ ${TagKey}		문자열
aws:ResourceTag/ ${TagKey}		문자열
aws:TagKeys		문자열

Amazon GameLift에 사용되는 작업, 리소스 및 조건 키

Amazon GameLift(서비스 접두사: `gamelift`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon GameLift에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptMatch	제안된 FlexMatch 매치의 플레이어 수락 또는 거부를 등록합니다.	쓰기			
CreateAlias	플릿에 대한 새 별칭을 정의합니다.	쓰기		aws:RequestTag/ ${TagKey} (p. 1182)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1182)	
CreateBuild	Amazon S3 버킷에 저장된 파일을 사용하여 새 게임 빌드를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1182) aws:TagKeys (p. 1182)	
CreateFleet	게임 서버를 실행할 새로운 컴퓨팅 리소스 플릿을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1182) aws:TagKeys (p. 1182)	
CreateGameSession	지정된 플릿에서 새 게임 세션을 시작합니다.	쓰기			
CreateGameSessionQueue	새 게임 세션 배치 요청을 처리하기 위한 새 대기열을 설정합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1182) aws:TagKeys (p. 1182)	
CreateMatchmakingConfiguration	새로운 FlexMatch 매치메이커를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1182) aws:TagKeys (p. 1182)	
CreateMatchmakingRuleSet	FlexMatch에 대한 새 매치메이킹 규칙 세트를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1182) aws:TagKeys (p. 1182)	
CreatePlayerSession	플레이어에 사용할 수 있는 게임 세션 슬롯을 예약합니다.	쓰기			
CreatePlayerSessions	여러 플레이어에 사용할 수 있는 게임 세션 슬롯을 예약합니다.	쓰기			
CreateScript	새 Realtime 서버 스크립트를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1182) aws:TagKeys (p. 1182)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateVpcPeeringAuthorization	GameLift가 GameLift 플릿 VPC와 다른 AWS 계정의 VPC 간에 피어링 연결을 생성하거나 삭제할 수 있도록 허용합니다.	쓰기			
CreateVpcPeeringConnection	GameLift 플릿 VPC와 다른 계정의 VPC 간에 피어링 연결을 설정합니다.	쓰기			
DeleteAlias	별칭을 삭제합니다.	쓰기	alias* (p. 1181)		
DeleteBuild	게임 빌드를 삭제합니다.	쓰기	build* (p. 1182)		
DeleteFleet	빈 플릿을 삭제합니다.	쓰기	fleet* (p. 1182)		
DeleteGameSessionQueue	기존 게임 세션 대기열을 삭제합니다.	쓰기	gameSessionQueue* (p. 1182)		
DeleteMatchmakingConfiguration	기존 FlexMatch 매치메이커를 삭제합니다.	쓰기	matchmakingConfiguration* (p. 1182)		
DeleteMatchmakingRuleSet	기존 FlexMatch 매치메이킹 규칙 세트를 삭제합니다.	쓰기	matchmakingRuleSet* (p. 1182)		
DeleteScalingPolicy	Auto Scaling 규칙 세트를 삭제합니다.	쓰기	fleet* (p. 1182)		
DeleteScript	Realtime 서버 스크립트를 삭제합니다.	쓰기	script* (p. 1182)		
DeleteVpcPeeringAuthorization	VPC 피어링 승인을 취소합니다.	쓰기			
DeleteVpcPeeringConnection	VPC 간의 피어링 연결을 제거합니다.	쓰기			
DescribeAlias	별칭에 대한 속성을 검색합니다.	Read	alias* (p. 1181)		
DescribeBuild	게임 빌드에 대한 속성을 검색합니다.	Read	build* (p. 1182)		
DescribeEC2InstanceLimits	EC2 인스턴스 유형에 대해 허용되는 최대 사용량 및 현재 사용량을 검색합니다.	Read			
DescribeFleetAttributes	플릿에 대한 상태를 포함한 일반 속성을 검색합니다.	Read			
DescribeFleetCapacity	플릿에 대한 현재 용량 설정을 검색합니다.	Read			
DescribeFleetEvents	플릿의 이벤트 로그에서 항목을 검색합니다.	Read	fleet* (p. 1182)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeFleetPortSettings	플릿에 대한 인바운드 연결 권한을 검색합니다.	Read	fleet* (p. 1182)		
DescribeFleetUtilization	플릿에 대한 사용률 통계를 검색합니다.	Read			
DescribeGameSessionDetails	보호 정책을 포함하여 플릿의 게임 세션에 대한 속성을 검색합니다.	Read			
DescribeGameSessionPlacement	게임 세션 배치 요청의 세부 정보를 검색합니다.	Read			
DescribeGameSessionQueues	게임 세션 대기열의 속성을 검색합니다.	Read			
DescribeGameSessions	플릿의 게임 세션에 대한 속성을 검색합니다.	Read			
DescribeInstances	플릿의 인스턴스에 대한 정보를 검색합니다.	Read	fleet* (p. 1182)		
DescribeMatchmaking	매치메이킹 티켓의 세부 정보를 검색합니다.	Read			
DescribeMatchmakingConfigurations	FlexMatch 매치메이커의 속성을 검색합니다.	Read			
DescribeMatchmakingRuleSets	FlexMatch 매치메이킹 규칙 세트의 속성을 검색합니다.	Read			
DescribePlayerSessions	게임 세션에서 플레이어 세션의 속성을 검색합니다.	Read			
DescribeRuntimeConfiguration	플릿에 대한 현재 실행 시간 구성을 검색합니다.	Read	fleet* (p. 1182)		
DescribeScalingPolicies	플릿에 적용된 모든 조정 정책을 검색합니다.	Read	fleet* (p. 1182)		
DescribeScript	Realtime 서버 스크립트의 속성을 검색합니다.	Read	script* (p. 1182)		
DescribeVpcPeeringAuthorizations	유효한 VPC 피어링 승인을 검색합니다.	Read			
DescribeVpcPeeringConnections	활성 또는 보류 중인 VPC 피어링 연결에 대한 세부 정보를 검색합니다.	Read			
GetGameSessionLogUrl	게임 세션에 대해 저장된 로그의 위치를 검색합니다.	Read			
GetInstanceAccess	지정된 플릿 인스턴스에 대한 원격 액세스를 요청합니다.	Read	fleet* (p. 1182)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListAliases	현재 리전에 정의된 모든 별칭을 검색합니다.	List			
ListBuilds	현재 리전의 모든 게임 빌드를 검색합니다.	List			
ListFleets	현재 리전의 모든 플릿에 대한 플릿 ID 목록을 검색합니다.	List			
ListScripts	현재 리전의 모든 Realtime 서버 스크립트에 대한 속성을 검색합니다.	List			
ListTagsForResource	GameLift 리소스에 대한 태그를 나열합니다.	List	alias (p. 1181)		
			build (p. 1182)		
			fleet (p. 1182)		
			gameSessionQueue (p. 1182)		
			matchmakingConfiguration (p. 1182)		
			matchmakingRuleSet (p. 1182)		
			script (p. 1182)		
PutScalingPolicy	플릿 Auto Scaling 정책을 생성 또는 업데이트합니다.	쓰기	fleet* (p. 1182)		
RequestUploadCredentials	새 게임 빌드를 업로드할 때 사용할 새 업로드 자격 증명을 검색합니다.	Read	build* (p. 1182)		
ResolveAlias	별칭과 연결된 플릿 ID를 검색합니다.	Read	alias* (p. 1181)		
SearchGameSessions	검색 조건 세트와 일치하는 게임 세션을 검색합니다.	Read			
StartFleetActions	StopFleetActions()를 사용하여 일시 중단된 후 플릿에 대한 Auto Scaling 활동을 다시 시작합니다.	쓰기	fleet* (p. 1182)		
StartGameSessionPlacement	게임 세션 배치 요청을 게임 세션 대기열로 보냅니다.	쓰기	gameSessionQueue* (p. 1182)		
StartMatchBackfill	FlexMatch 매치메이킹을 요청하여 기존 게임 세션에서 사용 가능한 플레이어 슬롯을 채웁니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartMatchmaking	플레이어 한 명 또는 한 그룹에 대해 FlexMatch 매치메이킹을 요청하고, 결과 매치를 위한 게임 세션 배치를 요청합니다.	쓰기			
StopFleetActions	플릿에서 Auto Scaling 활동을 일시 중단합니다.	쓰기	fleet* (p. 1182)		
StopGameSessionPlacement	진행 중인 게임 세션 배치 요청을 취소합니다.	쓰기			
StopMatchmaking	진행 중인 매치메이킹 또는 매치 채우기 요청을 취소합니다.	쓰기			
TagResource	GameLift 리소스의 태그를 지정합니다.	태그 지정	alias (p. 1181)		
			build (p. 1182)		
			fleet (p. 1182)		
			gameSessionQueue (p. 1182)		
			matchmakingConfiguration (p. 1182)		
			matchmakingRuleSet (p. 1182)		
			script (p. 1182)		
				aws:RequestTag/${TagKey} (p. 1182) aws:TagKeys (p. 1182)	
UntagResource	GameLift 리소스의 태그 지정을 해제합니다.	태그 지정	alias (p. 1181)		
			build (p. 1182)		
			fleet (p. 1182)		
			gameSessionQueue (p. 1182)		
			matchmakingConfiguration (p. 1182)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			matchmakingRuleSet (p. 1182)		
			script (p. 1182)		
				aws:TagKeys (p. 1182)	
UpdateAlias	기존 별칭의 속성을 업데이트합니다.	쓰기	alias* (p. 1181)		
UpdateBuild	기존 빌드의 메타데이터를 업데이트합니다.	쓰기	build* (p. 1182)		
UpdateFleetAttributes	기존 플릿의 일반 속성을 업데이트합니다.	쓰기	fleet* (p. 1182)		
UpdateFleetCapacity	플릿의 용량 설정을 조정합니다.	쓰기	fleet* (p. 1182)		
UpdateFleetPortSettings	플릿의 포트 설정을 조정합니다.	쓰기	fleet* (p. 1182)		
UpdateGameSession	기존 게임 세션의 속성을 업데이트합니다.	쓰기			
UpdateGameSessionQueue	기존 게임 세션 대기열의 속성을 업데이트합니다.	쓰기	gameSessionQueue* (p. 1182)		
UpdateMatchmakingConfiguration	기존 FlexMatch 매치메이킹 구성의 속성을 업데이트합니다.	쓰기	matchmakingConfiguration* (p. 1182)		
UpdateRuntimeConfiguration	기존 플릿의 인스턴스에서 서버 프로세스가 구성되는 방식을 업데이트합니다.	쓰기	fleet* (p. 1182)		
UpdateScript	기존 Realtime 서버 스크립트의 메타데이터 및 콘텐츠를 업데이트합니다.	쓰기	script* (p. 1182)		
ValidateMatchmakingRuleSet	FlexMatch 매치메이킹 규칙 세트의 구문을 검증합니다.	Read			

Amazon GameLift에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1175)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
alias	`arn:${Partition}:gamelift:${Region}::alias/${AliasId}`	aws:ResourceTag/${TagKey} (p. 1182)

리소스 유형	ARN	조건 키
build	`arn:${Partition}:gamelift:${Region}:${AccountId}:build/${BuildId}`	aws:ResourceTag/${TagKey} (p. 1182)
script	`arn:${Partition}:gamelift:${Region}:${AccountId}:script/${ScriptId}`	aws:ResourceTag/${TagKey} (p. 1182)
fleet	`arn:${Partition}:gamelift:${Region}:${Account}:fleet/${FleetId}`	aws:ResourceTag/${TagKey} (p. 1182)
gameSessionQueue	`arn:${Partition}:gamelift:${Region}:${Account}:gamesessionqueue/${GameSessionQueueName}`	aws:ResourceTag/${TagKey} (p. 1182)
matchmakingConfiguration	`arn:${Partition}:gamelift:${Region}:${Account}:matchmakingconfiguration/${MatchmakingConfigurationName}`	aws:ResourceTag/${TagKey} (p. 1182)
matchmakingRuleSet	`arn:${Partition}:gamelift:${Region}:${Account}:matchmakingruleset/${MatchmakingRuleSetName}`	aws:ResourceTag/${TagKey} (p. 1182)

Amazon GameLift의 조건 키

Amazon GameLift는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에서 전달되는 태그를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에서 전달되는 태그 키를 기준으로 작업을 필터링합니다.	문자열

Amazon Glacier에 사용되는 작업, 리소스 및 조건 키

Amazon Glacier(서비스 접두사: `glacier`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Glacier에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AbortMultipartUpload	멀티파트 업로드를 업로드 ID로 식별하여 중단합니다	쓰기	vault* (p. 1185)		
AbortVaultLock	볼트 잠금이 Locked 상태가 아닐 경우 볼트 잠금 프로세스를 중단합니다.	권한 관리	vault* (p. 1185)		
AddTagsToVault	볼트에 지정된 태그를 추가합니다.	태그 지정	vault* (p. 1185)		
CompleteMultipartUpload	멀티파트 업로드 프로세스를 완료합니다	쓰기	vault* (p. 1185)		
CompleteVaultLock	볼트 잠금 프로세스를 완료합니다.	권한 관리	vault* (p. 1185)		
CreateVault	지정된 이름으로 새로운 볼트를 생성합니다.	쓰기	vault* (p. 1185)		
DeleteArchive	볼트에서 아카이브를 삭제합니다.	쓰기	vault* (p. 1185)		
				glacier:ArchiveAgeInDays (p. 1185)	
DeleteVault	볼트를 삭제합니다.	쓰기	vault* (p. 1185)		
DeleteVaultAccessPolicy	지정된 볼트와 연결된 액세스 정책을 삭제합니다.	권한 관리	vault* (p. 1185)		
DeleteVaultNotifications	볼트에 설정되어 있는 알림 구성을 삭제합니다	쓰기	vault* (p. 1185)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeJob	이전에 시작한 작업에 대한 정보를 반환합니다.	Read	vault* (p. 1185)		
DescribeVault	볼트에 대한 정보를 반환합니다.	Read	vault* (p. 1185)		
GetDataRetrievalPolicy	GET 요청에 지정된 계정 및 리전의 현재 데이터 가져오기 정책을 반환합니다.	Read			
GetJobOutput	시작한 작업의 출력을 다운로드합니다.	Read	vault* (p. 1185)		
GetVaultAccessPolicy	볼트에 설정되어 있는 액세스 정책 하위 리소스를 가져옵니다.	Read	vault* (p. 1185)		
GetVaultLock	지정된 볼트에 설정되어 있는 잠금 정책 하위 리소스에서 속성을 가져옵니다.	Read	vault* (p. 1185)		
GetVaultNotifications	볼트에 설정되어 있는 알림 구성 하위 리소스를 가져옵니다.	Read	vault* (p. 1185)		
InitiateJob	지정된 유형의 작업을 시작합니다.	쓰기	vault* (p. 1185)		
				glacier:ArchiveAgeInDays (p. 1185)	
InitiateMultipartUpload	멀티파트 업로드를 시작합니다.	쓰기	vault* (p. 1185)		
InitiateVaultLock	볼트 잠금 프로세스를 시작합니다.	권한 관리	vault* (p. 1185)		
ListJobs	진행 중인 볼트에 대한 작업과 최근에 마친 작업을 나열합니다.	List	vault* (p. 1185)		
ListMultipartUploads	지정된 볼트에 대해 진행 중인 멀티파트 업로드를 나열합니다.	List	vault* (p. 1185)		
ListParts	특정 멀티파트 업로드에서 업로드된 아카이브의 파트를 나열합니다.	List	vault* (p. 1185)		
ListProvisionedCapacity	이번 작업에서는 지정한 AWS 계정에서 프로비저닝된 용량을 나열합니다.	List			
ListTagsForVault	볼트에 연결된 모든 태그를 나열합니다.	List	vault* (p. 1185)		
ListVaults	모든 볼트를 나열합니다.	List			
PurchaseProvisionedCapacity	이번 작업에서는 AWS 계정에 프로비저닝된 용량 단위를 구매합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RemoveTagsFromVault	볼트에 연결된 태그 집합에서 하나 이상의 태그를 제거합니다.	태그 지정	vault* (p. 1185)		
SetDataRetrievalPolicy	PUT 요청에 지정된 리전의 데이터 가져오기 정책을 설정한 후 규정합니다.	권한 관리			
SetVaultAccessPolicy	볼트에 대한 액세스 정책을 구성하여 기존 정책을 덮어씁니다.	권한 관리	vault* (p. 1185)		
SetVaultNotifications	볼트 알림을 구성합니다.	쓰기	vault* (p. 1185)		
UploadArchive	아카이브를 볼트에 추가합니다	쓰기	vault* (p. 1185)		
UploadMultipartPart	아카이브 파트를 업로드합니다	쓰기	vault* (p. 1185)		

Amazon Glacier에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1183)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
vault	`arn:${Partition}:glacier:${Region}:${Account}:vaults/${VaultName}`	

Amazon Glacier에 사용되는 조건 키

Amazon Glacier는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
glacier:ArchiveAgeInDays	아카이브가 볼트에 저장된 기간(일).	문자열
glacier:ResourceTag/	고객 정의 태그.	문자열

AWS Global Accelerator에 사용되는 작업, 리소스 및 조건 키

AWS Global Accelerator(서비스 접두사: `globalaccelerator`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Global Accelerator에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AdvertiseByoipCidr	고유 IP 주소 가져오기(BYOIP)를 통해 액셀러레이터와 함께 사용하도록 프로비저닝되는 IPv4 주소 범위를 공급합니다.	쓰기			
CreateAccelerator	액셀러레이터를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1188) aws:TagKeys (p. 1188)	
CreateEndpointGroup	엔드포인트 그룹을 추가합니다.	쓰기	listener* (p. 1188)		
CreateListener	리스너를 추가합니다.	쓰기	accelerator* (p. 1188)		
DeleteAccelerator	액셀러레이터를 삭제합니다.	쓰기	accelerator* (p. 1188)		
DeleteEndpointGroup	엔드포인트 그룹을 삭제합니다.	쓰기	endpointgroup* (p. 1188)		
DeleteListener	리스너를 삭제합니다.	쓰기	listener* (p. 1188)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeprovisionByoipCidr	고유 IP 주소 가져오기(BYOIP)를 통해 액셀러레이터와 함께 사용하도록 프로비저닝한 지정된 주소 범위를 해제하고 해당 주소 풀을 삭제합니다.	쓰기			
DescribeAccelerator	액셀러레이터를 설명합니다.	Read	accelerator* (p. 1188)		
DescribeAcceleratorAttributes	액셀러레이터 속성을 설명합니다.	Read	accelerator* (p. 1188)		
DescribeEndpointGroup	엔드포인트 그룹을 설명합니다.	Read	endpointgroup* (p. 1188)		
DescribeListener	리스너를 설명합니다.	Read	listener* (p. 1188)		
ListAccelerators	액셀러레이터를 나열합니다.	List			
ListByoipCidrs	byoip cidrs를 나열합니다.	List			
ListEndpointGroups	엔드포인트 그룹을 나열합니다.	List	listener* (p. 1188)		
ListListeners	리스너를 나열합니다.	List	accelerator* (p. 1188)		
ListTagsForResource	globalaccelerator 리소스에 대한 태그를 나열합니다.	Read	accelerator (p. 1188)		
ProvisionByoipCidr	고유 IP 주소 가져오기(BYOIP)를 통해 액셀러레이터와 함께 사용할 주소 범위를 프로비저닝하고 해당 주소 풀을 생성합니다.	쓰기			
TagResource	globalaccelerator 리소스에 태그를 추가합니다.	태그 지정	accelerator (p. 1188)		
				aws:RequestTag/${TagKey} (p. 1188) aws:TagKeys (p. 1188)	
UntagResource	globalaccelerator 리소스에서 태그를 제거합니다.	태그 지정	accelerator (p. 1188)		
				aws:TagKeys (p. 1188)	
UpdateAccelerator	액셀러레이터를 업데이트합니다.	쓰기	accelerator* (p. 1188)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateAcceleratorAttributes	액셀러레이터 속성을 업데이트합니다.	쓰기	accelerator* (p. 1188)		
UpdateEndpointGroup	엔드포인트 그룹을 업데이트합니다.	쓰기	endpointgroup* (p. 1188)		
UpdateListener	리스너를 업데이트합니다.	쓰기	listener* (p. 1188)		
WithdrawByoipCidr	주소 풀로 프로비저닝된 IPv4 주소 범위의 공급을 중지합니다.	쓰기			

AWS Global Accelerator에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1186)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
accelerator	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${AcceleratorId}`	aws:ResourceTag/${TagKey} (p. 1188)
listener	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${AcceleratorId}/listener/${ListenerId}`	aws:ResourceTag/${TagKey} (p. 1188)
endpointgroup	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${AcceleratorId}/listener/${ListenerId}/endpoint-group/${EndpointGroupId}`	aws:ResourceTag/${TagKey} (p. 1188)

AWS Global Accelerator에 사용되는 조건 키

AWS Global Accelerator는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Glue에 사용되는 작업, 리소스 및 조건 키

AWS Glue(서비스 접두사: `glue`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Glue에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchCreatePartition	하나 이상의 파티션을 생성할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
BatchDeleteConnection	하나 이상의 연결을 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			connection* (p. 1201)		
BatchDeletePartition	하나 이상의 파티션을 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			table* (p. 1201)		
BatchDeleteTable	하나 이상의 테이블을 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
BatchDeleteTableVersion	테이블의 버전을 하나 이상 삭제할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
			tableversion* (p. 1201)		
BatchGetCrawlers	하나 이상의 크롤러를 검색할 수 있는 권한을 부여합니다.	Read			
BatchGetDevEndpoints	하나 이상의 개발 엔드포인트를 검색할 수 있는 권한을 부여합니다.	Read			
BatchGetJobs	하나 이상의 작업을 검색할 수 있는 권한을 부여합니다.	Read			
BatchGetPartition	하나 이상의 파티션을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
BatchGetTriggers	하나 이상의 트리거를 검색할 수 있는 권한을 부여합니다.	Read			
BatchGetWorkflows	하나 이상의 워크플로우를 검색할 수 있는 권한을 부여합니다.	Read			
BatchStopJobRun	작업에 대한 하나 이상의 작업 실행을 중지할 수 있는 권한을 부여합니다.	쓰기			
CancelMLTaskRun	실행 중인 ML 작업 실행을 중지할 수 있는 권한을 부여합니다.	쓰기	mlTransform* (p. 1201)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateClassifier	분류자를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateConnection	연결을 생성할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			connection* (p. 1201)		
CreateCrawler	크롤러를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1201) aws:TagKeys (p. 1202)	
CreateDatabase	데이터베이스를 생성할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
CreateDevEndpoint	개발 엔드포인트를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1201) aws:TagKeys (p. 1202)	
CreateJob	작업을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1201) aws:TagKeys (p. 1202)	
CreateMLTransform	ML 변환을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreatePartition	파티션을 생성할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
CreateScript	스크립트를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateSecurityConfiguration	보안 구성을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateTable	테이블을 생성할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			database* (p. 1201)		
			table* (p. 1201)		
CreateTrigger	트리거를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1201) aws:TagKeys (p. 1202)	
CreateUserDefinedFunction	함수 정의를 생성할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			userdefinedfunction* (p. 1201)		
CreateWorkflow	워크플로우를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1201) aws:TagKeys (p. 1202)	
DeleteClassifier	분류자를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteConnection	연결을 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			connection* (p. 1201)		
DeleteCrawler	크롤러를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteDatabase	데이터베이스를 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
DeleteDevEndpoint	개발 엔드포인트를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteJob	작업을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteMLTransform	ML 변환을 삭제할 수 있는 권한을 부여합니다.	쓰기	mlTransform* (p. 1201)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeletePartition	파티션을 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
DeleteResourcePolicy	리소스 정책을 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
DeleteSecurityConfiguration	보안 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteTable	테이블을 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
DeleteTableVersion	테이블의 버전을 삭제할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
			tableversion* (p. 1201)		
DeleteTrigger	트리거를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteUserDefinedFunction	함수 정의를 삭제할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			userdefinedfunction* (p. 1201)		
DeleteWorkflow	워크플로우를 삭제할 권한을 부여합니다.	쓰기			
GetCatalogImportStatus	카탈로그 가져오기 상태를 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
GetClassifier	분류자를 검색할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetClassifiers	모든 분류자를 나열할 수 있는 권한을 부여합니다.	Read			
GetConnection	연결을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			connection* (p. 1201)		
GetConnections	연결의 목록을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			connection* (p. 1201)		
GetCrawler	크롤러를 검색할 수 있는 권한을 부여합니다.	Read			
GetCrawlerMetrics	크롤러에 대한 지표를 검색할 수 있는 권한을 부여합니다.	Read			
GetCrawlers	모든 크롤러를 검색할 수 있는 권한을 부여합니다.	Read			
GetDataCatalogEncryptionSettings	카탈로그 암호화 설정을 검색할 수 있는 권한을 부여합니다.	Read			
GetDatabase	데이터베이스를 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
GetDatabases	모든 데이터베이스를 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
GetDataflowGraph	스크립트를 DAG(방향성 비순환 그래프)로 변환할 수 있는 권한을 부여합니다.	Read			
GetDevEndpoint	개발 엔드포인트를 검색할 수 있는 권한을 부여합니다.	Read			
GetDevEndpoints	모든 개발 엔드포인트를 검색할 수 있는 권한을 부여합니다.	Read			
GetJob	작업을 검색할 수 있는 권한을 부여합니다.	Read			
GetJobBookmark	작업 북마크를 검색할 수 있는 권한을 부여합니다.	Read			
GetJobRun	작업 실행을 검색할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetJobRuns	작업의 모든 작업 실행을 검색할 수 있는 권한을 부여합니다.	Read			
GetJobs	모든 현재 작업을 검색할 수 있는 권한을 부여합니다.	Read			
GetMLTaskRun	ML 작업 실행을 검색할 수 있는 권한을 부여합니다.	Read	mlTransform* (p. 1201)		
GetMLTaskRuns	모든 ML 작업 실행을 검색할 수 있는 권한을 부여합니다.	List	mlTransform* (p. 1201)		
GetMLTransform	ML 변환을 검색할 수 있는 권한을 부여합니다.	Read	mlTransform* (p. 1201)		
GetMLTransforms	모든 ML 변환을 검색할 수 있는 권한을 부여합니다.	List			
GetMapping	매핑을 생성할 수 있는 권한을 부여합니다.	쓰기			
GetPartition	파티션을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
GetPartitions	테이블의 파티션을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
GetPlan	스크립트의 매핑을 검색할 수 있는 권한을 부여합니다.	Read			
GetResourcePolicy	리소스 정책을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
GetSecurityConfiguration	보안 구성을 검색할 수 있는 권한을 부여합니다.	Read			
GetSecurityConfigurations	하나 이상의 보안 구성을 검색할 수 있는 권한을 부여합니다.	Read			
GetTable	테이블을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			table* (p. 1201)		
GetTableVersion	테이블의 버전을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
			tableversion* (p. 1201)		
GetTableVersions	테이블의 버전 목록을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
			tableversion* (p. 1201)		
GetTables	데이터베이스에서 테이블을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
GetTags	리소스와 연결된 모든 태그를 검색할 수 있는 권한을 부여합니다.	Read	crawler (p. 1201)		
			devendpoint (p. 1201)		
			job (p. 1201)		
			trigger (p. 1201)		
			workflow (p. 1201)		
GetTrigger	트리거를 검색할 수 있는 권한을 부여합니다.	Read			
GetTriggers	작업과 연결된 트리거를 검색할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetUserDefinedFunction	함수 정의를 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			userdefinedfunction* (p. 1201)		
GetUserDefinedFunctions	여러 함수 정의를 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			userdefinedfunction* (p. 1201)		
GetWorkflow	워크플로우를 가져올 수 있는 권한을 부여합니다.	Read			
GetWorkflowRun	워크플로우 실행을 가져올 수 있는 권한을 부여합니다.	Read			
GetWorkflowRunProperties	워크플로우 실행 속성을 가져올 수 있는 권한을 부여합니다.	Read			
GetWorkflowRuns	모든 워크플로우 실행을 가져올 수 있는 권한을 부여합니다.	Read			
ImportCatalogToGlue	Athena 데이터 카탈로그를 AWS Glue로 가져올 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
ListCrawlers	모든 크롤러를 검색할 수 있는 권한을 부여합니다.	List			
ListDevEndpoints	모든 개발 엔드포인트를 검색할 수 있는 권한을 부여합니다.	List			
ListJobs	모든 현재 작업을 검색할 수 있는 권한을 부여합니다.	List			
ListMLTransforms	모든 ML 변환을 검색할 수 있는 권한을 부여합니다.	List			
ListTriggers	모든 트리거를 검색할 수 있는 권한을 부여합니다.	List			
ListWorkflows	모든 워크플로우를 가져올 수 있는 권한을 부여합니다.	List			
PutDataCatalogEncryptionSettings	카탈로그 암호화 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
PutResourcePolicy	리소스 정책을 업데이트할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutWorkflowRunProperties	워크플로우 실행 속성을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
ResetJobBookmark	작업 북마크를 재설정할 수 있는 권한을 부여합니다.	쓰기			
SearchTables	카탈로그에서 테이블을 검색할 수 있는 권한을 부여합니다.	Read	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
StartCrawler	크롤러를 시작할 수 있는 권한을 부여합니다.	쓰기			
StartCrawlerSchedule	크롤러의 예약 상태를 SCHEDULED로 변경할 수 있는 권한을 부여합니다.	쓰기			
StartExportLabelsTaskRun	레이블 내보내기 ML 작업 실행을 시작할 수 있는 권한을 부여합니다.	쓰기	mlTransform* (p. 1201)		
StartImportLabelsTaskRun	레이블 가져오기 ML 작업 실행을 시작할 수 있는 권한을 부여합니다.	쓰기	mlTransform* (p. 1201)		
StartJobRun	작업 실행을 시작할 수 있는 권한을 부여합니다.	쓰기			
StartMLEvaluationTaskRun	평가 ML 작업 실행을 시작할 수 있는 권한을 부여합니다.	쓰기	mlTransform* (p. 1201)		
StartMLLabelingSetGenerationTaskRun	레이블 지정 세트 생성 ML 작업 실행을 시작할 수 있는 권한을 부여합니다.	쓰기	mlTransform* (p. 1201)		
StartTrigger	트리거를 시작할 수 있는 권한을 부여합니다.	쓰기			
StartWorkflowRun	워크플로우 실행을 시작할 수 있는 권한을 부여합니다.	쓰기			
StopCrawler	실행 중인 크롤러를 중지할 수 있는 권한을 부여합니다.	쓰기			
StopCrawlerSchedule	크롤러의 예약 상태를 NOT_SCHEDULED로 변경할 수 있는 권한을 부여합니다.	쓰기			
StopTrigger	트리거를 중지할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
TagResource	리소스에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	crawler (p. 1201)		
			devendpoint (p. 1201)		
			job (p. 1201)		
			trigger (p. 1201)		
			workflow (p. 1201)		
				aws:TagKeys (p. 1202) aws:RequestTag/${TagKey} (p. 1201)	
UntagResource	리소스와 연결된 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	crawler (p. 1201)		
			devendpoint (p. 1201)		
			job (p. 1201)		
			trigger (p. 1201)		
			workflow (p. 1201)		
				aws:TagKeys (p. 1202)	
UpdateClassifier	분류자를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateConnection	연결을 업데이트할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			connection* (p. 1201)		
UpdateCrawler	크롤러를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateCrawlerSchedule	크롤러의 일정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateDatabase	데이터베이스를 업데이트할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			database* (p. 1201)		
UpdateDevEndpoint	개발 엔드포인트를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateJob	작업을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateMLTransform	ML 변환을 업데이트할 수 있는 권한을 부여합니다.	쓰기	mlTransform* (p. 1201)		
UpdatePartition	파티션을 업데이트할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
UpdateTable	테이블을 업데이트할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			table* (p. 1201)		
UpdateTrigger	트리거를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateUserDefinedFunction	함수 정의를 업데이트할 수 있는 권한을 부여합니다.	쓰기	catalog* (p. 1201)		
			database* (p. 1201)		
			userdefinedfunction* (p. 1201)		
UpdateWorkflow	워크플로우를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UseMLTransforms	Glue ETL 스크립트 내에서 ML 변환을 사용할 수 있는 권한을 부여합니다.	쓰기	mlTransform* (p. 1201)		

AWS Glue에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1189)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
catalog	`arn:${Partition}:glue:${Region}:${Account}:catalog/${CatalogName}`	
database	`arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}`	
table	`arn:${Partition}:glue:${Region}:${Account}:table/${TableName}`	
tableversion	`arn:${Partition}:glue:${Region}:${Account}:tableVersion/${TableVersionName}`	
connection	`arn:${Partition}:glue:${Region}:${Account}:connection/${ConnectionName}`	
userdefinedfunction	`arn:${Partition}:glue:${Region}:${Account}:userDefinedFunction/${UserDefinedFunctionName}`	
devendpoint	`arn:${Partition}:glue:${Region}:${Account}:devendpoint/${DevEndpointName}`	aws:ResourceTag/${TagKey} (p. 1201)
job	`arn:${Partition}:glue:${Region}:${Account}:job/${JobName}`	aws:ResourceTag/${TagKey} (p. 1201)
trigger	`arn:${Partition}:glue:${Region}:${Account}:trigger/${TriggerName}`	aws:ResourceTag/${TagKey} (p. 1201)
crawler	`arn:${Partition}:glue:${Region}:${Account}:crawler/${CrawlerName}`	aws:ResourceTag/${TagKey} (p. 1201)
workflow	`arn:${Partition}:glue:${Region}:${Account}:workflow/${WorkflowName}`	aws:ResourceTag/${TagKey} (p. 1201)
mlTransform	`arn:${Partition}:glue:${Region}:${Account}:mlTransform/${TransformId}`	aws:ResourceTag/${TagKey} (p. 1201)

AWS Glue의 조건 키

AWS Glue는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Ground Station에 사용되는 작업, 리소스 및 조건 키

AWS Ground Station(서비스 접두사: `groundstation`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Ground Station에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelContact	접촉을 취소할 수 있는 권한을 부여합니다.	쓰기	Contact* (p. 1205)		
CreateConfig	구성을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1206) aws:TagKeys (p. 1206)	
CreateDataflowEndpointGroup	데이터 흐름 엔드포인트 그룹을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1206)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1206)	
CreateMissionProfile	미션 프로파일을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1206) aws:TagKeys (p. 1206)	
DeleteConfig	구성을 삭제할 수 있는 권한을 부여합니다.	쓰기	Config* (p. 1205)		
DeleteDataflowEndpointGroup	데이터 흐름 엔드포인트 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	DataflowEndpointGroup* (p. 1205)		
DeleteMissionProfile	미션 프로파일을 삭제할 수 있는 권한을 부여합니다.	쓰기	MissionProfile* (p. 1205)		
DescribeContact	접촉을 설명할 수 있는 권한을 부여합니다.	Read	Contact* (p. 1205)		
GetConfig	구성을 반환할 수 있는 권한을 부여합니다.	Read	Config* (p. 1205)		
GetDataflowEndpointGroup	데이터 흐름 엔드포인트 그룹을 반환할 수 있는 권한을 부여합니다.	Read	DataflowEndpointGroup* (p. 1205)		
GetMinuteUsage	분 사용을 반환할 수 있는 권한을 부여합니다.	Read			
GetMissionProfile	미션 프로파일을 검색할 수 있는 권한을 부여합니다.	Read	MissionProfile* (p. 1205)		
GetSatellite	위성에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read	Satellite* (p. 1205)		
ListConfigs	과거 구성의 목록을 반환할 수 있는 권한을 부여합니다.	List			
ListContacts	접촉 목록을 반환할 수 있는 권한을 부여합니다.	List			
ListDataflowEndpointGroups	데이터 흐름 엔드포인트 그룹을 나열할 수 있는 권한을 부여합니다.	List			
ListGroundStations	지상국을 나열할 수 있는 권한을 부여합니다.	List			
ListMissionProfiles	미션 프로파일의 목록을 반환할 수 있는 권한을 부여합니다.	List			
ListSatellites	위성을 나열할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTagsForResource	리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	Config (p. 1205)		
			Contact (p. 1205)		
			DataflowEndpointGroup (p. 1205)		
			MissionProfile (p. 1205)		
ReserveContact	접촉을 예약할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1206) aws:TagKeys (p. 1206)	
TagResource	리소스 태그를 할당할 수 있는 권한을 부여합니다.	태그 지정	Config (p. 1205)		
			Contact (p. 1205)		
			DataflowEndpointGroup (p. 1205)		
			MissionProfile (p. 1205)		
				aws:TagKeys (p. 1206) aws:RequestTag/${TagKey} (p. 1206)	
UntagResource	리소스 태그를 할당 취소할 수 있는 권한을 부여합니다.	태그 지정	Config (p. 1205)		
			Contact (p. 1205)		
			DataflowEndpointGroup (p. 1205)		
			MissionProfile (p. 1205)		
				aws:TagKeys (p. 1206)	
UpdateConfig	구성을 업데이트할 수 있는 권한을 부여합니다.	쓰기	Config* (p. 1205)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateMissionProfile	미션 프로파일을 업데이트할 수 있는 권한을 부여합니다.	쓰기	MissionProfile* (p. 1205)		

AWS Ground Station에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1202)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Config	`arn:${Partition}:groundstation:${Region}:${Account}:config/${configType}/${configId}`	aws:ResourceTag/${TagKey} (p. 1206) groundstation:configId (p. 1206) groundstation:configType (p. 1206)
Contact	`arn:${Partition}:groundstation:${Region}:${Account}:contact/${contactId}`	aws:ResourceTag/${TagKey} (p. 1206) groundstation:contactId (p. 1206)
DataflowEndpointGroup	`arn:${Partition}:groundstation:${Region}:${Account}:dataflow-endpoint-group/${dataflowEndpointGroupId}`	aws:ResourceTag/${TagKey} (p. 1206) groundstation:dataflowEndpointGroupId (p. 1206)
GroundStationResource	`arn:${Partition}:groundstation:${Region}:${Account}:groundstation:${groundStationId}`	groundstation:groundStationId (p. 1206)
MissionProfile	`arn:${Partition}:groundstation:${Region}:${Account}:mission-profile/${missionProfileId}`	aws:ResourceTag/${TagKey} (p. 1206) groundstation:missionProfileId (p. 1206)
Satellite	`arn:${Partition}:groundstation:${Region}:${Account}:satellite/${satelliteId}`	groundstation:satelliteId (p. 1206)

AWS Ground Station에 사용되는 조건 키

AWS Ground Station은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	Ground Station 서비스에 대한 사용자의 요청에 있는 키를 기준으로 액세스를 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	Ground Station 서비스에 대한 사용자의 요청에 있는 모든 태그 키 이름의 목록을 기준으로 액세스를 필터링합니다.	문자열
groundstation:configId	구성의 ID를 기준으로 액세스를 필터링합니다.	문자열
groundstation:configType	구성의 유형을 기준으로 액세스를 필터링합니다.	문자열
groundstation:contactId	연락처의 ID를 기준으로 액세스를 필터링합니다.	문자열
groundstation:dataflowEndpointGroupId	데이터 흐름 엔드포인트 그룹의 ID를 기준으로 액세스를 필터링합니다.	문자열
groundstation:groundStationId	지상국의 ID를 기준으로 액세스를 필터링합니다.	문자열
groundstation:missionProfileId	미션 프로파일의 ID를 기준으로 액세스를 필터링합니다.	문자열
groundstation:satelliteId	위성의 ID를 기준으로 액세스를 필터링합니다.	문자열

Amazon GroundTruth Labeling에 사용되는 작업, 리소스 및 조건 키

Amazon GroundTruth Labeling(서비스 접두사: `groundtruthlabeling`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에서 사용할 수 있는 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon GroundTruth Labeling에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeConsoleJob [권한만 해당]	GroundTruthLabeling 작업의 상태를 가져옵니다.	Read			
ListDatasetObjects [권한만 해당]	매니페스트 파일의 데이터 세트 객체를 나열하는 페이지 매김 목록 API입니다.	Read			
RunFilterOrSampleDataset [권한만 해당]	S3 select를 사용하여 매니페스트 파일에서 레코드를 필터링합니다. 랜덤 샘플링을 기반으로 샘플 항목을 가져옵니다.	쓰기			
RunGenerateManifestByCrawling [권한만 해당]	S3 접두사를 나열하고 해당 위치에서 객체로부터 매니페스트 파일을 생성합니다.	쓰기			

Amazon GroundTruth Labeling에서 정의한 리소스 유형

Amazon GroundTruth Labeling은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon GroundTruth Labeling에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon GroundTruth Labeling에 사용되는 조건 키

GroundTruth Labeling에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon GuardDuty에 사용되는 작업, 리소스 및 조건 키

Amazon GuardDuty(서비스 접두사: `guardduty`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon GuardDuty에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptInvitation	GuardDuty 멤버 계정으로의 초대를 수락할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
ArchiveFindings	GuardDuty 결과를 보관할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
CreateDetector	탐지기를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1213) aws:TagKeys (p. 1214)	
CreateFilter	GuardDuty 필터를 생성할 수 있는 권한을 부여합니다. 필터는 결과를 필터링하는 데 사용되는 결과 속성과 조건을 정의합니다.	쓰기	detector* (p. 1213)		
				aws:RequestTag/${TagKey} (p. 1213) aws:TagKeys (p. 1214)	
CreateIPSet	IPSet를 생성할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
				aws:RequestTag/${TagKey} (p. 1213) aws:TagKeys (p. 1214)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateMembers	GuardDuty 멤버 계정을 생성할 수 있는 권한을 부여합니다. 멤버를 생성하는 데 사용된 계정이 GuardDuty 마스터 계정이 됩니다.	쓰기	detector* (p. 1213)		
CreatePublishingDestination	게시 대상을 생성할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		s3:GetObject s3:ListBucket
CreateSampleFindings	샘플 결과를 생성할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
CreateThreatIntelSet	GuardDuty ThreatIntelSet를 생성할 수 있는 권한을 부여합니다. ThreatIntelSet는 GuardDuty가 결과를 생성하는 데 사용하는 알려진 악성 IP 주소로 구성됩니다.	쓰기	detector* (p. 1213)		
				aws:RequestTag/${TagKey} (p. 1213) aws:TagKeys (p. 1214)	
DeclineInvitations	GuardDuty 멤버 계정으로의 초대를 거부할 수 있는 권한을 부여합니다.	쓰기			
DeleteDetector	GuardDuty 탐지기를 삭제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
DeleteFilter	GuardDuty 필터를 삭제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
			filter* (p. 1213)		
DeleteIPSet	GuardDuty IPSet를 삭제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
			ipset* (p. 1213)		
DeleteInvitations	GuardDuty 멤버 계정으로의 초대를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteMembers	GuardDuty 멤버 계정을 삭제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
DeletePublishingDestination	게시 대상을 삭제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
			publishingdestination* (p. 1213)		
DeleteThreatIntelSet	GuardDuty ThreatIntelSet를 삭제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			threatintelset* (p. 1213)		
DescribePublishingDestination	게시 대상에 대한 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
			publishingdestination* (p. 1213)		
DisassociateFromMasterAccount	GuardDuty 마스터 계정에서 GuardDuty 멤버 계정을 연결 해제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
DisassociateMembers	GuardDuty 마스터 계정에서 GuardDuty 멤버 계정을 연결 해제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
GetDetector	GuardDuty 탐지기를 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
GetFilter	GuardDuty 필터를 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
			filter* (p. 1213)		
GetFindings	GuardDuty 결과를 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
GetFindingsStatistics	GuardDuty 결과 통계 목록을 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
GetIPSet	GuardDuty IPSet를 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
			ipset* (p. 1213)		
GetInvitationsCount	지정된 계정으로 전송된 모든 GuardDuty 초대의 수를 검색할 수 있는 권한을 부여합니다. 수락된 초대는 포함되지 않습니다.	Read			
GetMasterAccount	멤버 계정과 연결된 GuardDuty 마스터 계정의 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
GetMembers	마스터 계정과 연결된 멤버 계정을 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
GetThreatIntelSet	GuardDuty ThreatIntelSet를 검색할 수 있는 권한을 부여합니다.	Read	detector* (p. 1213)		
			threatintelset* (p. 1213)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
InviteMembers	GuardDuty를 활성화하고 다른 AWS 계정을 GuardDuty 멤버 계정으로 초대할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
ListDetectors	GuardDuty 탐지기 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListFilters	GuardDuty 필터 목록을 검색할 수 있는 권한을 부여합니다.	List	detector* (p. 1213)		
ListFindings	GuardDuty 결과 목록을 검색할 수 있는 권한을 부여합니다.	List	detector* (p. 1213)		
ListInvitations	AWS 계정으로 전송된 모든 GuardDuty 멤버십 초대의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListMembers	마스터 계정과 연결된 GuardDuty 멤버 계정의 목록을 검색할 수 있는 권한을 부여합니다.	List	detector* (p. 1213)		
ListPublishingDestinations	게시 대상 목록을 검색할 수 있는 권한을 부여합니다.	List	detector* (p. 1213)		
ListTagsForResource	GuardDuty 리소스와 연결된 태그 목록을 검색할 수 있는 권한을 부여합니다.	List	detector (p. 1213)		
			filter (p. 1213)		
			ipset (p. 1213)		
			threatintelset (p. 1213)		
ListThreatIntelSets	GuardDuty ThreatIntelSet 목록을 검색할 수 있는 권한을 부여합니다.	List	detector* (p. 1213)		
StartMonitoringMembers	마스터 계정에 GuardDuty 멤버 계정의 결과를 모니터링할 수 있는 권한을 부여합니다. StopMonitoringMembers 작업을 사용하여 멤버 계정의 모니터링을 비활성화한 후 사용합니다.	쓰기	detector* (p. 1213)		
StopMonitoringMembers	멤버 계정의 결과 모니터링을 비활성화할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
TagResource	GuardDuty 리소스에 태그를 추가할 수 있는 권한을 부여합니다. 리소스당 태그는 50개로 제한됩니다.	쓰기	detector (p. 1213)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			filter (p. 1213)		
			ipset (p. 1213)		
			threatintelset (p. 1213)		
				aws:RequestTag/${TagKey} (p. 1213) aws:TagKeys (p. 1214)	
UnarchiveFindings	GuardDuty 결과를 보관 해제할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
UntagResource	GuardDuty 리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	쓰기	detector (p. 1213)		
			filter (p. 1213)		
			ipset (p. 1213)		
			threatintelset (p. 1213)		
				aws:TagKeys (p. 1214)	
UpdateDetector	GuardDuty 탐지기를 업데이트할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
UpdateFilter	GuardDuty 필터를 업데이트할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
			filter* (p. 1213)		
UpdateFindingsFeedback	GuardDuty 결과를 유용하거나 유용하지 않음으로 표시하기 위해 결과 피드백을 업데이트할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
UpdateIPSet	GuardDuty IPSet를 업데이트할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
			ipset* (p. 1213)		
UpdatePublishingDestination	게시 대상을 업데이트할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		s3:GetObject s3:ListBucket

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			publishingdestination* (p. 1213)		
UpdateThreatIntelSet	GuardDuty ThreatIntelSet를 업데이트할 수 있는 권한을 부여합니다.	쓰기	detector* (p. 1213)		
			threatintelset* (p. 1213)		

Amazon GuardDuty에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1208)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
detector	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}`	aws:ResourceTag/${TagKey} (p. 1214)
filter	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/filter/${FilterName}`	aws:ResourceTag/${TagKey} (p. 1214)
ipset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/ipset/${IPSetId}`	aws:ResourceTag/${TagKey} (p. 1214)
threatintelset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${ThreatIntelSetId}`	aws:ResourceTag/${TagKey} (p. 1214)
publishingdestination	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${PublishingDestinationId}`	

Amazon GuardDuty에 사용되는 조건 키

Amazon GuardDuty는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Health API 및 알림에 사용되는 작업, 리소스 및 조건 키

AWS Health APIs and Notifications(서비스 접두사: `health`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Health API 및 알림에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeAffectedAccountsForOrganization	조직에서 지정된 이벤트의 영향을 받은 계정의 목록을 가져옵니다.	Read			organizations:ListAccount
DescribeAffectedEntities	지정된 이벤트의 영향을 받는 개체의 목록을 가져옵니다.	Read	event* (p. 1216)		
				health:eventTypeCode (p. 1216)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				health:service (p. 1216)	
DescribeAffectedEntitiesForOrganization	조직의 지정된 이벤트 및 계정의 영향을 받은 엔터티의 목록을 가져옵니다.	Read			organizations:ListAccount
DescribeEntityAggregates	지정된 각 이벤트의 영향을 받는 개체 수를 반환합니다.	Read			
DescribeEventAggregates	각 이벤트 유형(문제, 예약된 변경 및 계정 알림)의 이벤트 수를 반환합니다.	Read			
DescribeEventDetails	하나 이상의 지정된 이벤트에 대한 세부적인 정보를 반환합니다.	Read	event* (p. 1216)		
				health:eventTypeCode (p. 1216) health:service (p. 1216)	
DescribeEventDetailsForOrganization	조직에서 제공된 계정에 대해 하나 이상의 지정된 이벤트에 대한 상세 정보를 반환합니다.	Read			organizations:ListAccount
DescribeEventTypes	지정된 필터 기준에 맞는 이벤트 유형을 반환합니다.	Read			
DescribeEvents	지정된 필터 기준에 맞는 이벤트에 대한 정보를 반환합니다.	Read			
DescribeEventsForOrganization	조직의 지정된 필터 기준에 맞는 이벤트에 대한 정보를 반환합니다.	Read			organizations:ListAccount
DescribeHealthServiceAccessStatusForOrganization	조직 보기 기능의 활성화 또는 비활성화 상태를 반환합니다.	권한 관리			organizations:ListAccount
DisableHealthServiceAccessForOrganization	조직 보기 기능을 비활성화합니다.	권한 관리			organizations:DisableAWS organizations:ListAccount
EnableHealthServiceAccessForOrganization	조직 보기 기능을 활성화합니다.	권한 관리			iam:CreateServiceLinkedI organizations:EnableAWS organizations:ListAccount

AWS Health APIs and Notifications에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1214)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
event	`arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*`	

AWS Health API 및 알림에 사용되는 조건 키

AWS Health APIs and Notifications는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
health:eventTypeCode	이벤트의 유형입니다.	문자열
health:service	이벤트의 서비스입니다.	문자열

IAM Access Analyzer에 사용되는 작업, 리소스 및 조건 키

IAM Access Analyzer(서비스 접두사: `access-analyzer`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

IAM Access Analyzer에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateAnalyzer	분석기를 생성할 수 있는 권한을 부여합니다.	쓰기	Analyzer* (p. 1219)		
				aws:RequestTag/${TagKey} (p. 1219) aws:TagKeys (p. 1219)	
CreateArchiveRule	지정된 분석기에 대한 아카이브 규칙을 생성할 수 있는 권한을 부여합니다.	쓰기	Analyzer* (p. 1219)		
			ArchiveRule* (p. 1219)		
DeleteAnalyzer	지정된 분석기를 삭제할 수 있는 권한을 부여합니다.	쓰기	Analyzer* (p. 1219)		
				aws:RequestTag/${TagKey} (p. 1219) aws:TagKeys (p. 1219)	
DeleteArchiveRule	지정된 분석기의 아카이브 규칙을 삭제할 수 있는 권한을 부여합니다.	쓰기	Analyzer* (p. 1219)		
			ArchiveRule* (p. 1219)		
GetAnalyzedResource	분석된 리소스에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read			
GetAnalyzer	분석기에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	Analyzer* (p. 1219)		
				aws:RequestTag/${TagKey} (p. 1219) aws:TagKeys (p. 1219)	
GetArchiveRule	지정된 분석기의 아카이브 규칙에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	Analyzer* (p. 1219)		
			ArchiveRule* (p. 1219)		
GetFinding	결과를 검색할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListAnalyzedResources	분석된 리소스 목록을 검색할 수 있는 권한을 부여합니다.	Read			
ListAnalyzers	분석기 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListArchiveRules	분석기에서 아카이브 규칙 목록을 검색할 수 있는 권한을 부여합니다.	List	Analyzer* (p. 1219)		
ListFindings	분석기에서 결과 목록을 검색할 수 있는 권한을 부여합니다.	Read			
ListTagsForResource	리소스에 적용된 태그 목록을 검색할 수 있는 권한을 부여합니다.	Read	Analyzer (p. 1219)		
StartResourceScan	리소스에 적용된 정책에 대한 스캔을 시작할 수 있는 권한을 부여합니다.	쓰기			
TagResource	리소스에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	Analyzer (p. 1219)		
				aws:RequestTag/${TagKey} (p. 1219) aws:TagKeys (p. 1219)	
UntagResource	리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	Analyzer (p. 1219)		
				aws:RequestTag/${TagKey} (p. 1219) aws:TagKeys (p. 1219)	
UpdateArchiveRule	아카이브 규칙을 수정할 수 있는 권한을 부여합니다.	쓰기	Analyzer* (p. 1219)		
			ArchiveRule* (p. 1219)		
UpdateFindings	결과를 수정할 수 있는 권한을 부여합니다.	쓰기			

IAM Access Analyzer에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1216)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Analyzer	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${analyzerName}`	aws:ResourceTag/${TagKey} (p. 1219)
ArchiveRule	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${analyzerName}/archive-rule/${ruleName}`	

IAM Access Analyzer의 조건 키

IAM Access Analyzer는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Identity And Access Management에 사용되는 작업, 리소스 및 조건 키

Identity And Access Management(서비스 접두사: `iam`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Identity And Access Management에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddClientIDToOpenIDConnectProvider	지정된 IAM OpenID Connect(OIDC) 공급자 리소스에 대해 등록된 ID 목록에 새 클라이언트 ID(대상)를 추가할 권한을 부여합니다.	쓰기	oidc-provider* (p. 1231)		
AddRoleToInstanceProfile	IAM 역할을 지정된 인스턴스 프로파일에 추가하는 권한을 부여합니다.	쓰기	instance-profile* (p. 1231)		
AddUserToGroup	IAM 사용자를 지정된 인스턴스 프로파일에 추가하는 권한을 부여합니다.	쓰기	group* (p. 1231)		
AttachGroupPolicy	관리형 정책을 지정된 IAM 그룹에 연결하는 권한을 부여합니다.	권한 관리	group* (p. 1231)		
				iam:PolicyARN (p. 1232)	
AttachRolePolicy	관리형 정책을 지정된 IAM 역할에 연결하는 권한을 부여합니다.	권한 관리	role* (p. 1231)		
				iam:PolicyARN (p. 1232) iam:PermissionsBoundary (p. 1232)	
AttachUserPolicy	관리형 정책을 지정된 IAM 사용자에게 연결하는 권한을 부여합니다.	권한 관리	user* (p. 1232)		
				iam:PolicyARN (p. 1232) iam:PermissionsBoundary (p. 1232)	
ChangePassword	IAM 사용자가 자체 암호를 변경할 권한을 부여합니다.	쓰기	user* (p. 1232)		
CreateAccessKey	지정된 IAM 사용자에게 액세스 키 및 보안 액세스 키를 생성할 수 있는 권한을 부여합니다.	쓰기	user* (p. 1232)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateAccountAlias	AWS 계정에 대한 별칭을 생성할 권한을 부여합니다.	쓰기			
CreateGroup	새 그룹을 생성할 권한을 부여합니다.	쓰기	group* (p. 1231)		
CreateInstanceProfile	새 인스턴스 프로파일을 생성할 권한을 부여합니다.	쓰기	instance-profile* (p. 1231)		
CreateLoginProfile	지정된 IAM 사용자에 대한 암호를 생성할 권한을 부여합니다.	쓰기	user* (p. 1232)		
CreateOpenIDConnectProvider	OpenID Connect(OIDC)를 지원하는 자격 증명 공급자(IdP)를 설명하는 IAM 리소스를 생성할 권한을 부여합니다.	쓰기	oidc-provider* (p. 1231)		
CreatePolicy	새 관리형 정책을 생성할 권한을 부여합니다.	권한 관리	policy* (p. 1231)		
CreatePolicyVersion	지정된 관리형 정책의 새 버전을 생성할 권한을 부여합니다.	권한 관리	policy* (p. 1231)		
CreateRole	새 역할을 생성할 권한을 부여합니다.	쓰기	role* (p. 1231)		
				iam:PermissionsBoundary (p. 1232)	
CreateSAMLProvider	SAML 2.0을 지원하는 자격 증명 공급자(IdP)를 설명하는 IAM 리소스를 생성할 권한을 부여합니다.	쓰기	saml-provider* (p. 1231)		
CreateServiceLinkedRole	AWS 서비스가 대신 작업을 수행할 수 있도록 허용하는 IAM 역할을 생성할 권한을 부여합니다.	쓰기	role* (p. 1231)		
				iam:AWSServiceName (p. 1232)	
CreateServiceSpecificCredential	IAM 사용자에 대한 새 서비스별 자격 증명을 생성할 권한을 부여합니다.	쓰기	user* (p. 1232)		
CreateUser	새 IAM 사용자를 생성할 권한을 부여합니다.	쓰기	user* (p. 1232)		
				iam:PermissionsBoundary (p. 1232)	
CreateVirtualMFADevice	새 가상 MFA 디바이스를 생성할 권한을 부여합니다.	쓰기	mfa* (p. 1231)		
DeactivateMFADevice	지정된 MFA 디바이스를 비활성화하고 원래 활성화된 IAM 사용자와의 연결을 제거할 권한을 부여합니다.	쓰기	user* (p. 1232)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteAccessKey	지정된 IAM 사용자와 연결된 액세스 키 페어를 삭제할 권한을 부여합니다.	쓰기	user* (p. 1232)		
DeleteAccountAlias	지정된 AWS 계정 별칭을 삭제할 권한을 부여합니다.	쓰기			
DeleteAccountPasswordPolicy	AWS 계정에 대한 암호 정책을 제거할 권한을 부여합니다.	권한 관리			
DeleteGroup	지정된 IAM 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1231)		
DeleteGroupPolicy	그룹에서 지정된 IAM 인라인 정책을 삭제할 권한을 부여합니다.	권한 관리	group* (p. 1231)		
DeleteInstanceProfile	지정된 인스턴스 프로파일을 삭제할 권한을 부여합니다.	쓰기	instance-profile* (p. 1231)		
DeleteLoginProfile	지정된 IAM 사용자에 대한 암호를 삭제할 권한을 부여합니다.	쓰기	user* (p. 1232)		
DeleteOpenIDConnectProvider	IAM에서 OpenID Connect 자격 증명 공급자(IdP) 리소스 객체를 삭제할 권한을 부여합니다.	쓰기	oidc-provider* (p. 1231)		
DeletePolicy	지정된 관리형 정책을 삭제하고 정책이 연결된 IAM 엔터티(사용자, 그룹 또는 역할)로부터 정책을 제거할 권한을 부여합니다.	권한 관리	policy* (p. 1231)		
DeletePolicyVersion	지정된 관리형 정책에서 버전을 삭제할 권한을 부여합니다.	권한 관리	policy* (p. 1231)		
DeleteRole	지정된 역할을 삭제할 권한을 부여합니다.	쓰기	role* (p. 1231)		
DeleteRolePermissionsBoundary	역할로부터 권한 경계를 제거할 권한을 부여합니다.	권한 관리	role* (p. 1231)		
				iam:PermissionsBoundary (p. 1232)	
DeleteRolePolicy	지정된 역할에서 지정된 IAM 인라인 정책을 삭제할 권한을 부여합니다.	권한 관리	role* (p. 1231)		
				iam:PermissionsBoundary (p. 1232)	
DeleteSAMLProvider	IAM에서 SAML 공급자 리소스를 삭제할 권한을 부여합니다.	쓰기	saml-provider* (p. 1231)		
DeleteSSHPublicKey	지정된 SSH 퍼블릭 키를 삭제할 권한을 부여합니다.	쓰기	user* (p. 1232)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteServerCertificate	지정된 서버 자격 증명을 삭제할 권한을 부여합니다.	쓰기	server-certificate* (p. 1231)		
DeleteServiceLinkedRole	서비스에서 더 이상 사용하지 않는 경우 특정 AWS 서비스와 연결된 IAM 역할을 삭제할 권한을 부여합니다.	쓰기	role* (p. 1231)		
DeleteServiceSpecificCredential	IAM 사용자에 대해 지정된 서비스별 자격 증명을 삭제할 권한을 부여합니다.	쓰기	user* (p. 1232)		
DeleteSigningCertificate	지정된 IAM 사용자와 연결된 서명 인증서를 삭제할 권한을 부여합니다.	쓰기	user* (p. 1232)		
DeleteUser	지정된 IAM 사용자를 삭제할 권한을 부여합니다.	쓰기	user* (p. 1232)		
DeleteUserPermissionsBoundary	지정된 IAM 사용자로부터 권한 경계를 제거할 권한을 부여합니다.	권한 관리	user* (p. 1232)		
				iam:PermissionsBoundary (p. 1232)	
DeleteUserPolicy	IAM 사용자로부터 지정된 IAM 인라인 정책을 삭제할 권한을 부여합니다.	권한 관리	user* (p. 1232)		
				iam:PermissionsBoundary (p. 1232)	
DeleteVirtualMFADevice	가상 MFA 디바이스를 삭제할 권한을 부여합니다.	쓰기	mfa (p. 1231)		
			sms-mfa (p. 1232)		
DetachGroupPolicy	지정된 IAM 그룹에서 관리형 정책을 분리하는 권한을 부여합니다.	권한 관리	group* (p. 1231)		
				iam:PolicyARN (p. 1232)	
DetachRolePolicy	지정된 역할에서 관리형 정책을 분리하는 권한을 부여합니다.	권한 관리	role* (p. 1231)		
				iam:PolicyARN (p. 1232) iam:PermissionsBoundary (p. 1232)	
DetachUserPolicy	지정된 IAM 사용자로부터 관리형 정책을 분리하는 권한을 부여합니다.	권한 관리	user* (p. 1232)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				iam:PolicyARN (p. 1232) iam:PermissionsBoundary (p. 1232)	
EnableMFADevice	MFA 디바이스를 활성화하고 지정된 IAM 사용자와 연결할 권한을 부여합니다.	쓰기	user* (p. 1232)		
GenerateCredentialReport	AWS 계정에 대한 자격 증명 보고서를 생성할 권한을 부여합니다.	Read			
GenerateOrganizationsAccessReport	AWS Organizations 엔터티에 대한 액세스 보고서를 생성할 권한을 부여합니다.	Read	access-report* (p. 1231)		organizations:DescribePo organizations:ListChildren organizations:ListParents organizations:ListPoliciesl organizations:ListRoots organizations:ListTargetsl
				iam:OrganizationsPolicyId (p. 1232)	
GenerateServiceLastAccessedDetails	IAM 리소스에 대해 서비스에서 마지막으로 액세스한 데이터 보고서를 생성할 권한을 부여합니다.	Read			
GetAccessKeyLastUsed	지정된 액세스 키가 마지막으로 사용된 경우에 대한 정보를 검색할 권한을 부여합니다.	Read	user* (p. 1232)		
GetAccountAuthorizationDetails	서로의 관계를 포함하여 AWS 계정의 모든 IAM 사용자, 그룹, 역할 및 정책에 대한 정보를 검색할 권한을 부여합니다.	Read			
GetAccountPasswordPolicy	AWS 계정에 대한 암호 정책을 검색할 권한을 부여합니다.	Read			
GetAccountSummary	AWS 계정에서 IAM 개체 사용 및 IAM 할당량에 대한 정보를 검색할 권한을 부여합니다.	List			
GetContextKeysForCustomPolicy	지정된 정책에서 참조되는 모든 컨텍스트 키의 목록을 검색할 권한을 부여합니다.	Read			
GetContextKeysForPrincipalPolicy	지정된 IAM 자격 증명(사용자, 그룹 또는 역할)과 연결된 모든 IAM 정책에서 참조되는 모든 컨텍스트 키의 목록을 검색할 권한을 부여합니다.	Read	group (p. 1231)		
			role (p. 1231)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			user (p. 1232)		
GetCredentialReport	AWS 계정에 대한 자격 증명 보고서를 검색할 권한을 부여합니다.	Read			
GetGroup	지정된 IAM 그룹의 IAM 사용자 목록을 검색할 권한을 부여합니다.	Read	group* (p. 1231)		
GetGroupPolicy	지정된 IAM 그룹에 포함된 인라인 정책 문서를 검색할 권한을 부여합니다.	Read	group* (p. 1231)		
GetInstanceProfile	인스턴스 프로파일의 경로, GUID, ARN 및 역할을 포함하여 지정된 인스턴스 프로파일에 대한 정보를 검색할 권한을 부여합니다.	Read	instance-profile* (p. 1231)		
GetLoginProfile	지정된 IAM 사용자에 대한 사용자 이름 및 암호 생성 날짜를 검색할 권한을 부여합니다.	List	user* (p. 1232)		
GetOpenIDConnectProvider	IAM에서 OpenID Connect(OIDC) 공급자 리소스에 대한 정보를 검색할 권한을 부여합니다.	Read	oidc-provider* (p. 1231)		
GetOrganizationsAccessReport	AWS Organizations 액세스 보고서를 검색할 권한을 부여합니다.	Read			
GetPolicy	정책의 기본 버전과 정책이 연결된 자격 증명의 총 수를 포함하여 지정된 관리형 정책에 대한 정보를 검색할 권한을 부여합니다.	Read	policy* (p. 1231)		
GetPolicyVersion	정책 문서를 포함하여 지정된 관리형 정책의 버전에 대한 정보를 검색할 권한을 부여합니다.	Read	policy* (p. 1231)		
GetRole	역할의 경로, GUID, ARN 및 역할의 신뢰 정책을 포함하여 지정된 역할에 대한 정보를 검색할 권한을 부여합니다.	Read	role* (p. 1231)		
GetRolePolicy	지정된 IAM 역할에 포함된 인라인 정책 문서를 검색할 권한을 부여합니다.	Read	role* (p. 1231)		
GetSAMLProvider	IAM SAML 공급자 리소스를 생성하거나 업데이트할 때 업로드된 SAML 공급자 메타 문서를 검색할 권한을 부여합니다.	Read	saml-provider* (p. 1231)		
GetSSHPublicKey	키에 대한 메타데이터를 포함하여 지정된 SSH 퍼블릭 키를 검색할 권한을 부여합니다.	Read	user* (p. 1232)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetServerCertificate	IAM에 저장된 지정된 서버 인증서에 대한 정보를 검색할 권한을 부여합니다.	Read	server-certificate* (p. 1231)		
GetServiceLastAccessedDetails	서비스에서 마지막으로 액세스한 데이터 보고서에 대한 정보를 검색할 권한을 부여합니다.	Read			
GetServiceLastAccessedDetailsWithEntities	서비스에서 마지막으로 액세스한 데이터 보고서에서 엔터티에 대한 정보를 검색할 권한을 부여합니다.	Read			
GetServiceLinkedRoleDeletionStatus	IAM 서비스 연결 역할 삭제 상태를 검색할 권한을 부여합니다.	Read	role* (p. 1231)		
GetUser	지정된 IAM 사용자의 정보(사용자 생성 날짜, 경로, 고유 ID, ARN 등)를 검색할 권한을 부여합니다.	Read	user* (p. 1232)		
GetUserPolicy	지정된 IAM 사용자에 포함된 인라인 정책 문서를 검색할 권한을 부여합니다.	Read	user* (p. 1232)		
ListAccessKeys	지정된 IAM 사용자와 연결된 액세스 키 ID에 대한 정보를 나열할 권한을 부여합니다.	List	user* (p. 1232)		
ListAccountAliases	AWS 계정과 연결된 계정 별칭을 나열할 권한을 부여합니다.	List			
ListAttachedGroupPolicies	지정된 IAM 그룹에 연결된 모든 관리형 정책을 나열할 권한을 부여합니다.	List	group* (p. 1231)		
ListAttachedRolePolicies	지정된 IAM 역할에 연결된 모든 관리형 정책을 나열할 권한을 부여합니다.	List	role* (p. 1231)		
ListAttachedUserPolicies	지정된 IAM 사용자에 연결된 모든 관리형 정책을 나열할 권한을 부여합니다.	List	user* (p. 1232)		
ListEntitiesForPolicy	지정된 관리형 정책이 연결된 모든 IAM 자격 증명을 나열할 권한을 부여합니다.	List	policy* (p. 1231)		
ListGroupPolicies	지정된 IAM 그룹에 포함된 인라인 정책의 이름을 나열할 권한을 부여합니다.	List	group* (p. 1231)		
ListGroups	지정된 경로 접두사가 있는 IAM 그룹을 나열할 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListGroupsForUser	지정된 IAM 사용자가 속하는 IAM 그룹을 나열할 권한을 부여합니다.	List	user* (p. 1232)		
ListInstanceProfiles	지정된 경로 접두사가 있는 인스턴스 프로파일을 나열할 권한을 부여합니다.	List	instance-profile* (p. 1231)		
ListInstanceProfilesForRole	연결된 IAM 역할이 지정된 인스턴스 프로파일을 나열할 권한을 부여합니다.	List	role* (p. 1231)		
ListMFADevices	IAM 사용자에 대해 MFA 디바이스를 나열할 권한을 부여합니다.	List	user (p. 1232)		
ListOpenIDConnectProviders	AWS 계정에 정의된 IAM OpenID Connect(OIDC) 공급자 리소스 객체에 대한 정보를 나열할 권한을 부여합니다.	List			
ListPolicies	모든 관리형 정책을 나열할 권한을 부여합니다.	List			
ListPoliciesGrantingServiceAccess	특정 서비스에 엔터티 액세스를 부여하는 정책에 대한 정보를 나열할 권한을 부여합니다.	List			
ListPolicyVersions	현재 정책의 기본 버전으로 설정된 버전을 포함하여 지정된 관리형 정책의 버전에 대한 정보를 나열할 권한을 부여합니다.	List	policy* (p. 1231)		
ListRolePolicies	지정된 IAM 역할에 포함된 인라인 정책의 이름을 나열할 권한을 부여합니다.	List	role* (p. 1231)		
ListRoleTags	지정된 IAM 역할에 연결된 태그를 나열할 권한을 부여합니다.	List	role* (p. 1231)		
ListRoles	지정된 경로 접두사가 있는 IAM 역할을 나열할 권한을 부여합니다.	List			
ListSAMLProviders	IAM에서 SAML 공급자 리소스를 나열할 권한을 부여합니다.	List			
ListSSHPublicKeys	지정된 IAM 사용자와 연결된 SSH 퍼블릭 키에 대한 정보를 나열할 권한을 부여합니다.	List	user* (p. 1232)		
ListServerCertificates	지정된 경로 접두사가 있는 서버 인증서를 나열할 권한을 부여합니다.	List			
ListServiceSpecificCredentials	지정된 IAM 사용자와 연결된 서비스별 자격 증명에 대한 정보를 나열할 권한을 부여합니다.	List	user* (p. 1232)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListSigningCertificates	지정된 IAM 사용자와 연결된 서명 인증서에 대한 정보를 나열할 권한을 부여합니다.	List	user* (p. 1232)		
ListUserPolicies	지정된 IAM 사용자에 포함된 인라인 정책의 이름을 나열할 권한을 부여합니다.	List	user* (p. 1232)		
ListUserTags	지정된 IAM 사용자에 연결된 태그를 나열할 권한을 부여합니다.	List	user* (p. 1232)		
ListUsers	지정된 경로 접두사가 있는 IAM 사용자를 나열할 권한을 부여합니다.	List			
ListVirtualMFADevices	할당 상태에 따라 가상 MFA 디바이스를 나열할 권한을 부여합니다.	List			
PassRole [권한만 해당]	서비스에 역할을 전달할 권한을 부여합니다.	쓰기	role* (p. 1231)		
				iam:AssociatedResourceArn (p. 1232) iam:PassedToService (p. 1232)	
PutGroupPolicy	지정된 IAM 그룹에 포함된 인라인 정책 문서를 생성 또는 업데이트할 권한을 부여합니다.	권한 관리	group* (p. 1231)		
PutRolePermissionsBoundary	관리형 정책을 역할에 대한 권한 경계로 설정할 권한을 부여합니다.	권한 관리	role* (p. 1231)		
				iam:PermissionsBoundary (p. 1232)	
PutRolePolicy	지정된 IAM 역할에 포함된 인라인 정책 문서를 생성 또는 업데이트할 권한을 부여합니다.	권한 관리	role* (p. 1231)		
				iam:PermissionsBoundary (p. 1232)	
PutUserPermissionsBoundary	관리형 정책을 IAM 사용자에 대한 권한 경계로 설정할 권한을 부여합니다.	권한 관리	user* (p. 1232)		
				iam:PermissionsBoundary (p. 1232)	
PutUserPolicy	지정된 IAM 사용자에 포함된 인라인 정책 문서를 생성 또는 업데이트할 권한을 부여합니다.	권한 관리	user* (p. 1232)		
				iam:PermissionsBoundary (p. 1232)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RemoveClientIDFromOpenIDConnectProvider	지정된 IAM OpenID Connect(OIDC) 공급자 리소스의 클라이언트 ID 목록에서 클라이언트 ID(대상)를 제거할 권한을 부여합니다.	쓰기	oidc-provider* (p. 1231)		
RemoveRoleFromInstanceProfile	지정된 EC2 인스턴스 프로파일에서 지정된 IAM 역할을 제거할 권한을 부여합니다.	쓰기	instance-profile* (p. 1231)		
RemoveUserFromGroup	지정된 그룹에서 IAM 사용자를 제거할 권한을 부여합니다.	쓰기	group* (p. 1231)		
ResetServiceSpecificCredential	IAM 사용자에 대한 기존 서비스별 자격 증명의 암호를 재설정할 권한을 부여합니다.	쓰기	user* (p. 1232)		
ResyncMFADevice	지정된 MFA 디바이스와 IAM 엔터티(사용자 또는 역할)와 동기화할 권한을 부여합니다.	쓰기	user* (p. 1232)		
SetDefaultPolicyVersion	지정한 정책에서 버전을 정책의 기본 버전으로 설정할 권한을 부여합니다.	권한 관리	policy* (p. 1231)		
SetSecurityTokenServicePreferences	STS 전역 엔드포인트 토큰 버전을 설정할 권한을 부여합니다.	쓰기			
SimulateCustomPolicy	자격 증명 기반 정책 또는 리소스 기반 정책이 특정 API 작업 및 리소스에 대한 권한을 부여하는지 여부를 시뮬레이션할 권한을 부여합니다.	Read			
SimulatePrincipalPolicy	지정된 IAM 엔터티(사용자 또는 역할)에 연결된 자격 증명 기반 정책이 특정 API 작업 및 리소스에 대한 권한을 부여하는지 여부를 시뮬레이션할 권한을 부여합니다.	Read	group (p. 1231)		
			role (p. 1231)		
			user (p. 1232)		
TagRole	IAM 역할에 태그를 추가할 권한을 부여합니다.	태그 지정	role* (p. 1231)		
TagUser	IAM 사용자에 태그를 추가할 권한을 부여합니다.	태그 지정	user* (p. 1232)		
UntagRole	역할로부터 지정된 태그를 제거할 권한을 부여합니다.	태그 지정	role* (p. 1231)		
UntagUser	사용자로부터 지정된 태그를 제거할 권한을 부여합니다.	태그 지정	user* (p. 1232)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateAccessKey	지정된 액세스 키의 상태를 활성 또는 비활성으로 업데이트할 권한을 부여합니다.	쓰기	user* (p. 1232)		
UpdateAccountPasswordPolicy	AWS 계정에 대한 암호 정책 설정을 업데이트할 권한을 부여합니다.	쓰기			
UpdateAssumeRolePolicy	IAM 개체에 역할을 수임할 권한을 부여하는 정책을 업데이트할 권한을 부여합니다.	권한 관리	role* (p. 1231)		
UpdateGroup	지정된 IAM 그룹의 이름 또는 경로를 업데이트할 권한을 부여합니다.	쓰기	group* (p. 1231)		
UpdateLoginProfile	지정된 IAM 사용자에 대한 암호를 변경할 권한을 부여합니다.	쓰기	user* (p. 1232)		
UpdateOpenIDConnectProviderThumbprint	OpenID Connect(OIDC) 공급자 리소스와 연결된 서버 인증서 지문의 전체 목록을 업데이트할 권한을 부여합니다.	쓰기	oidc-provider* (p. 1231)		
UpdateRole	역할의 설명 또는 최대 세션 기간 설정을 업데이트할 권한을 부여합니다.	쓰기	role* (p. 1231)		
UpdateRoleDescription	역할의 설명만을 업데이트할 권한을 부여합니다.	쓰기	role* (p. 1231)		
UpdateSAMLProvider	기존 SAML 공급자 리소스에 대한 메타데이터 문서를 업데이트할 권한을 부여합니다.	쓰기	saml-provider* (p. 1231)		
UpdateSSHPublicKey	IAM 사용자의 SSH 퍼블릭 키 상태를 활성 또는 비활성으로 업데이트할 권한을 부여합니다.	쓰기	user* (p. 1232)		
UpdateServerCertificate	IAM에 저장된 지정된 서버 인증서의 이름 또는 경로를 업데이트할 권한을 부여합니다.	쓰기	server-certificate* (p. 1231)		
UpdateServiceSpecificCredential	IAM 사용자에 대한 서비스별 자격 증명의 상태를 활성 또는 비활성으로 업데이트할 권한을 부여합니다.	쓰기	user* (p. 1232)		
UpdateSigningCertificate	지정된 사용자 서명 인증서의 상태를 활성 또는 비활성으로 업데이트할 권한을 부여합니다.	쓰기	user* (p. 1232)		
UpdateUser	지정된 IAM 사용자의 이름 또는 경로를 업데이트할 권한을 부여합니다.	쓰기	user* (p. 1232)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UploadSSHPublicKey	SSH 퍼블릭 키를 업로드하고 지정된 IAM 사용자와 연결할 권한을 부여합니다.	쓰기	user* (p. 1232)		
UploadServerCertificate	AWS 계정에 대한 서버 인증서 개체를 업로드할 권한을 부여합니다.	쓰기	server-certificate* (p. 1231)		
UploadSigningCertificate	X.509 서명 인증서를 업로드하고 지정된 IAM 사용자와 연결할 권한을 부여합니다.	쓰기	user* (p. 1232)		

Identity And Access Management에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1219)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
access-report	`arn:${Partition}:iam::${Account}:access-report/${EntityPath}`	
assumed-role	`arn:${Partition}:iam::${Account}:assumed-role/${RoleName}/${RoleSessionName}`	
federated-user	`arn:${Partition}:iam::${Account}:federated-user/${UserName}`	
group	`arn:${Partition}:iam::${Account}:group/${GroupNameWithPath}`	
instance-profile	`arn:${Partition}:iam::${Account}:instance-profile/${InstanceProfileNameWithPath}`	
mfa	`arn:${Partition}:iam::${Account}:mfa/${Path}/${MfaTokenId}`	
oidc-provider	`arn:${Partition}:iam::${Account}:oidc-provider/${OidcProviderName}`	
policy	`arn:${Partition}:iam::${Account}:policy/${PolicyNameWithPath}`	
role	`arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}`	iam:ResourceTag/${TagKey} (p. 1232)
saml-provider	`arn:${Partition}:iam::${Account}:saml-provider/${SamlProviderName}`	
server-certificate	`arn:${Partition}:iam::${Account}:server-certificate/${CertificateNameWithPath}`	

리소스 유형	ARN	조건 키
sms-mfa	`arn:${Partition}:iam::${Account}:sms-mfa/${MfaTokenIdWithPath}`	
user	`arn:${Partition}:iam::${Account}:user/${UserNameWithPath}`	iam:ResourceTag/${TagKey} (p. 1232)

Identity And Access Management의 조건 키

Identity And Access Management는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
iam:AWSServiceName	이 역할이 연결되는 AWS 서비스에 따라 액세스를 필터링합니다.	문자열
iam:AssociatedResourceArn	역할이 대신 사용될 리소스를 기준으로 필터링합니다.	ARN
iam:OrganizationsPolicyId	AWS Organizations 정책의 ID에 따라 액세스를 필터링합니다.	문자열
iam:PassedToService	이 역할이 전달되는 AWS 서비스에 따라 액세스를 필터링합니다.	문자열
iam:PermissionsBoundary	지정된 정책이 IAM 엔터티(사용자 또는 역할)의 권한 경계로 설정되는 경우 액세스를 필터링합니다.	문자열
iam:PolicyARN	IAM 정책의 ARN에 따라 액세스를 필터링합니다.	ARN
iam:ResourceTag/${TagKey}	IAM 엔터티(사용자 또는 역할)에 연결된 태그에 따라 액세스를 필터링합니다.	문자열

AWS Import Export Disk Service에 사용되는 작업, 리소스 및 조건 키

AWS Import Export Disk Service(서비스 접두사: `importexport`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Import Export Disk Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelJob	이 작업은 지정된 작업을 취소합니다. 작업 소유자만이 이를 취소할 수 있습니다. 작업이 이미 시작되었거나 완료된 경우에는 취소 작업이 실패합니다.	쓰기			
CreateJob	이 작업은 데이터 업로드 또는 다운로드를 예약하는 프로세스를 시작합니다.	쓰기			
GetShippingLabel	이 작업은 프로세싱을 위해 장치를 AWS에 배송할 때 사용할 선불 배송 라벨을 생성합니다.	Read			
GetStatus	이 작업은 프로세싱 파이프라인 내 작업의 위치, 결과의 상태, 작업과 연결된 서명 값 등 작업에 대한 정보를 반환합니다.	Read			
ListJobs	이 작업은 요청자와 연결된 작업을 반환합니다.	List			
UpdateJob	이 작업을 사용하면 새로운 매니페스트 파일을 제공하여 원래 매니페스트 파일에 지정된 파라미터를 변경할 수 있습니다.	쓰기			

AWS Import Export Disk Service에서 정의한 리소스 유형

AWS Import Export Disk Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Import Export Disk Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Import Export Disk Service의 조건 키

Import/Export에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Inspector에 사용되는 작업, 리소스 및 조건 키

Amazon Inspector(서비스 접두사: `inspector`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Inspector에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddAttributesToFindings	결과의 ARN에 의해 지정되는 결과에 속성(키 및 값 페어)을 할당합니다.	쓰기			
CreateAssessmentTarget	CreateResourceGroup에 의해 생성되는 리소스 그룹의 ARN을 사용하는 새 평가 대상을 생성합니다.	쓰기			
CreateAssessmentTemplate	평가 대상의 ARN에 의해 지정되는 평가 대상에 대한 평가 템플릿을 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateResourceGroup	Amazon Inspector 평가 대상에 포함할 EC2 인스턴스를 선택하는 데 사용되는 지정된 태그 집합(키 및 값 페어)을 사용하는 리소스 그룹을 생성합니다.	쓰기			
DeleteAssessmentRun	평가 실행의 ARN에 의해 지정되는 평가 실행을 삭제합니다.	쓰기			
DeleteAssessmentTarget	평가 대상의 ARN에 의해 지정되는 평가 대상을 삭제합니다.	쓰기			
DeleteAssessmentTemplate	평가 템플릿의 ARN에 의해 지정되는 평가 템플릿을 삭제합니다.	쓰기			
DescribeAssessmentRuns	평가 실행의 ARN에 의해 지정되는 평가 실행을 설명합니다.	Read			
DescribeAssessmentTargets	평가 대상의 ARN에 의해 지정되는 평가 대상을 설명합니다.	Read			
DescribeAssessmentTemplates	평가 대상의 ARN에 의해 지정되는 평가 템플릿을 설명합니다.	Read			
DescribeCrossAccountAccessRole	Amazon Inspector가 귀하의 AWS 계정에 액세스할 수 있도록 활성화하는 IAM 역할을 설명합니다.	Read			
DescribeFindings	결과의 ARN에 의해 지정되는 결과를 설명합니다.	Read			
DescribeResourceGroups	리소스 그룹의 ARN에 의해 지정되는 리소스 그룹을 설명합니다.	Read			
DescribeRulesPackages	규칙 패키지의 ARN에 의해 지정되는 규칙 패키지를 설명합니다.	Read			
GetTelemetryMetadata	지정된 평가 실행을 위해 수집되는 데이터에 대한 정보.	Read			
ListAssessmentRunAgents	평가 실행의 ARN에 의해 지정되는 평가 실행의 에이전트를 나열합니다.	List			
ListAssessmentRuns	평가 템플릿의 ARN에 의해 지정되는 평가 템플릿에 해당되는 평가 실행을 나열합니다.	List			
ListAssessmentTargets	이 AWS 계정 내 평가 대상의 ARN을 나열합니다.	List			
ListAssessmentTemplates	평가 대상의 ARN에 의해 지정되는 평가 대상에 해당되는 평가 템플릿을 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListEventSubscriptions	평가 템플릿의 ARN에 의해 지정되는 평가 템플릿에 대한 모든 이벤트 구독을 나열합니다.	List			
ListFindings	평가 실행의 ARN에 의해 지정되는 평가 실행에 의해 생성되는 결과를 나열합니다.	List			
ListRulesPackages	사용 가능한 모든 Amazon Inspector 규칙 패키지를 나열합니다.	List			
ListTagsForResource	평가 템플릿과 연결된 모든 태그를 나열합니다.	List			
PreviewAgents	지정된 평가 대상의 일부인 EC2 인스턴스에 설치된 에이전트를 미리 봅니다.	Read			
RegisterCrossAccountAccessRole	평가 실행 시작 시점에 또는 PreviewAgents 작업을 호출할 때 Amazon Inspector가 EC2 인스턴스를 나열하기 위해 사용하는 IAM 역할을 등록합니다.	쓰기			
RemoveAttributesFromFindings	지정된 키가 포함된 속성이 존재하는 결과의 ARN에 의해 지정되는 결과에서 전체 속성(키 및 값 페어)을 제거합니다.	쓰기			
SetTagsForResource	태그(키 및 값 페어)를 평가 템플릿의 ARN에 의해 지정되는 평가 템플릿으로 설정합니다.	태그 지정			
StartAssessmentRun	평가 템플릿의 ARN에 의해 지정되는 평가 실행을 시작합니다.	쓰기			
StopAssessmentRun	평가 실행의 ARN에 의해 지정되는 평가 실행을 중지합니다.	쓰기			
SubscribeToEvent	지정된 이벤트에 대한 Amazon Simple Notification Service(SNS) 알림을 지정된 SNS 주제에 보내는 프로세스를 활성화합니다.	쓰기			
UnsubscribeFromEvent	지정된 이벤트에 대한 Amazon Simple Notification Service(SNS) 알림을 지정된 SNS 주제에 보내는 프로세스를 비활성화합니다.	쓰기			
UpdateAssessmentTarget	평가 대상의 ARN에 의해 지정되는 평가 대상을 업데이트합니다.	쓰기			

Amazon Inspector에서 정의한 리소스 유형

Amazon Inspector는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Inspector에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Inspector에 사용되는 조건 키

Inspector에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS IoT에 사용되는 작업, 리소스 및 조건 키

AWS IoT(서비스 접두사: `iot`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS IoT에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptCertificateTransfer	대기 중인 인증서 전송을 수락합니다.	쓰기			
AddThingToBillingGroup	지정된 결제 그룹에 사물을 추가합니다.	쓰기	billinggroup* (p. 1252)		
			thing* (p. 1252)		
AddThingToThingGroup	지정된 사물 그룹에 사물을 추가합니다.	쓰기	thing* (p. 1252)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			thinggroup* (p. 1252)		
AssociateTargetsWithJob	그룹을 연속 작업과 연결합니다.	쓰기	job* (p. 1252)		
			thing* (p. 1252)		
			thinggroup* (p. 1252)		
AttachPolicy	정책을 지정한 대상에 연결합니다.	권한 관리	cert (p. 1253)		
			thinggroup (p. 1252)		
AttachPrincipalPolicy	지정한 정책을 지정한 보안 주체(인증서 또는 다른 자격 증명)에 연결합니다.	권한 관리	cert (p. 1253)		
AttachSecurityProfile	Device Defender 보안 프로필을 사물 그룹이나 이 계정에 연결합니다.	쓰기	securityprofile* (p. 1253)		
			thinggroup (p. 1252)		
AttachThingPrincipal	지정한 보안 주체를 지정한 사물에 연결합니다.	쓰기			
CancelAuditTask	진행 중인 감사를 취소합니다. 감사는 예정된 감사이거나 온디맨드 감사일 수 있습니다.	쓰기			
CancelCertificateTransfer	지정한 인증서에 대해 대기 중인 전송을 취소합니다.	쓰기			
CancelJob	작업을 취소합니다.	쓰기	job* (p. 1252)		
CancelJobExecution	특정 디바이스의 작업 실행을 취소합니다.	쓰기	job* (p. 1252)		
			thing* (p. 1252)		
ClearDefaultAuthorizer	기본 권한 부여자를 삭제합니다.	쓰기			
CloseTunnel	터널을 닫습니다.	쓰기	tunnel* (p. 1252)		
				iot:Delete (p. 1254)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Connect	지정된 클라이언트로서 연결합니다.	쓰기	client* (p. 1252)		
CreateAuthorizer	권한 부여자를 생성합니다.	쓰기	authorizer* (p. 1253)		
CreateBillingGroup	결제 그룹을 생성합니다.	태그 지정	billinggroup* (p. 1252)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
CreateCertificateFromCsr	지정된 인증서 서명 요청을 사용하여 X.509 인증서를 생성합니다.	쓰기			
CreateDynamicThingGroup	동적 사물 그룹을 생성합니다.	태그 지정	dynamicthinggroup* (p. 1252)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
CreateJob	작업을 생성합니다.	쓰기	job* (p. 1252)		
			thing* (p. 1252)		
			thinggroup* (p. 1252)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
CreateKeysAndCertificate	2048비트 RSA 키 페어를 생성한 후 발급된 퍼블릭 키를 사용해 X.509 인증서를 발급합니다.	쓰기			
CreateOTAUpdate	OTA 업데이트 작업을 생성합니다.	쓰기	otaupdate* (p. 1253)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
CreatePolicy	AWS IoT 정책을 생성합니다.	쓰기			
CreatePolicyVersion	지정한 AWS IoT 정책의 새로운 버전을 생성합니다.	쓰기	policy* (p. 1253)		
CreateProvisioningClaim	프로비저닝 클레임을 만듭니다.	쓰기	provisioningtemplate* (p. 1253)		
CreateProvisioningTemplate	플릿 프로비저닝 템플릿을 생성합니다.	쓰기	provisioningtemplate* (p. 1253)		
CreateProvisioningTemplateVersion	새 버전의 플릿 프로비저닝 템플릿을 생성합니다.	쓰기	provisioningtemplate* (p. 1253)		
CreateRoleAlias	역할 별칭을 생성합니다.	쓰기	role* (p. 1253)		
			rolealias* (p. 1253)		
CreateScheduledAudit	지정된 시간 간격으로 실행되는 예정된 감사를 생성합니다.	태그 지정	scheduledaudit* (p. 1253)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
CreateSecurityProfile	Device Defender 보안 프로필을 생성합니다.	태그 지정	securityprofile* (p. 1253)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
CreateStream	새 AWS IoT 스트림을 생성합니다.	쓰기	stream* (p. 1253)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateThing	사물 레지스트리에서 사물을 생성합니다.	쓰기	thing* (p. 1252)		
			billinggroup (p. 1252)		
CreateThingGroup	사물 그룹을 만듭니다.	태그 지정	thinggroup* (p. 1252)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
CreateThingType	새로운 사물 유형을 생성합니다.	태그 지정	thingtype* (p. 1252)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
CreateTopicRule	규칙을 생성합니다.	쓰기	rule* (p. 1253)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
DeleteAccountAuditConfiguration	계정과 연결된 감사 구성을 삭제합니다.	쓰기			
DeleteAuthorizer	지정한 권한 부여자를 삭제합니다.	쓰기	authorizer* (p. 1253)		
DeleteBillingGroup	지정된 결제 그룹을 삭제합니다.	태그 지정	billinggroup* (p. 1252)		
DeleteCACertificate	등록된 CA 인증서를 삭제합니다.	쓰기	cacert* (p. 1253)		
DeleteCertificate	지정한 인증서를 삭제합니다.	쓰기	cert* (p. 1253)		
DeleteDynamicThingGroup	지정된 동적 사물 그룹을 삭제합니다.	태그 지정	dynamicthinggroup* (p. 1252)		
DeleteJob	특정 작업과 그와 관련한 작업 실행을 삭제합니다.	쓰기	job* (p. 1252)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteJobExecution	작업 실행을 삭제합니다.	쓰기	job* (p. 1252)		
			thing* (p. 1252)		
DeleteOTAUpdate	OTA 업데이트 작업을 삭제합니다.	쓰기	otaupdate* (p. 1253)		
DeletePolicy	지정된 정책을 삭제합니다.	쓰기	policy* (p. 1253)		
DeletePolicyVersion	지정된 정책에서 지정된 버전을 삭제합니다.	쓰기	policy* (p. 1253)		
DeleteProvisioningTemplate	플릿 프로비저닝 템플릿을 삭제합니다.	쓰기	provisioningtemplate* (p. 1253)		
DeleteProvisioningTemplateVersion	플릿 프로비저닝 템플릿 버전을 삭제합니다.	쓰기	provisioningtemplate* (p. 1253)		
DeleteRegistrationCode	CA 인증서 등록 코드를 삭제합니다.	쓰기			
DeleteRoleAlias	지정된 역할 별칭을 삭제합니다.	쓰기	rolealias* (p. 1253)		
DeleteScheduledAudit	예정된 감사를 삭제합니다.	쓰기	scheduledaudit* (p. 1253)		
DeleteSecurityProfile	Device Defender 보안 프로필을 삭제합니다.	쓰기	securityprofile* (p. 1253)		
DeleteStream	지정된 스트림을 삭제합니다.	쓰기	stream* (p. 1253)		
DeleteThing	지정된 사물을 삭제합니다.	쓰기	thing* (p. 1252)		
DeleteThingGroup	지정된 사물 그룹을 삭제합니다.	태그 지정	thinggroup* (p. 1252)		
DeleteThingShadow	지정된 사물 섀도우를 삭제합니다.	쓰기	thing* (p. 1252)		
DeleteThingType	지정한 사물 유형을 삭제합니다.	태그 지정	thingtype* (p. 1252)		
DeleteTopicRule	지정된 규칙을 삭제합니다.	쓰기	rule* (p. 1253)		
DeleteV2LoggingLevel	지정된 v2 로깅 수준을 삭제합니다.	쓰기			
DeprecateThingType	지정된 사물 유형을 사용 중단합니다.	쓰기	thingtype* (p. 1252)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeAccountAuditConfiguration	계정의 감사 구성에 대한 정보를 가져옵니다.	Read			
DescribeAuditTask	Device Defender 감사에 대한 정보를 가져옵니다.	Read			
DescribeAuthorizer	권한 부여자에 대해 설명합니다.	Read	authorizer* (p. 1253)		
DescribeBillingGroup	지정된 결제 그룹에 대한 정보를 가져옵니다.	Read	billinggroup* (p. 1252)		
DescribeCACertificate	등록된 CA 인증서에 대해 설명합니다.	Read	cacert* (p. 1253)		
DescribeCertificate	지정한 인증서에 대한 정보를 가져옵니다.	Read	cert* (p. 1253)		
DescribeDefaultAuthorizer	기본 권한 부여자에 대해 설명합니다.	Read			
DescribeEndpoint	호출하는 AWS 계정에 따라 고유한 엔드포인트를 반환합니다.	Read			
DescribeEventConfigurations	계정 이벤트 구성을 반환합니다.	Read			
DescribeIndex	지정된 인덱스에 대한 정보를 가져옵니다.	Read	index* (p. 1252)		
DescribeJob	작업에 대해 설명합니다.	Read	job* (p. 1252)		
DescribeJobExecution	작업 실행에 대해 설명합니다.	Read	job (p. 1252)		
			thing (p. 1252)		
DescribeProvisioningTemplate	플릿 프로비저닝 템플릿에 대한 정보를 반환합니다.	Read	provisioningtemplate* (p. 1253)		
DescribeProvisioningTemplateVersion	플릿 프로비저닝 템플릿 버전에 대한 정보를 반환합니다.	Read	provisioningtemplate* (p. 1253)		
DescribeRoleAlias	역할 별칭에 대해 설명합니다.	Read	rolealias* (p. 1253)		
DescribeScheduledAudit	예정된 감사에 대한 정보를 가져옵니다.	Read	scheduledaudit* (p. 1253)		
DescribeSecurityProfile	Device Defender 보안 프로필에 대한 정보를 가져옵니다.	Read	securityprofile* (p. 1253)		
DescribeStream	지정된 스트림에 대한 정보를 가져옵니다.	Read	stream* (p. 1253)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeThing	지정된 사물에 대한 정보를 가져옵니다.	Read	thing* (p. 1252)		
DescribeThingGroup	지정된 사물 그룹에 대한 정보를 가져옵니다.	Read	thinggroup* (p. 1252)		
DescribeThingRegistrationTask	대량 사물 등록 작업에 대한 정보를 가져옵니다.	Read			
DescribeThingType	지정한 사물 유형에 대한 정보를 가져옵니다.	Read	thingtype* (p. 1252)		
DescribeTunnel	터널에 대해 설명합니다.	Read	tunnel* (p. 1252)		
DetachPolicy	지정한 대상에서 정책을 분리합니다.	권한 관리	cert (p. 1253)		
			thinggroup (p. 1252)		
DetachPrincipalPolicy	지정한 인증서에서 지정한 정책을 제거합니다.	권한 관리	cert (p. 1253)		
DetachSecurityProfile	사물 그룹이나 이 계정에서 Device Defender 보안 프로필을 연결 해제합니다.	쓰기	securityprofile* (p. 1253)		
			thinggroup (p. 1252)		
DetachThingPrincipal	지정한 사물에서 지정한 보안 주체를 분리합니다.	쓰기			
DisableTopicRule	지정된 규칙을 비활성화합니다.	쓰기	rule* (p. 1253)		
EnableTopicRule	지정된 규칙을 활성화합니다.	쓰기	rule* (p. 1253)		
GetCardinality	IoT 플릿 인덱스에 대한 카디널리티를 가져옵니다.	Read	index* (p. 1252)		
GetEffectivePolicies	적용 중인 정책을 가져옵니다.	Read	cert (p. 1253)		
GetIndexingConfiguration	현재 플릿 인덱싱 구성을 가져옵니다.	Read			
GetJobDocument	작업 문서를 가져옵니다.	Read	job* (p. 1252)		
GetLoggingOptions	로깅 옵션을 가져옵니다.	Read			
GetOTAUpdate	OTA 업데이트 작업에 대한 정보를 가져옵니다.	Read	otaupdate* (p. 1253)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetPendingJobExecutions	종료 상태가 아닌 사물의 모든 작업 목록을 가져옵니다.	Read	thing* (p. 1252)		
GetPercentiles	IoT 플릿 인덱스에 대한 백분위수를 가져옵니다.	Read	index* (p. 1252)		
GetPolicy	기본 버전의 정책 문서와 함께 지정한 정책에 대한 정보를 가져옵니다.	Read	policy* (p. 1253)		
GetPolicyVersion	지정한 정책 버전에 대한 정보를 가져옵니다.	Read	policy* (p. 1253)		
GetRegistrationCode	CA 인증서를 AWS IoT에 등록할 때 사용할 등록 코드를 가져옵니다.	Read			
GetStatistics	IoT 플릿 인덱스에 대한 통계를 가져옵니다.	Read	index* (p. 1252)		
GetThingShadow	사물 섀도우를 가져옵니다.	Read	thing* (p. 1252)		
GetTopicRule	지정된 규칙에 대한 정보를 가져옵니다.	Read	rule* (p. 1253)		
GetV2LoggingOptions	v2 로깅 옵션을 가져옵니다.	Read			
ListActiveViolations	지정된 Device Defender 보안 프로필 또는 사물에 대한 활성 위반을 나열합니다.	List	securityprofile (p. 1253)		
			thing (p. 1252)		
ListAttachedPolicies	지정한 사물 그룹에 연결되어 있는 정책을 나열합니다.	List			
ListAuditFindings	지정된 기간 동안 수행된 Device Defender 감사의 결과를 나열합니다.	List			
ListAuditTasks	지정된 기간 동안 수행된 Device Defender 감사를 나열합니다.	List			
ListAuthorizers	계정에 등록된 권한 부여자를 나열합니다.	List			
ListBillingGroups	모든 결제 그룹을 나열합니다.	List			
ListCACertificates	AWS 계정에 등록된 CA 인증서를 나열합니다.	List			
ListCertificates	인증서를 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListCertificatesByCA	지정한 CA 인증서에서 서명한 디바이스 인증서를 나열합니다.	List			
ListIndices	플릿 인덱스에 대한 모든 인덱스를 나열합니다.	List			
ListJobExecutionsForJob	임의 작업에 대한 작업 실행을 나열합니다.	List	job* (p. 1252)		
ListJobExecutionsForThing	지정한 사물에 대한 작업 실행을 나열합니다.	List	thing* (p. 1252)		
ListJobs	작업을 나열합니다.	List			
ListOTAUpdates	계정의 OTA 업데이트 작업을 나열합니다.	List			
ListOutgoingCertificates	전송 중이지만 아직 수락되지 않은 인증서를 나열합니다.	List			
ListPolicies	정책을 나열합니다.	List			
ListPolicyPrincipals	지정한 정책과 연결되어 있는 보안 주체를 나열합니다.	List			
ListPolicyVersions	지정된 정책의 버전들을 나열하고 기본 버전을 식별합니다.	List			
ListPrincipalPolicies	지정한 보안 주체에 연결되어 있는 정책을 나열합니다. Amazon Cognito 자격 증명을 사용하는 경우에는 ID가 Amazon Cognito 자격 증명 형식을 따라야 합니다.	List			
ListPrincipalThings	지정한 보안 주체와 연결되어 있는 사물을 나열합니다.	List			
ListProvisioningTemplateVersions	플릿 프로비저닝 템플릿 버전의 목록입니다.	List	provisioningtemplate* (p. 1253)		
ListProvisioningTemplates	AWS 계정의 플릿 프로비저닝 템플릿을 나열합니다.	List			
ListRoleAliases	역할 별칭을 나열합니다.	List			
ListScheduledAudits	예정된 감사를 모두 나열합니다.	List			
ListSecurityProfiles	생성한 Device Defender 보안 프로필을 나열합니다.	List			
ListSecurityProfilesForTarget	대상에 연결된 Device Defender 보안 프로필을 나열합니다.	List	thinggroup (p. 1252)		
ListStreams	계정에 속한 스트림을 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTagsForResource	지정된 리소스에 대한 모든 태그를 나열합니다.	List	billinggroup (p. 1252)		
			dynamicthinggroup (p. 1252)		
			job (p. 1252)		
			otaupdate (p. 1253)		
			rule (p. 1253)		
			scheduledaudit (p. 1253)		
			securityprofile (p. 1253)		
			stream (p. 1253)		
			thinggroup (p. 1252)		
			thingtype (p. 1252)		
ListTargetsForPolicy	지정한 정책이 적용되는 대상을 나열합니다.	List	policy* (p. 1253)		
ListTargetsForSecurityProfile	지정된 Device Defender 보안 프로필과 연결된 대상을 나열합니다.	List	securityprofile* (p. 1253)		
ListThingGroups	모든 사물 그룹을 나열합니다.	List			
ListThingGroupsForThing	지정된 사물이 속한 사물 그룹을 나열합니다.	List	thing* (p. 1252)		
ListThingPrincipals	지정한 사물과 연결되어 있는 보안 주체를 나열합니다.	List			
ListThingRegistrationTaskReports	대량 사물 등록 작업에 대한 정보를 나열합니다.	List			
ListThingRegistrationTasks	대량 사물 등록 작업을 나열합니다.	List			
ListThingTypes	모든 사물 유형을 나열합니다.	List			
ListThings	모든 사물을 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListThingsInBillingGroup	지정된 결제 그룹에 속한 모든 사물을 나열합니다.	List	billinggroup* (p. 1252)		
ListThingsInThingGroup	지정된 사물 그룹에 속한 모든 사물을 나열합니다.	List	thinggroup* (p. 1252)		
ListTopicRules	특정 주제에 대한 규칙을 나열합니다.	List			
ListTunnels	터널을 나열합니다.	List			
ListV2LoggingLevels	v2 로깅 수준을 나열합니다.	List			
ListViolationEvents	지정된 기간 동안 발견된 Device Defender 보안 프로필 위반을 나열합니다.	List	securityprofile (p. 1253)		
			thing (p. 1252)		
OpenTunnel	터널을 엽니다.	쓰기		aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254) iot:ThingGroupArn (p. 1254) iot:TunnelDestinationService (p. 1254)	
Publish	지정된 주제에 게시합니다.	쓰기	topic* (p. 1253)		
Receive	지정된 주제로부터 수신합니다.	쓰기	topic* (p. 1253)		
RegisterCACertificate	CA 인증서를 AWS IoT에 등록합니다.	쓰기			
RegisterCertificate	디바이스 인증서를 AWS IoT에 등록합니다.	쓰기			
RegisterThing	사물을 등록합니다.	쓰기			
RejectCertificateTransfer	대기 중인 인증서 전송을 거부합니다.	쓰기	cert* (p. 1253)		
RemoveThingFromBillingGroup	지정된 결제 그룹에서 사물을 제거합니다.	쓰기	billinggroup* (p. 1252)		
			thing* (p. 1252)		
RemoveThingFromThingGroup	지정된 사물 그룹에서 사물을 제거합니다.	쓰기	thing* (p. 1252)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			thinggroup* (p. 1252)		
ReplaceTopicRule	지정된 규칙을 대체합니다.	쓰기	rule* (p. 1253)		
SearchIndex	IoT 플릿 인덱스를 검색합니다.	Read	index* (p. 1252)		
SetDefaultAuthorizer	기본 권한 부여자를 설정합니다. 이 작업은 권한 부여자를 지정하지 않고 웹소켓에 연결하는 경우에 사용됩니다.	권한 관리	authorizer* (p. 1253)		
SetDefaultPolicyVersion	지정한 정책에서 지정한 버전을 정책의 기본(유효) 버전으로 설정합니다.	권한 관리	policy* (p. 1253)		
SetLoggingOptions	로깅 옵션을 설정합니다.	쓰기			
SetV2LoggingLevel	v2 로깅 수준을 설정합니다.	쓰기			
SetV2LoggingOptions	v2 로깅 옵션을 설정합니다.	쓰기			
StartNextPendingJobExecution	사물의 다음 번 대기 중 작업 실행을 가져오고 시작합니다.	쓰기	thing* (p. 1252)		
StartOnDemandAuditTask	온디맨드 Device Defender 감사를 시작합니다.	쓰기			
StartThingRegistrationTask	대량 사물 등록 작업을 시작합니다.	쓰기			
StopThingRegistrationTask	대량 사물 등록 작업을 중지합니다.	쓰기			
Subscribe	지정된 TopicFilter를 구독합니다.	쓰기	topicfilter* (p. 1253)		
TagResource	지정된 리소스에 태그를 지정합니다.	태그 지정	billinggroup (p. 1252)		
			dynamicthinggroup (p. 1252)		
			job (p. 1252)		
			otaupdate (p. 1253)		
			rule (p. 1253)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			scheduledaudit (p. 1253)		
			securityprofile (p. 1253)		
			stream (p. 1253)		
			thinggroup (p. 1252)		
			thingtype (p. 1252)		
				aws:RequestTag/${TagKey} (p. 1254) aws:TagKeys (p. 1254)	
TestAuthorization	그룹 정책에 대해 정책 평가를 테스트합니다.	Read	cert (p. 1253)		
TestInvokeAuthorizer	테스트 목적으로 지정한 사용자 지정 권한 부여자를 호출합니다.	Read	authorizer* (p. 1253)		
TransferCertificate	지정한 인증서를 지정한 AWS 계정으로 전송합니다.	쓰기	cert* (p. 1253)		
UntagResource	지정된 리소스에서 태그를 제거합니다.	태그 지정	billinggroup (p. 1252)		
			dynamicthinggroup (p. 1252)		
			job (p. 1252)		
			otaupdate (p. 1253)		
			rule (p. 1253)		
			scheduledaudit (p. 1253)		
			securityprofile (p. 1253)		
			stream (p. 1253)		
			thinggroup (p. 1252)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			thingtype (p. 1252)		
				aws:TagKeys (p. 1254)	
UpdateAccountAuditConfiguration	이 계정에 대한 Device Defender 감사 설정을 구성하거나 재구성합니다.	쓰기			
UpdateAuthorizer	권한 부여자를 업데이트합니다	쓰기	authorizer* (p. 1253)		
UpdateBillingGroup	지정된 결제 그룹과 연결된 정보를 업데이트합니다.	쓰기	billinggroup* (p. 1252)		
UpdateCACertificate	등록된 CA 인증서를 업데이트합니다.	쓰기	cacert* (p. 1253)		
UpdateCertificate	지정한 인증서의 상태를 업데이트합니다. 이 작업은 멱등성을 갖습니다.	쓰기	cert* (p. 1253)		
UpdateDynamicThingGroup	동적 사물 그룹을 업데이트합니다.	쓰기	dynamicthinggroup* (p. 1252)		
UpdateEventConfigurations	이벤트 구성을 업데이트합니다.	쓰기			
UpdateIndexingConfiguration	플릿 인덱싱 구성을 업데이트합니다.	쓰기			
UpdateJob	작업을 업데이트합니다.	쓰기	job* (p. 1252)		
UpdateJobExecution	작업 실행을 업데이트합니다.	쓰기	thing* (p. 1252)		
UpdateProvisioningTemplate	플릿 프로비저닝 템플릿을 업데이트합니다	쓰기	provisioningtemplate* (p. 1253)		
UpdateRoleAlias	역할 별칭을 업데이트합니다.	쓰기	rolealias* (p. 1253)		
			role (p. 1253)		
UpdateScheduledAudit	수행되는 점검 및 감사가 발생하는 빈도를 비롯하여 예정된 감사를 업데이트합니다.	쓰기	scheduledaudit* (p. 1253)		
UpdateSecurityProfile	Device Defender 보안 프로필을 업데이트합니다.	쓰기	securityprofile* (p. 1253)		
UpdateStream	스트림 데이터를 업데이트합니다.	쓰기	stream* (p. 1253)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateThing	지정된 사물과 연결된 정보를 업데이트합니다.	쓰기	thing* (p. 1252)		
UpdateThingGroup	지정된 사물 그룹과 연결된 정보를 업데이트합니다.	쓰기	thinggroup* (p. 1252)		
UpdateThingGroupsForThing	사물이 속한 사물 그룹을 업데이트합니다.	쓰기	thing* (p. 1252)		
			thinggroup (p. 1252)		
UpdateThingShadow	사물 섀도우를 업데이트합니다.	쓰기	thing* (p. 1252)		
ValidateSecurityProfileBehaviors	Device Defender 보안 프로필 동작 사양을 검증합니다.	Read			

AWS IoT에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1237)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
client	`arn:${Partition}:iot:${Region}:${Account}:client/${ClientId}`	
index	`arn:${Partition}:iot:${Region}:${Account}:index/${IndexName}`	
job	`arn:${Partition}:iot:${Region}:${Account}:job/${JobId}`	aws:ResourceTag/${TagKey} (p. 1254)
tunnel	`arn:${Partition}:iot:${Region}:${Account}:tunnel/${TunnelId}`	aws:ResourceTag/${TagKey} (p. 1254)
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	
thinggroup	`arn:${Partition}:iot:${Region}:${Account}:thinggroup/${ThingGroupName}`	aws:ResourceTag/${TagKey} (p. 1254)
billinggroup	`arn:${Partition}:iot:${Region}:${Account}:billinggroup/${BillingGroupName}`	aws:ResourceTag/${TagKey} (p. 1254)
dynamicthinggroup	`arn:${Partition}:iot:${Region}:${Account}:thinggroup/${ThingGroupName}`	aws:ResourceTag/${TagKey} (p. 1254)
thingtype	`arn:${Partition}:iot:${Region}:${Account}:thingtype/${ThingTypeName}`	aws:ResourceTag/${TagKey} (p. 1254)

리소스 유형	ARN	조건 키
topic	`arn:${Partition}:iot:${Region}:${Account}:topic/${TopicName}`	
topicfilter	`arn:${Partition}:iot:${Region}:${Account}:topicfilter/${TopicFilter}`	
rolealias	`arn:${Partition}:iot:${Region}:${Account}:rolealias/${RoleAlias}`	
role	`arn:${Partition}:iam::${Account}:role/${Role}`	
authorizer	`arn:${Partition}:iot:${Region}:${Account}:authorizer/${AuthorizerName}`	
policy	`arn:${Partition}:iot:${Region}:${Account}:policy/${PolicyName}`	
cert	`arn:${Partition}:iot:${Region}:${Account}:cert/${Certificate}`	
cacert	`arn:${Partition}:iot:${Region}:${Account}:cacert/${CACertificate}`	
stream	`arn:${Partition}:iot:${Region}:${Account}:stream/${streamId}`	aws:ResourceTag/${TagKey} (p. 1254)
otaupdate	`arn:${Partition}:iot:${Region}:${Account}:otaupdate/${otaUpdateId}`	aws:ResourceTag/${TagKey} (p. 1254)
scheduledaudit	`arn:${Partition}:iot:${Region}:${Account}:scheduledaudit/${ScheduleName}`	aws:ResourceTag/${TagKey} (p. 1254)
securityprofile	`arn:${Partition}:iot:${Region}:${Account}:securityprofile/${SecurityProfileName}`	aws:ResourceTag/${TagKey} (p. 1254)
rule	`arn:${Partition}:iot:${Region}:${Account}:rule/${ruleName}`	aws:ResourceTag/${TagKey} (p. 1254)
provisioningtemplate	`arn:${Partition}:iot:${Region}:${Account}:provisioningtemplate/${provisioningTemplate}`	

AWS IoT의 조건 키

AWS IoT는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	IoT에 대한 사용자의 요청에 있는 태그 키입니다.	문자열
aws:ResourceTag/${TagKey}	IoT 리소스에 연결된 태그의 태그 키 구성 요소입니다.	문자열
aws:TagKeys	요청의 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열
iot:Delete	IoT 터널을 즉시 삭제할지 여부를 나타내는 플래그입니다.	Bool
iot:ThingGroupArn	IoT 터널에서 대상 IoT가 속하는 모든 IoT 사물 그룹 ARN의 목록입니다.	문자열
iot:TunnelDestinationService	IoT 터널에 대한 모든 대상 서비스의 목록입니다.	문자열

AWS IoT 1-Click에 사용되는 작업, 리소스 및 조건 키

AWS IoT 1-Click(서비스 접두사: `iot1click`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS IoT 1-Click에서 정의한 작업 (p. 1254)
- AWS IoT 1-Click에서 정의한 리소스 유형 (p. 1256)
- AWS IoT 1-Click의 조건 키 (p. 1257)

AWS IoT 1-Click에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateDeviceWithPlacement	배치에 디바이스 연결	쓰기	project* (p. 1257)		
ClaimDevicesByClaimCode	신청 코드로 디바이스의 배치 신청	Read			
CreatePlacement	프로젝트에서 새 배치 생성	쓰기	project* (p. 1257)		
CreateProject	새 프로젝트를 생성합니다	쓰기	project* (p. 1257)		
				aws:RequestTag/${TagKey} (p. 1257) aws:TagKeys (p. 1257)	
DeletePlacement	프로젝트에서 배치 삭제	쓰기	project* (p. 1257)		
DeleteProject	프로젝트 삭제	쓰기	project* (p. 1257)		
DescribeDevice	디바이스 설명	Read	device* (p. 1257)		
DescribePlacement	배치 설명	Read	project* (p. 1257)		
DescribeProject	프로젝트 설명	Read	project* (p. 1257)		
DisassociateDeviceFromPlacement	배치에서 디바이스 연결 해제	쓰기	project* (p. 1257)		
FinalizeDeviceClaim	디바이스 신청 완료	Read	device* (p. 1257)		
				aws:RequestTag/${TagKey} (p. 1257) aws:TagKeys (p. 1257)	
GetDeviceMethods	디바이스의 사용 가능한 메서드 가져오기	Read	device* (p. 1257)		
GetDevicesInPlacement	배치에 연결된 디바이스 가져오기	Read	project* (p. 1257)		
InitiateDeviceClaim	디바이스 신청 초기화	Read	device* (p. 1257)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
InvokeDeviceMethod	디바이스 메서드 호출	쓰기	device* (p. 1257)		
ListDeviceEvents	디바이스에서 게시한 지난 이벤트 나열	Read	device* (p. 1257)		
ListDevices	모든 디바이스 나열	List			
ListPlacements	프로젝트의 배치 나열	Read	project* (p. 1257)		
ListProjects	모든 프로젝트 나열	List			
ListTagsForResource	리소스에 할당한 태그(메타데이터)를 열거합니다.	List	device (p. 1257)		
			project (p. 1257)		
TagResource	특정 리소스에 태그를 추가하거나 수정합니다. 태그는 리소스 관리에 사용할 수 있는 메타데이터입니다.	쓰기	device (p. 1257)		
			project (p. 1257)		
				aws:RequestTag/${TagKey} (p. 1257) aws:TagKeys (p. 1257)	
UnclaimDevice	디바이스 신청 취소	Read	device* (p. 1257)		
UntagResource	리소스에서 특정 태그(메타데이터)를 제거합니다.	쓰기	device (p. 1257)		
			project (p. 1257)		
				aws:TagKeys (p. 1257)	
UpdateDeviceState	디바이스 상태 업데이트	쓰기	device* (p. 1257)		
UpdatePlacement	배치 업데이트	쓰기	project* (p. 1257)		
UpdateProject	프로젝트 업데이트	쓰기	project* (p. 1257)		

AWS IoT 1-Click에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1254)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유

형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
device	`arn:${Partition}:iot1click:${Region}:${Account}:devices/${DeviceId}`	aws:ResourceTag/${TagKey} (p. 1257)
project	`arn:${Partition}:iot1click:${Region}:${Account}:projects/${ProjectName}`	aws:ResourceTag/${TagKey} (p. 1257)

AWS IoT 1-Click의 조건 키

AWS IoT 1-Click은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	IoT 1-Click에 대한 사용자의 요청에 있는 태그 키입니다.	문자열
aws:ResourceTag/${TagKey}	IoT 1-Click 리소스에 연결된 태그 키-값 페어의 서문 문자열입니다.	문자열
aws:TagKeys	요청의 IoT 1-Click 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열

AWS IoT Analytics에 사용되는 작업, 리소스 및 조건 키

AWS IoT Analytics(서비스 접두사: `iotanalytics`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS IoT Analytics에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchPutMessage	메시지의 배치를 지정된 채널로 가져옵니다.	쓰기	channel* (p. 1261)		
CancelPipelineReprocessing	지정된 파이프라인에 대한 재처리를 취소합니다.	쓰기	pipeline* (p. 1261)		
CreateChannel	채널을 생성합니다.	쓰기	channel* (p. 1261)		
				aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262)	
CreateDataset	데이터 세트를 생성합니다.	쓰기	dataset* (p. 1261)		
				aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262)	
CreateDatasetContent	지정된 데이터 세트의 내용을 생성합니다(데이터 세트 작업을 실행하여).	쓰기	dataset* (p. 1261)		
CreateDatastore	데이터 스토어를 생성합니다.	쓰기	datastore* (p. 1261)		
				aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262)	
CreatePipeline	파이프라인을 생성합니다.	쓰기	pipeline* (p. 1261)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262)	
DeleteChannel	지정된 채널을 삭제합니다.	쓰기	channel* (p. 1261)		
DeleteDataset	지정된 데이터 세트를 삭제합니다.	쓰기	dataset* (p. 1261)		
DeleteDatasetContent	지정된 데이터 세트의 내용을 삭제합니다.	쓰기	dataset* (p. 1261)		
DeleteDatastore	지정된 데이터 스토어를 삭제합니다.	쓰기	datastore* (p. 1261)		
DeletePipeline	지정된 파이프라인을 삭제합니다.	쓰기	pipeline* (p. 1261)		
DescribeChannel	지정된 채널을 설명합니다.	Read	channel* (p. 1261)		
DescribeDataset	지정된 데이터 세트를 설명합니다.	Read	dataset* (p. 1261)		
DescribeDatastore	지정된 데이터 스토어를 설명합니다.	Read	datastore* (p. 1261)		
DescribeLoggingOptions	계정에 대한 로깅 옵션을 설명합니다.	Read			
DescribePipeline	지정된 파이프라인을 설명합니다.	Read	pipeline* (p. 1261)		
GetDatasetContent	지정된 데이터 세트의 내용을 가져옵니다.	Read	dataset* (p. 1261)		
ListChannels	계정에 대한 채널을 나열합니다.	List			
ListDatasets	계정에 대한 데이터 세트를 나열합니다.	List			
ListDatastores	계정에 대한 데이터 스토어를 나열합니다.	List			
ListPipelines	계정에 대한 파이프라인을 나열합니다.	List			
ListTagsForResource	리소스에 할당한 태그(메타데이터)를 열거합니다.	Read	channel (p. 1261)		
			dataset (p. 1261)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			datastore (p. 1261)		
			pipeline (p. 1261)		
PutLoggingOptions	계정에 대한 로깅 옵션을 설정합니다.	쓰기			
RunPipelineActivity	지정된 파이프라인 활동을 실행합니다.	Read			
SampleChannelData	지정된 채널의 데이터를 샘플링합니다.	Read	channel* (p. 1261)		
StartPipelineReprocessing	지정된 파이프라인에 대한 재처리를 시작합니다.	쓰기	pipeline* (p. 1261)		
TagResource	특정 리소스에 태그를 추가하거나 수정합니다. 태그는 리소스 관리에 사용할 수 있는 메타데이터입니다.	태그 지정	channel (p. 1261)		
			dataset (p. 1261)		
			datastore (p. 1261)		
			pipeline (p. 1261)		
				aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262)	
UntagResource	리소스에서 특정 태그(메타데이터)를 제거합니다.	태그 지정	channel (p. 1261)		
			dataset (p. 1261)		
			datastore (p. 1261)		
			pipeline (p. 1261)		
				aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateChannel	지정된 채널을 업데이트합니다.	쓰기	channel* (p. 1261)		
UpdateDataset	지정된 데이터 세트를 업데이트합니다.	쓰기	dataset* (p. 1261)		
UpdateDatastore	지정된 데이터 스토어를 업데이트합니다.	쓰기	datastore* (p. 1261)		
UpdatePipeline	지정된 파이프라인을 업데이트합니다.	쓰기	pipeline* (p. 1261)		

AWS IoT Analytics에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1257)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
channel	`arn:${Partition}:iotanalytics:${Region}:${Account}:channel/${ChannelName}`	aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262) iotanalytics:ResourceTag/${TagKey} (p. 1262)
dataset	`arn:${Partition}:iotanalytics:${Region}:${Account}:dataset/${DatasetName}`	aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262) iotanalytics:ResourceTag/${TagKey} (p. 1262)
datastore	`arn:${Partition}:iotanalytics:${Region}:${Account}:datastore/${DatastoreName}`	aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262) iotanalytics:ResourceTag/${TagKey} (p. 1262)
pipeline	`arn:${Partition}:iotanalytics:${Region}:${Account}:pipeline/${PipelineName}`	aws:RequestTag/${TagKey} (p. 1262) aws:TagKeys (p. 1262)

리소스 유형	ARN	조건 키
		iotanalytics:ResourceTag/${TagKey} (p. 1262)

AWS IoT Analytics에 사용되는 조건 키

AWS IoT Analytics는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	IoT Analytics에 대한 사용자의 요청에 있는 태그 키입니다.	문자열
aws:TagKeys	요청의 IoT Analytics 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열
iotanalytics:ResourceTag/${TagKey}	IoT Analytics 리소스에 연결된 태그 키-값 페어의 서문 문자열입니다.	문자열

AWS IoT Device Tester에 사용할 수 있는 작업, 리소스 및 조건 키

AWS IoT Device Tester(서비스 접두사: `iot-device-tester`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에서 사용할 수 있는 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS IoT Device Tester에서 정의한 작업 (p. 1262)
- AWS IoT Device Tester에서 정의한 리소스 유형 (p. 1263)
- AWS IoT Device Tester에 대한 조건 키 (p. 1263)

AWS IoT Device Tester에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CheckVersion	IoT Device Tester가 지정된 제품, 테스트 제품군 및 디바이스 테스터 버전의 호환성을 확인할 수 있는 권한을 부여합니다.	Read			
DownloadTestSuite	IoT Device Tester가 호환되는 테스트 제품군 버전을 다운로드할 수 있는 권한을 부여합니다.	Read			
LatestIdt	IoT Device Tester가 사용 가능한 최신 버전의 디바이스 테스터에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read			
SendMetrics	IoT Device Tester가 사용자를 대신하여 사용량 지표를 전송할 수 있도록 권한을 부여	쓰기			
SupportedVersion	IoT Device Tester가 지원되는 제품 및 테스트 제품군 버전 목록을 가져올 수 있는 권한을 부여합니다.	Read			

AWS IoT Device Tester에서 정의한 리소스 유형

AWS IoT Device Tester는 IAM 정책 문의 `Resource` 요소에서 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS IoT Device Tester에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`을 지정합니다.

AWS IoT Device Tester에 대한 조건 키

IoT Device Tester에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS IoT Events에 사용되는 작업, 리소스 및 조건 키

AWS IoT Events(서비스 접두사: `iotevents`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS IoT Events에서 정의한 작업 (p. 1264)
- AWS IoT Events에서 정의한 리소스 유형 (p. 1266)

- AWS IoT Events에 사용되는 조건 키 (p. 1266)

AWS IoT Events에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchPutMessage	AWS IoT Events 시스템에 일련의 메시지를 보냅니다.	쓰기	input* (p. 1266)		
BatchUpdateDetector	AWS IoT Events 시스템에서 감지기를 업데이트합니다.	쓰기	input* (p. 1266)		
CreateDetectorModel	감지기 모델을 생성합니다.	쓰기	detectorModel* (p. 1266)		
				aws:RequestTag/${TagKey} (p. 1266) aws:TagKeys (p. 1266)	
CreateInput	입력을 생성합니다.	쓰기	input* (p. 1266)		
				aws:RequestTag/${TagKey} (p. 1266) aws:TagKeys (p. 1266)	
DeleteDetectorModel	감지기 모델을 삭제합니다.	쓰기	detectorModel* (p. 1266)		
DeleteInput	입력을 삭제합니다.	쓰기	input* (p. 1266)		
DescribeDetector	지정된 감지기(인스턴스)에 대한 정보를 반환합니다.	Read	detectorModel* (p. 1266)		
DescribeDetectorModel	감지기 모델을 설명합니다.	Read	detectorModel* (p. 1266)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeInput	입력을 설명합니다.	Read	input* (p. 1266)		
DescribeLoggingOptions	AWS IoT Events 로깅 옵션의 현재 설정을 가져옵니다.	Read			
ListDetectorModelVersions	감지기 모델의 모든 버전을 나열합니다. 각 감지기 모델 버전과 연결된 메타데이터만 반환됩니다.	List	detectorModel* (p. 1266)		
ListDetectorModels	사용자가 생성한 감지기 모델을 나열합니다. 각 감지기 모델과 연결된 메타데이터만 반환됩니다.	List			
ListDetectors	감지기(감지기 모델의 인스턴스)를 나열합니다.	List	detectorModel* (p. 1266)		
ListInputs	사용자가 생성한 입력을 나열합니다.	List			
ListTagsForResource	리소스에 할당한 태그(메타데이터)를 열거합니다.	Read	detectorModel (p. 1266)		
			input (p. 1266)		
PutLoggingOptions	AWS IoT Events 로깅 옵션을 설정하거나 업데이트합니다.	쓰기			
TagResource	특정 리소스에 태그를 추가하거나 수정합니다. 태그는 리소스 관리에 사용할 수 있는 메타데이터입니다.	태그 지정	detectorModel (p. 1266)		
			input (p. 1266)		
				aws:RequestTag/${TagKey} (p. 1266) aws:TagKeys (p. 1266)	
UntagResource	리소스에서 특정 태그(메타데이터)를 제거합니다.	태그 지정	detectorModel (p. 1266)		
			input (p. 1266)		
				aws:TagKeys (p. 1266)	
UpdateDetectorModel	감지기 모델을 업데이트합니다.	쓰기	detectorModel* (p. 1266)		
UpdateInput	입력을 업데이트합니다.	쓰기	input* (p. 1266)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateInputRouting	입력 라우팅을 업데이트합니다.	쓰기	input* (p. 1266)		

AWS IoT Events에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1264)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
detectorModel	`arn:${Partition}:iotevents:${Region}:${Account}:detectorModel/${DetectorModelName}`	aws:ResourceTag/${TagKey} (p. 1266)
input	`arn:${Partition}:iotevents:${Region}:${Account}:input/${inputName}`	aws:ResourceTag/${TagKey} (p. 1266)

AWS IoT Events에 사용되는 조건 키

AWS IoT Events는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	IoT Events에 대한 사용자의 요청에 있는 태그 키입니다.	문자열
aws:ResourceTag/${TagKey}	태그 값이 IoT Events 리소스에 연결된 태그 키입니다.	문자열
aws:TagKeys	요청의 IoT Events 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열

AWS IoT Greengrass에 사용되는 작업, 리소스 및 조건 키

AWS IoT Greengrass(서비스 접두사: `greengrass`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS IoT Greengrass에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateRoleToGroup	역할을 그룹과 연결할 수 있는 권한을 부여합니다. 이 역할의 권한은 Greengrass 코어 Lambda 함수 및 연결이 다른 AWS 서비스에서 작업을 수행하도록 허용하지 않습니다.	쓰기	group* (p. 1276)		
AssociateServiceRoleToAccount	역할을 계정과 연결할 수 있는 권한을 부여합니다. AWS IoT Greengrass는 이 역할을 사용하여 Lambda 함수 및 AWS IoT 리소스에 액세스합니다.	권한 관리			
CreateConnectorDefinition	커넥터 정의를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
CreateConnectorDefinitionVersion	기존 커넥터 정의의 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	connectorDefinition* (p. 1277)		
CreateCoreDefinition	코어 정의를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
CreateCoreDefinitionVersion	기존 코어 정의의 버전을 생성할 수 있는 권한을 부여합니다. Greengrass 그룹에는 각각 정확	쓰기	coreDefinition* (p. 1276)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	히 1개의 Greengrass 코어가 있어야 합니다.				
CreateDeployment	배포를 생성할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1276)		
CreateDeviceDefinition	디바이스 정의를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
CreateDeviceDefinitionVersion	기존 디바이스 정의의 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	deviceDefinition* (p. 1276)		
CreateFunctionDefinition	Lambda 함수 및 구성의 목록이 포함된, 그룹에서 사용할 Lambda 함수 정의를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
CreateFunctionDefinitionVersion	기존 Lambda 함수 정의의 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	functionDefinition* (p. 1276)		
CreateGroup	그룹을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
CreateGroupCertificateAuthority	그룹에 대한 CA를 생성하거나 기존 CA를 교체할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1276)		
CreateGroupVersion	이미 정의된 그룹의 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1276)		
CreateLoggerDefinition	로거 정의를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
CreateLoggerDefinitionVersion	기존 로거 정의의 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	loggerDefinition* (p. 1276)		
CreateResourceDefinition	리소스의 목록이 포함된, 그룹에서 사용할 리소스 정의를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateResourceDefinitionVersion	기존 리소스 정의의 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	resourceDefinition* (p. 1277)		
CreateSoftwareUpdateJob	Greengrass 코어를 트리거하여 실행 중인 소프트웨어를 업데이트할 AWS IoT 작업을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateSubscriptionDefinition	구독 정의를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
CreateSubscriptionDefinitionVersion	기존 구독 정의의 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	subscriptionDefinition* (p. 1276)		
DeleteConnectorDefinition	커넥터 정의를 삭제할 수 있는 권한을 부여합니다.	쓰기	connectorDefinition* (p. 1277)		
DeleteCoreDefinition	코어 정의를 삭제할 수 있는 권한을 부여합니다. 배포에서 현재 사용 중인 정의를 삭제하면 향후 배포에 영향을 미칩니다.	쓰기	coreDefinition* (p. 1276)		
DeleteDeviceDefinition	디바이스 정의를 삭제할 수 있는 권한을 부여합니다. 배포에서 현재 사용 중인 정의를 삭제하면 향후 배포에 영향을 미칩니다.	쓰기	deviceDefinition* (p. 1276)		
DeleteFunctionDefinition	Lambda 함수 정의를 삭제할 수 있는 권한을 부여합니다. 배포에서 현재 사용 중인 정의를 삭제하면 향후 배포에 영향을 미칩니다.	쓰기	functionDefinition* (p. 1276)		
DeleteGroup	배포에서 현재 사용되지 않는 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1276)		
DeleteLoggerDefinition	로거 정의를 삭제할 수 있는 권한을 부여합니다. 배포에서 현재 사용 중인 정의를 삭제하면 향후 배포에 영향을 미칩니다.	쓰기	loggerDefinition* (p. 1276)		
DeleteResourceDefinition	리소스 정의를 삭제할 수 있는 권한을 부여합니다.	쓰기	resourceDefinition* (p. 1277)		
DeleteSubscriptionDefinition	구독 정의를 삭제할 수 있는 권한을 부여합니다. 배포에서 현재 사용 중인 정의를 삭제하면 향후 배포에 영향을 미칩니다.	쓰기	subscriptionDefinition* (p. 1276)		
DisassociateRoleFromGroup	그룹에서 역할을 연결 해제할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1276)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DisassociateServiceRoleFromAccount	계정에서 서비스 역할을 연결 해제할 수 있는 권한을 부여합니다. 서비스 역할이 없으면 배포가 작동하지 않습니다.	쓰기			
GetAssociatedRole	그룹과 연결된 역할을 검색할 수 있는 권한을 부여합니다.	Read	group* (p. 1276)		
GetBulkDeploymentStatus	대량 배포의 상태를 반환할 수 있는 권한을 부여합니다.	Read	bulkDeployment* (p. 1276)		
GetConnectivityInfo	코어의 연결 정보를 검색할 수 있는 권한을 부여합니다.	Read	connectivityInfo* (p. 1275)		
GetConnectorDefinition	커넥터 정의에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	connectorDefinition* (p. 1277)		
GetConnectorDefinitionVersion	커넥터 정의 버전에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	connectorDefinition* (p. 1277)		
			connectorDefinitionVersion* (p. 1277)		
GetCoreDefinition	코어 정의에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	coreDefinition* (p. 1276)		
GetCoreDefinitionVersion	코어 정의 버전에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	coreDefinition* (p. 1276)		
			coreDefinitionVersion* (p. 1276)		
GetDeploymentStatus	배포의 상태를 반환할 수 있는 권한을 부여합니다.	Read	deployment* (p. 1276)		
			group* (p. 1276)		
GetDeviceDefinition	디바이스 정의에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	deviceDefinition* (p. 1276)		
GetDeviceDefinitionVersion	디바이스 정의 버전에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	deviceDefinition* (p. 1276)		
			deviceDefinitionVersion* (p. 1276)		
GetFunctionDefinition	생성 시간, 최신 버전 등 Lambda 함수 정의에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	functionDefinition* (p. 1276)		
GetFunctionDefinitionVersion	버전에 포함된 Lambda 함수 및 구성 등 Lambda 함수 정의 버전에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	functionDefinition* (p. 1276)		
			functionDefinitionVersion* (p. 1276)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetGroup	그룹에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	group* (p. 1276)		
GetGroupCertificateAuthority	그룹과 연결된 CA의 퍼블릭 키를 반환할 수 있는 권한을 부여합니다.	Read	certificateAuthority* (p. 1275)		
			group* (p. 1276)		
GetGroupCertificateConfiguration	그룹이 사용하는 CA의 현재 구성을 검색할 수 있는 권한을 부여합니다.	Read	group* (p. 1276)		
GetGroupVersion	그룹 버전에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	group* (p. 1276)		
			groupVersion* (p. 1276)		
GetLoggerDefinition	로거 정의에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	loggerDefinition* (p. 1276)		
GetLoggerDefinitionVersion	로거 정의 버전에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	loggerDefinition* (p. 1276)		
			loggerDefinitionVersion* (p. 1277)		
GetResourceDefinition	생성 시간, 최신 버전 등 리소스 정의에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	resourceDefinition* (p. 1277)		
GetResourceDefinitionVersion	버전에 포함된 리소스 등 리소스 정의 버전에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	resourceDefinition* (p. 1277)		
			resourceDefinitionVersion* (p. 1277)		
GetServiceRoleForAccount	계정에 연결된 서비스 역할을 검색할 수 있는 권한을 부여합니다.	Read			
GetSubscriptionDefinition	구독 정의에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	subscriptionDefinition* (p. 1276)		
GetSubscriptionDefinitionVersion	구독 정의 버전에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	subscriptionDefinition* (p. 1276)		
			subscriptionDefinitionVersion* (p. 1276)		
ListBulkDeploymentDetailedReports	대량 배포 작업에서 시작된 배포 및 현재 배포 상태의 페이지 매김 목록을 검색할 수 있는 권한을 부여합니다.	List	bulkDeployment* (p. 1276)		
ListBulkDeployments	대량 배포의 목록을 검색할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListConnectorDefinitionVersions	커넥터 정의의 버전을 나열할 수 있는 권한을 부여합니다.	List	connectorDefinition* (p. 1277)		
ListConnectorDefinitions	커넥터 정의의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListCoreDefinitionVersions	코어 정의의 버전을 나열할 수 있는 권한을 부여합니다.	List	coreDefinition* (p. 1276)		
ListCoreDefinitions	코어 정의의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListDeployments	그룹의 모든 배포의 목록을 검색할 수 있는 권한을 부여합니다.	List	group* (p. 1276)		
ListDeviceDefinitionVersions	디바이스 정의의 버전을 나열할 수 있는 권한을 부여합니다.	List	deviceDefinition* (p. 1276)		
ListDeviceDefinitions	디바이스 정의의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListFunctionDefinitionVersions	Lambda 함수 정의의 버전을 나열할 수 있는 권한을 부여합니다.	List	functionDefinition* (p. 1276)		
ListFunctionDefinitions	Lambda 함수 정의의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListGroupCertificateAuthorities	그룹에 대한 현재 CA의 목록을 검색할 수 있는 권한을 부여합니다.	List	group* (p. 1276)		
ListGroupVersions	그룹의 버전을 나열할 수 있는 권한을 부여합니다.	List	group* (p. 1276)		
ListGroups	그룹의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListLoggerDefinitionVersions	로거 정의의 버전을 나열할 수 있는 권한을 부여합니다.	List	loggerDefinition* (p. 1276)		
ListLoggerDefinitions	로거 정의의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListResourceDefinitionVersions	리소스 정의의 버전을 나열할 수 있는 권한을 부여합니다.	List	resourceDefinition* (p. 1277)		
ListResourceDefinitions	리소스 정의의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListSubscriptionDefinitionVersions	구독 정의의 버전을 나열할 수 있는 권한을 부여합니다.	List	subscriptionDefinition* (p. 1276)		
ListSubscriptionDefinitions	구독 정의의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.	List	bulkDeployment (p. 1276)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			connectorDefinition (p. 1277)		
			coreDefinition (p. 1276)		
			deviceDefinition (p. 1276)		
			functionDefinition (p. 1276)		
			group (p. 1276)		
			loggerDefinition (p. 1276)		
			resourceDefinition (p. 1277)		
			subscriptionDefinition (p. 1276)		
				aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
ResetDeployments	그룹의 배포를 재설정할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1276)		
StartBulkDeployment	한 작업으로 여러 그룹을 배포할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
StopBulkDeployment	대량 배포의 실행을 중지할 수 있는 권한을 부여합니다.	쓰기	bulkDeployment* (p. 1276)		
TagResource	리소스에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	bulkDeployment (p. 1276)		
			connectorDefinition (p. 1277)		
			coreDefinition (p. 1276)		
			deviceDefinition (p. 1276)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			functionDefinition (p. 1276)		
			group (p. 1276)		
			loggerDefinition (p. 1276)		
			resourceDefinition (p. 1277)		
			subscriptionDefinition (p. 1276)		
				aws:RequestTag/${TagKey} (p. 1277) aws:TagKeys (p. 1278)	
UntagResource	리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	bulkDeployment (p. 1276)		
			connectorDefinition (p. 1277)		
			coreDefinition (p. 1276)		
			deviceDefinition (p. 1276)		
			functionDefinition (p. 1276)		
			group (p. 1276)		
			loggerDefinition (p. 1276)		
			resourceDefinition (p. 1277)		
			subscriptionDefinition (p. 1276)		
				aws:TagKeys (p. 1278)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateConnectivityInfo	Greengrass 코어의 연결 정보를 업데이트할 수 있는 권한을 부여합니다. 이 코어가 있는 그룹에 속한 모든 디바이스는 이 정보를 수신하여 코어의 위치를 찾고 해당 코어에 연결합니다.	쓰기	connectivityInfo* (p. 1275)		
UpdateConnectorDefinition	커넥터 정의를 업데이트할 수 있는 권한을 부여합니다.	쓰기	connectorDefinition* (p. 1277)		
UpdateCoreDefinition	코어 정의를 업데이트할 수 있는 권한을 부여합니다.	쓰기	coreDefinition* (p. 1276)		
UpdateDeviceDefinition	디바이스 정의를 업데이트할 수 있는 권한을 부여합니다.	쓰기	deviceDefinition* (p. 1276)		
UpdateFunctionDefinition	Lambda 함수 정의를 업데이트할 수 있는 권한을 부여합니다.	쓰기	functionDefinition* (p. 1276)		
UpdateGroup	그룹을 업데이트할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1276)		
UpdateGroupCertificateConfiguration	그룹의 인증서 만료 시간을 업데이트할 수 있는 권한을 부여합니다.	쓰기	group* (p. 1276)		
UpdateLoggerDefinition	로거 정의를 업데이트할 수 있는 권한을 부여합니다.	쓰기	loggerDefinition* (p. 1276)		
UpdateResourceDefinition	리소스 정의를 업데이트할 수 있는 권한을 부여합니다.	쓰기	resourceDefinition* (p. 1277)		
UpdateSubscriptionDefinition	구독 정의를 업데이트할 수 있는 권한을 부여합니다.	쓰기	subscriptionDefinition* (p. 1276)		

AWS IoT Greengrass에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1267)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
artifact	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/deployments/${DeploymentId}/artifacts/lambda/${ArtifactId}`	
certificateAuthority	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/`	

리소스 유형	ARN	조건 키
	`${GroupId}/certificateauthorities/${CertificateAuthorityId}`	
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/deployments/${DeploymentId}`	
bulkDeployment	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/bulk/deployments/${BulkDeploymentId}`	aws:ResourceTag/${TagKey} (p. 1277)
group	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}`	aws:ResourceTag/${TagKey} (p. 1277)
groupVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/versions/${VersionId}`	
coreDefinition	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}`	aws:ResourceTag/${TagKey} (p. 1277)
coreDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}/versions/${VersionId}`	
deviceDefinition	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}`	aws:ResourceTag/${TagKey} (p. 1277)
deviceDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}/versions/${VersionId}`	
functionDefinition	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}`	aws:ResourceTag/${TagKey} (p. 1277)
functionDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}/versions/${VersionId}`	
subscriptionDefinition	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}`	aws:ResourceTag/${TagKey} (p. 1277)
subscriptionDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}/versions/${VersionId}`	
loggerDefinition	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}`	aws:ResourceTag/${TagKey} (p. 1277)

리소스 유형	ARN	조건 키
loggerDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}/versions/${VersionId}`	
resourceDefinition	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}`	aws:ResourceTag/${TagKey} (p. 1277)
resourceDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}/versions/${VersionId}`	
connectorDefinition	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}`	aws:ResourceTag/${TagKey} (p. 1277)
connectorDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}/versions/${VersionId}`	

AWS IoT Greengrass의 조건 키

AWS IoT Greengrass는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:CurrentTime	현재 날짜 및 시간에 대한 날짜/시간 조건을 확인하여 액세스를 필터링합니다.	날짜
aws:EpochTime	Epoch 또는 UNIX 시간의 현재 날짜 및 시간에 대한 날짜/시간 조건을 확인하여 액세스를 필터링합니다.	날짜
aws:MultiFactorAuthAge	Multi-Factor Authentication(MFA)을 사용하여 발행된 요청에서 MFA가 유효성을 검사한 보안 자격 증명이 경과한 시간(단위: 초)을 확인하여 액세스를 필터링합니다.	숫자
aws:MultiFactorAuthPresent	Multi-Factor Authentication(MFA)을 사용하여 현재 요청을 수행한 임시 보안 자격 증명의 유효성을 검사했는지 여부를 확인하여 액세스를 필터링합니다.	부울
aws:RequestTag/${TagKey}	각 필수 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그 값을 기준으로 작업을 필터링합니다.	문자열
aws:SecureTransport	SSL을 사용하여 요청을 보냈는지 여부를 확인하여 액세스를 필터링합니다.	부울

조건 키	설명	유형
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열
aws:UserAgent	요청자의 클라이언트 애플리케이션을 기준으로 액세스를 필터링합니다.	문자열

AWS IoT SiteWise에 사용되는 작업, 리소스 및 조건 키

AWS IoT SiteWise(서비스 접두사: `iotsitewise`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS IoT SiteWise에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateAssets	지정된 모델 계층 구조를 통해 하위 자산을 상위 자산에 연결합니다.	쓰기	asset* (p. 1284)		
AssociateViewEntities	지정된 그룹에 대한 보기 내에서 지정된 엔터티를 연결합니다.	쓰기	group* (p. 1284)		
			view* (p. 1284)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			asset (p. 1284)		
BatchAssociateProjectAssets	지정된 프로젝트에 자산을 연결할 수 있는 권한을 부여합니다.	쓰기	project* (p. 1284)		
BatchDisassociateProjectAssets	지정된 프로젝트에서 자산을 연결 해제할 수 있는 권한을 부여합니다.	쓰기	project* (p. 1284)		
BatchPutAssetPropertyValue	지정된 속성에 대한 속성 값의 배치를 보냅니다.	쓰기	asset* (p. 1284)		
CreateAccessPolicy	지정된 포털 또는 프로젝트에 대한 액세스 정책을 생성할 수 있는 권한을 부여합니다.	권한 관리	portal (p. 1284)		
			project (p. 1284)		
CreateAsset	자산을 생성합니다.	쓰기	asset-model* (p. 1284)		
CreateAssetModel	자산 모형을 생성합니다.	쓰기			
CreateAssetTemplate	자산 템플릿을 생성합니다.	쓰기			
CreateDashboard	지정된 프로젝트 내에서 대시보드를 생성할 수 있는 권한을 부여합니다.	쓰기	project* (p. 1284)		
CreateGroup	그룹을 생성합니다.	쓰기			
CreateMeasurementDataStore	측정 데이터 스토어를 등록합니다.	쓰기			
CreateMetricType	지표 유형을 생성합니다.	쓰기			
CreatePortal	포털을 생성할 수 있는 권한을 부여합니다.	쓰기			sso:CreateManagedAppli
CreateProject	지정된 포털 내에서 프로젝트를 생성할 수 있는 권한을 부여합니다.	쓰기	portal* (p. 1284)		
CreateView	보기를 생성합니다.	쓰기			
DeleteAccessPolicy	지정된 액세스 정책을 삭제할 수 있는 권한을 부여합니다.	권한 관리	access-policy* (p. 1284)		
DeleteAsset	지정된 자산을 삭제합니다.	쓰기	asset* (p. 1284)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteAssetModel	지정된 자산 모델을 삭제합니다.	쓰기	asset-model* (p. 1284)		
DeleteAssetTemplate	지정된 자산 템플릿을 삭제합니다.	쓰기	asset-template* (p. 1284)		
DeleteDashboard	지정된 대시보드를 삭제할 수 있는 권한을 부여합니다.	쓰기	dashboard* (p. 1284)		
DeleteGroup	지정된 그룹을 삭제합니다.	쓰기	group* (p. 1284)		
DeleteMeasurementDataStore	지정된 측정 데이터 스토어를 등록 취소합니다.	쓰기	measurement-data-store* (p. 1284)		
DeleteMetricType	지정된 지표 유형을 삭제합니다.	쓰기	metric-type* (p. 1284)		
DeletePortal	지정된 포털을 삭제할 수 있는 권한을 부여합니다.	쓰기	portal* (p. 1284)		sso:DeleteManagedApplic
DeleteProject	지정된 프로젝트를 삭제할 수 있는 권한을 부여합니다.	쓰기	project* (p. 1284)		
DeleteView	지정된 보기를 삭제합니다.	쓰기	view* (p. 1284)		
DeregisterViewEntities	지정된 보기에서 지정된 자산 및 그룹을 등록 취소합니다.	쓰기	view* (p. 1284)		
			asset (p. 1284)		
			group (p. 1284)		
DescribeAccessPolicy	지정된 액세스 정책을 설명할 수 있는 권한을 부여합니다.	권한 관리	access-policy* (p. 1284)		
DescribeAsset	지정된 자산을 설명합니다.	Read	asset* (p. 1284)		
DescribeAssetModel	지정된 자산 모델을 설명합니다.	Read	asset-model* (p. 1284)		
DescribeAssetProperty	지정된 자산 속성을 설명합니다.	Read	asset* (p. 1284)		
DescribeAssetTemplates	지정된 자산 템플릿을 설명합니다.	Read	asset-template* (p. 1284)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeAssets	지정된 자산을 설명합니다.	Read	asset* (p. 1284)		
DescribeDashboard	지정된 대시보드를 설명할 수 있는 권한을 부여합니다.	Read	dashboard* (p. 1284)		
DescribeGroups	계정의 그룹을 설명합니다.	Read	group* (p. 1284)		
DescribeLoggingOptions	계정에 대한 로깅 옵션을 설명합니다.	Read			
DescribeMeasurementDataStores	지정된 측정 데이터 스토어를 설명합니다.	Read	measurement-data-store* (p. 1284)		
DescribeMetricTypes	계정의 지표 유형을 설명합니다.	Read	metric-type* (p. 1284)		
DescribePortal	지정된 포털을 설명할 수 있는 권한을 부여합니다.	Read	portal* (p. 1284)		
DescribeProject	지정된 프로젝트를 설명할 수 있는 권한을 부여합니다.	Read	project* (p. 1284)		
DescribeViews	지정된 보기를 설명합니다.	Read	view* (p. 1284)		
DisassociateAssets	지정된 모델 계층 구조에서 상위 자산과 하위 자산의 연결을 해제합니다.	쓰기	asset* (p. 1284)		
DisassociateViewEntities	지정된 그룹에 대한 보기 내에서 지정된 엔터티를 연결 해제합니다.	쓰기	group* (p. 1284)		
			view* (p. 1284)		
			asset (p. 1284)		
GetAssetPropertyAggregates	지정된 속성에 대해 집계된 속성 값을 가져옵니다.	Read	asset* (p. 1284)		
GetAssetPropertyValue	지정된 속성에 대한 최신 속성 값을 가져옵니다.	Read	asset* (p. 1284)		
GetAssetPropertyValueHistory	지정된 속성에 대한 속성 값 기록을 가져옵니다.	Read	asset* (p. 1284)		
GetMeasurementData	지정된 측정 및 시간 간격의 측정 데이터를 가져옵니다.	Read	measurement* (p. 1284)		
GetMetricData	지정된 지표 및 시간 간격의 지표 데이터를 가져옵니다.	Read	metric* (p. 1284)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListAccessPolicies	지정된 포털 또는 프로젝트에 대한 액세스 정책을 나열할 수 있는 권한을 부여합니다.	권한 관리	portal (p. 1284)		
			project (p. 1284)		
ListAssetModels	계정에 대한 자산 모델을 나열합니다.	List			
ListAssetTemplates	계정의 자산 템플릿을 나열합니다.	List			
ListAssets	계정의 자산을 나열합니다.	List	asset-model (p. 1284)		
ListAssociatedAssets	지정된 모델 계층 구조를 통해 상위 자산에 연결된 자산을 나열합니다.	List	asset* (p. 1284)		
ListDashboards	지정된 프로젝트 내의 대시보드를 나열할 수 있는 권한을 부여합니다.	List	project* (p. 1284)		
ListGroups	계정의 그룹을 나열합니다.	List			
ListMeasurementDataStores	계정의 측정 데이터 스토어를 나열합니다.	List			
ListMeasurementDataStreams	지정된 측정 데이터 스토어의 측정 데이터 스트림을 나열합니다.	List	measurement-data-store* (p. 1284)		
ListMetricTypes	계정의 지표 유형을 나열합니다.	List			
ListPortals	계정에 포털을 나열할 수 있는 권한을 부여합니다.	List			
ListProjectAssets	지정된 프로젝트에 연결된 자산을 나열할 수 있는 권한을 부여합니다.	List	project* (p. 1284)		
ListProjects	지정된 포털 내에서 프로젝트를 나열할 수 있는 권한을 부여합니다.	List	portal* (p. 1284)		
ListViewEntities	지정된 보기의 자산 및 그룹을 나열합니다.	List	view* (p. 1284)		
			asset (p. 1284)		
			group (p. 1284)		
ListViews	계정의 보기를 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutLoggingOptions	로깅 옵션을 설정합니다.	쓰기			
RegisterViewEntities	지정된 보기에 지정된 자산 및 그룹을 등록합니다.	쓰기	view* (p. 1284)		
			asset (p. 1284)		
			group (p. 1284)		
UpdateAccessPolicy	지정된 액세스 정책을 업데이트할 수 있는 권한을 부여합니다.	권한 관리	access-policy* (p. 1284)		
UpdateAsset	지정된 자산을 업데이트합니다.	쓰기	asset* (p. 1284)		
UpdateAssetModel	지정된 자산 모델을 업데이트합니다.	쓰기	asset-model* (p. 1284)		
UpdateAssetProperty	지정된 자산 속성을 업데이트합니다.	쓰기	asset* (p. 1284)		
UpdateAssetTemplate	지정된 자산 템플릿을 업데이트합니다.	쓰기	asset-template* (p. 1284)		
UpdateDashboard	지정된 대시보드를 업데이트할 수 있는 권한을 부여합니다.	쓰기	dashboard* (p. 1284)		
UpdateGroup	지정된 그룹을 업데이트합니다.	쓰기	group* (p. 1284)		
UpdateMeasurementDataStore	측정 데이터 스토어에 대한 메타데이터를 업데이트합니다.	쓰기	measurement-data-store* (p. 1284)		
UpdatePortal	지정된 포털을 업데이트할 수 있는 권한을 부여합니다.	쓰기	portal* (p. 1284)		
UpdateProject	지정된 프로젝트를 업데이트할 수 있는 권한을 부여합니다.	쓰기	project* (p. 1284)		
UpdateView	지정된 보기를 업데이트합니다.	쓰기	view* (p. 1284)		

AWS IoT SiteWise에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1278)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
asset	`arn:${Partition}:iotsitewise:${Region}:${Account}:asset/${AssetId}`	
asset-template	`arn:${Partition}:iotsitewise:${Region}:${Account}:asset-template/${AssetTemplateId}`	
asset-model	`arn:${Partition}:iotsitewise:${Region}:${Account}:asset-model/${AssetModelId}`	
gateway	`arn:${Partition}:iotsitewise:${Region}:${Account}:gateway/${GatewayId}`	
group	`arn:${Partition}:iotsitewise:${Region}:${Account}:group/${GroupId}`	
measurement	`arn:${Partition}:iotsitewise:${Region}:${Account}:measurement/${MeasurementId}`	
measurement-data-store	`arn:${Partition}:iotsitewise:${Region}:${Account}:measurement-data-store/${MeasurementDataStoreId}`	
metric	`arn:${Partition}:iotsitewise:${Region}:${Account}:metric/${MetricId}`	
metric-type	`arn:${Partition}:iotsitewise:${Region}:${Account}:metric-type/${MetricTypeId}`	
view	`arn:${Partition}:iotsitewise:${Region}:${Account}:view/${ViewId}`	
portal	`arn:${Partition}:iotsitewise:${Region}:${Account}:portal/${PortalId}`	
project	`arn:${Partition}:iotsitewise:${Region}:${Account}:project/${ProjectId}`	
dashboard	`arn:${Partition}:iotsitewise:${Region}:${Account}:dashboard/${DashboardId}`	
access-policy	`arn:${Partition}:iotsitewise:${Region}:${Account}:access-policy/${AccessPolicyId}`	

AWS IoT SiteWise에 사용되는 조건 키

AWS IoT SiteWise는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
iotsitewise:assetHierarchyPath	슬래시로 구분된 자산 계층 구조에서 자산 ID의 문자열입니다.	문자열

조건 키	설명	유형
iotsitewise:childAssetId	다른 자산에 대한 하위 자산으로 연결된 자산의 ID입니다.	문자열
iotsitewise:group	그룹 ID입니다.	문자열
iotsitewise:portal	포털 ID입니다.	문자열
iotsitewise:project	프로젝트 ID입니다.	문자열
iotsitewise:propertyId	속성 ID입니다.	문자열
iotsitewise:user	사용자 ID입니다.	문자열

AWS IoT Things Graph에 사용되는 작업, 리소스 및 조건 키

AWS IoT Things Graph(서비스 접두사: `iotthingsgraph`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS IoT Things Graph에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateEntityToThing	사용자의 레지스트리에 구체적으로 등록된 사물과 디바이스를 연결합니다. 사물은 한 번에 한 디바	쓰기			iot:DescribeThing iot:DescribeThingGroup

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	이스에만 연결될 수 있습니다. 사물을 새로운 디바이스 ID와 연결할 경우 이전 연결이 제거됩니다.				
CreateFlowTemplate	워크플로우 템플릿을 생성합니다. 워크플로우는 사용자의 네임스페이스에서만 생성될 수 있습니다. (퍼블릭 네임스페이스에는 개체만이 포함됩니다.) 워크플로우는 지정된 네임스페이스에서 개체만 포함할 수 있습니다. 워크플로우는 다른 네임스페이스 버전이 요청에서 지정되지 않은 한 사용자의 네임스페이스의 최신 버전에서 개체에 대해 검증됩니다.	쓰기			
CreateSystemInstance	지정된 구성과 사물로 시스템 인스턴스를 생성합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 1290) aws:TagKeys (p. 1290)	
CreateSystemTemplate	시스템을 생성합니다. 시스템은 다른 네임스페이스 버전이 요청에서 지정되지 않은 한 사용자의 네임스페이스의 최신 버전에서 개체에 대해 검증됩니다.	쓰기			
DeleteFlowTemplate	워크플로우를 삭제합니다. 새로운 시스템 또는 시스템 인스턴스에 삭제된 워크플로우가 포함되어 있으면 업데이트 또는 배포할 수 없습니다. 기존 시스템 인스턴스는 삭제된 워크플로우가 포함되어 있더라도 계속해서 실행할 수 있습니다(시스템 인스턴스 배포 시 생성된 워크플로우 스냅샷을 사용하기 때문입니다).	쓰기	Workflow* (p. 1289)		
DeleteNamespace	지정된 네임스페이스를 삭제합니다. 그러면 네임스페이스의 개체까지 모두 삭제됩니다. 따라서 이 작업을 실행하기 전에 먼저 네임스페이스의 시스템과 워크플로우를 삭제하십시오.	쓰기			
DeleteSystemInstance	시스템 인스턴스를 삭제합니다. 이전에 배포되지 않았거나, 대상에서 배포되지 않은 인스턴스만 삭제할 수 있습니다. 사용자는 삭제된 시스템 인스턴스와 동일한 ID로 시스템 인스턴스를 새롭게 생성할 수 있습니다.	쓰기	SystemInstance* (p. 1289)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteSystemTemplate	시스템을 삭제합니다. 새로운 시스템 인스턴스에는 삭제된 시스템이 포함될 수 없습니다. 기존 시스템 인스턴스에 삭제된 시스템이 포함되어 있더라도 계속해서 실행 가능합니다. 배포 시 생성된 시스템 스냅샷을 사용하기 때문입니다.	쓰기	System* (p. 1289)		
DeploySystemInstance	시스템 인스턴스를 CreateSystemInstance에서 지정한 대상에 배포합니다.	쓰기	SystemInstance* (p. 1289)		
DeprecateFlowTemplate	지정된 워크플로우를 사용 중지합니다. 그러면 삭제가 가능한 워크플로우로 표시됩니다. 사용 중지된 워크플로우는 배포할 수 없지만 이전부터 워크플로우를 사용하던 시스템 인스턴스는 계속해서 실행 가능합니다.	쓰기	Workflow* (p. 1289)		
DeprecateSystemTemplate	지정된 시스템을 사용 중지합니다.	쓰기	System* (p. 1289)		
DescribeNamespace	사용자 네임스페이스의 최신 버전과 추적 중인 퍼블릭 버전을 가져옵니다.	Read			
DissociateEntityFromThing	구체적인 사물에서 디바이스 개체의 연결을 해제합니다. 이번 작업에서는 연결을 해제해야 하는 개체 유형만 사용합니다. 사물과 연결할 수 있는 특정 유형의 개체는 1개로 제한되기 때문입니다.	쓰기			iot:DescribeThing iot:DescribeThingGroup
GetEntities	지정된 개체에 대한 설명을 가져옵니다. 기본적으로 사용자 네임스페이스의 최신 버전을 사용합니다.	Read			
GetFlowTemplate	지정된 워크플로우에 대해 최신 버전의 DefinitionDocument 및 FlowTemplateSummary를 가져옵니다.	Read	Workflow* (p. 1289)		
GetFlowTemplateRevisions	지정된 워크플로우에 저장된 개정을 가져옵니다. 개정은 마지막 100개까지만 저장됩니다. 워크플로우를 사용 중지했을 때 이 작업을 실행하면 사용 중지 이전에 발생한 개정이 반환됩니다. 사용 중지된 워크플로우에서는 이 작업이 유효하지 않습니다.	Read	Workflow* (p. 1289)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetNamespaceDeletionStatus	네임스페이스 삭제 작업에 대한 상태를 가져옵니다.	Read			
GetSystemInstance	시스템 인스턴스를 가져옵니다.	Read	SystemInstance* (p. 1289)		
GetSystemTemplate	시스템을 가져옵니다.	Read	System* (p. 1289)		
GetSystemTemplateVersions	지정된 시스템 템플릿의 개정을 가져옵니다. 개정은 이전 100개까지만 저장됩니다. 시스템을 사용 중지했을 때 이 작업을 실행하면 사용 중지 이전에 발생한 개정이 반환됩니다. 사용 중지된 시스템에서는 이 작업이 유효하지 않습니다.	Read	System* (p. 1289)		
GetUploadStatus	지정된 업로드의 상태를 가져옵니다.	Read			
ListFlowExecutionMessages	단일 워크플로우 실행에 대한 세부 정보를 나열합니다.	List			
ListTagsForResource	지정된 리소스에 대한 모든 태그를 나열합니다.	List	SystemInstance (p. 1289)		
SearchEntities	지정된 유형의 개체를 검색합니다. 사용자의 네임스페이스와 추적 중인 퍼블릭 네임스페이스에서 개체를 검색할 수 있습니다.	Read			
SearchFlowExecutions	시스템 인스턴스의 워크플로우 실행을 검색합니다.	Read	SystemInstance* (p. 1289)		
SearchFlowTemplates	워크플로우에 대한 요약 정보를 검색합니다.	Read			
SearchSystemInstances	사용자 계정의 시스템 인스턴스를 검색합니다.	Read			
SearchSystemTemplates	사용자 계정의 시스템에 대한 요약 정보를 검색합니다. 워크플로우 ID를 기준으로 필터링하면 지정된 워크플로우를 사용하는 시스템만 반환되도록 할 수 있습니다.	Read			
SearchThings	지정한 개체와 연결된 사물을 검색합니다. 디바이스와 디바이스 모델을 기준으로 검색할 수 있습니다.	Read			
TagResource	지정된 리소스에 태그를 지정합니다.	태그 지정	SystemInstance (p. 1289)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1290) aws:TagKeys (p. 1290)	
UndeploySystemInstance	대상에서 시스템 인스턴스를 비롯해 연결된 트리거를 제거합니다.	쓰기	SystemInstance* (p. 1289)		
UntagResource	지정된 리소스에서 태그를 제거합니다.	태그 지정	SystemInstance (p. 1289)		
				aws:TagKeys (p. 1290)	
UpdateFlowTemplate	지정된 워크플로우를 업데이트합니다. 이미 배포된 시스템과 시스템 인스턴스에서 업데이트된 워크플로우를 사용할 경우 다시 배포할 때 워크플로우의 변경 사항을 볼 수 있습니다. 워크플로우는 지정된 네임스페이스에서 개체만 포함할 수 있습니다.	쓰기	Workflow* (p. 1289)		
UpdateSystemTemplate	지정된 시스템을 업데이트합니다. 워크플로우를 업데이트한 후에는 이 작업을 실행할 필요 없습니다. 시스템 인스턴스가 업데이트된 시스템을 사용할 경우 다시 배포할 때 시스템의 변경 사항을 볼 수 있습니다.	쓰기	System* (p. 1289)		
UploadEntityDefinitions	1개 이상의 개체 정의를 사용자 네임스페이스에 비동기 방식으로 업로드합니다.	쓰기			

AWS IoT Things Graph에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1285)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Workflow	`arn:${Partition}:iotthingsgraph:${Region}:${Account}:Workflow/${NamespacePath}`	
System	`arn:${Partition}:iotthingsgraph:${Region}:${Account}:System/${NamespacePath}`	
SystemInstance	`arn:${Partition}:iotthingsgraph:${Region}:${Account}:Deployment/${NamespacePath}`	aws:ResourceTag/${TagKey} (p. 1290)

AWS IoT Things Graph에 사용되는 조건 키

AWS IoT Things Graph는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	Things Graph 서비스에 대한 사용자의 요청에 있는 키를 기준으로 액세스를 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	Things Graph 서비스에 대한 사용자의 요청에 있는 모든 태그 키 이름의 목록을 기준으로 액세스를 필터링합니다.	문자열

AWS IQ에 사용되는 작업, 리소스 및 조건 키

AWS IQ(서비스 접두사: `iq`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

주제

AWS IQ에서 정의한 작업

AWS IQ에는 IAM 정책 문의 `Actions` 요소에 사용할 수 있는 API 작업이 없습니다. AWS IQ에 대한 액세스를 허용하려면 정책에서 `"Action": "iq:*"`를 지정하십시오.

AWS IQ에서 정의한 리소스 유형

AWS IQ는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS IQ에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS IQ에 사용되는 조건 키

IQ에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS IQ Permissions에 사용되는 작업, 리소스 및 조건 키

AWS IQ Permissions(서비스 접두사: `iq-permission`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

주제

AWS IQ Permissions에서 정의한 작업

AWS IQ Permissions에는 IAM 정책 문의 `Actions` 요소에 사용할 수 있는 API 작업이 없습니다. AWS IQ Permissions에 대한 액세스를 허용하려면 정책에서 `"Action": "iq-permission:*"`를 지정하십시오.

AWS IQ Permissions에서 정의한 리소스 유형

AWS IQ Permissions는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS IQ Permissions에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS IQ Permissions에 사용되는 조건 키

AWS IQ Permissions에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Kendra에 사용되는 작업, 리소스 및 조건 키

Amazon Kendra(서비스 접두사: `kendra`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Kendra에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchDeleteDocument	문서 일괄 삭제	쓰기	index* (p. 1293)		
BatchPutDocument	문서 일괄 넣기	쓰기	index* (p. 1293)		
CreateDataSource	데이터 소스 생성	쓰기	index* (p. 1293)		
CreateFaq	FAQ 생성	쓰기	index* (p. 1293)		
CreateIndex	인덱스 생성	쓰기			
DeleteFaq	FAQ 삭제	쓰기	faq* (p. 1293)		
			index* (p. 1293)		
DeleteIndex	인덱스 삭제	쓰기	index* (p. 1293)		
DescribeDataSource	데이터 소스 설명	Read	data-source* (p. 1293)		
			index* (p. 1293)		
DescribeFaq	FAQ 설명	Read	faq* (p. 1293)		
			index* (p. 1293)		
DescribeIndex	인덱스 설명	Read	index* (p. 1293)		
ListDataSourceSyncJobs	데이터 소스 동기화 작업 기록 가져오기	List	data-source* (p. 1293)		
			index* (p. 1293)		
ListDataSources	데이터 소스 나열	List	index* (p. 1293)		
ListFaqs	FAQ 나열	List	index* (p. 1293)		
ListIndices	인덱스 나열	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Query	문서 및 FAQ 질의	Read	index* (p. 1293)		
StartDataSourceSyncJob	데이터 소스 동기화 작업 시작	쓰기	data-source* (p. 1293)		
			index* (p. 1293)		
StopDataSourceSyncJob	데이터 소스 동기화 작업 중지	쓰기	data-source* (p. 1293)		
			index* (p. 1293)		
SubmitFeedback	쿼리 결과에 대한 피드백 보내기	쓰기	index* (p. 1293)		
UpdateDataSource	데이터 소스 업데이트	쓰기	data-source* (p. 1293)		
			index* (p. 1293)		
UpdateIndex	인덱스 업데이트	쓰기	index* (p. 1293)		

Amazon Kendra에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1291)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
index	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}`	
data-source	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/data-source/${DataSourceId}`	
faq	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/faq/${FaqId}`	

Amazon Kendra의 조건 키

Kendra에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Key Management Service에 사용되는 작업, 리소스 및 조건 키

AWS Key Management Service(서비스 접두사: `kms`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Key Management Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelKeyDeletion	고객 마스터 키의 예약된 삭제를 취소할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
ConnectCustomKeyStore	사용자 지정 키 스토어를 연결된 AWS CloudHSM 클러스터에 연결 또는 재연결할 수 있는 권한을 제어합니다.	쓰기			
CreateAlias	고객 마스터 키(CMK)의 별칭을 생성할 수 있는 권한을 제어합니다. 별칭은 고객 마스터 키와 연결할 수 있는 선택적인 기억하기 쉬운 이름입니다.	쓰기	alias* (p. 1303)		
			key* (p. 1303)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
CreateCustomKeyStore	사용자가 소유 및 관리하는 AWS CloudHSM 클러스터와 연결된 사용자 지정 키 스토어를 생성할 수 있는 권한을 제어합니다.	쓰기			cloudhsm:DescribeCluste
CreateGrant	고객 마스터 키에 권한 부여를 추가할 수 있는 권한을 제어합니다. 권한 부여를 사용하여 키 정책 또는 IAM 정책을 변경하지 않고 권한을 추가할 수 있습니다.	권한 관리	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:GrantConstraintType (p. 1304) kms:GrantIsForAWSResource (p. 1304) kms:ViaService (p. 1305)	
CreateKey	데이터 키 및 다른 민감한 정보를 보호하기 위해 사용할 수 있는 고객 마스터 키를 생성할 수 있는 권한을 제어합니다.	쓰기		kms:BypassPolicyLockoutSafetyCheck (p. 1304) kms:CustomerMasterKeySpec (p. 1304) kms:CustomerMasterKeyUsage (p. 1304) kms:KeyOrigin (p. 1304)	
Decrypt	고객 마스터 키 하에서 암호화된 암호화 텍스트를 암호화 해제할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:EncryptionAlgorithm (p. 1304) kms:EncryptionContextKeys (p. 1304) kms:ViaService (p. 1305)	
DeleteAlias	별칭을 삭제할 수 있는 권한을 제어합니다. 별칭은 고객 마스터 키와 연결할 수 있는 선택적인 기억하기 쉬운 이름입니다.	쓰기	alias* (p. 1303)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
DeleteCustomKeyStore	사용자 지정 키 스토어를 삭제할 수 있는 권한을 제어합니다.	쓰기			
DeleteImportedKeyMaterial	고객 마스터 키로 가져온 암호화 구성 요소를 삭제할 수 있는 권한을 제어합니다. 이 작업은 키를 사용할 수 없게 합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
DescribeCustomKeyStores	계정 및 리전의 사용자 지정 키 스토어에 대한 세부 정보를 볼 수 있는 권한을 제어합니다.	Read			
DescribeKey	고객 마스터 키에 대한 세부 정보를 볼 수 있는 권한을 제어합니다.	Read	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
DisableKey	암호화 작업에 사용하지 못하도록 고객 마스터 키를 비활성화할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
DisableKeyRotation	고객 관리형 고객 마스터 키의 자동 교체를 비활성화할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
DisconnectCustomKeyStore	연결된 AWS CloudHSM 클러스터에서 사용자 지정 키 스토어를 연결 해제할 수 있는 권한을 제어합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
EnableKey	고객 마스터 키(CMK)의 상태를 활성화하도록 변경할 수 있는 권한을 제어합니다. CMK가 암호화 작업에 사용될 수 있도록 허용합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
EnableKeyRotation	고객 마스터 키의 암호화 구성 요소의 자동 교체를 활성화할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
Encrypt	지정된 고객 마스터 키를 사용하여 데이터 및 데이터 키를 암호화할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:EncryptionAlgorithm (p. 1304) kms:EncryptionContextKeys (p. 1304) kms:ViaService (p. 1305)	
GenerateDataKey	고객 마스터 키를 사용하여 데이터 키를 생성할 수 있는 권한을 제어합니다. 데이터 키를 사용하여 AWS KMS 외부 데이터를 암호화할 수 있습니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:EncryptionAlgorithm (p. 1304) kms:EncryptionContextKeys (p. 1304) kms:ViaService (p. 1305)	
GenerateDataKeyPair	고객 마스터 키를 사용하여 데이터 키를 생성할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				kms:CallerAccount (p. 1304) kms:DataKeyPairSpec (p. 1304) kms:EncryptionAlgorithm (p. 1304) kms:EncryptionContextKeys (p. 1304) kms:ViaService (p. 1305)	
GenerateDataKeyPairWithoutPlaintext	고객 마스터 키를 사용하여 데이터 키를 생성할 수 있는 권한을 제어합니다. GenerateDataKeyPair 작업과 달리 이 작업은 일반 텍스트 복사본 없이 암호화된 프라이빗 키를 반환합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:DataKeyPairSpec (p. 1304) kms:EncryptionAlgorithm (p. 1304) kms:EncryptionContextKeys (p. 1304) kms:ViaService (p. 1305)	
GenerateDataKeyWithoutPlaintext	고객 마스터 키를 사용하여 데이터 키를 생성할 수 있는 권한을 제어합니다. GenerateDataKey 작업과 달리, 이 작업은 데이터 키의 일반 텍스트 버전 없이 암호화된 데이터 키를 반환합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:EncryptionAlgorithm (p. 1304) kms:EncryptionContextKeys (p. 1304) kms:ViaService (p. 1305)	
GenerateRandom	AWS KMS에서 암호로 보호되는 임의 바이트 문자열을 가져올 수 있는 권한을 제어합니다.	쓰기			
GetKeyPolicy	지정된 고객 마스터 키에 대한 키 정책을 볼 수 있는 권한을 제어합니다.	Read	key* (p. 1303)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
GetKeyRotationStatus	고객 마스터 키에서 자동 키 교체가 활성화되는지 여부를 결정할 권한을 제어합니다.	Read	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
GetParametersForImport	퍼블릭 키 및 가져오기 토큰을 포함하여 암호화 구성 요소를 고객 관리형 키로 가져오기 위해 필요한 데이터를 가져올 수 있는 권한을 제어합니다.	Read	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305) kms:WrappingAlgorithm (p. 1305) kms:WrappingKeySpec (p. 1305)	
GetPublicKey	비대칭 고객 마스터 키의 퍼블릭 키를 다운로드할 수 있는 권한을 제어합니다.	Read	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
ImportKeyMaterial	암호화 구성 요소를 고객 마스터 키로 가져올 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ExpirationModel (p. 1304) kms:ValidTo (p. 1305) kms:ViaService (p. 1305)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListAliases	계정에 정의되어 있는 별칭을 볼 수 있는 권한을 제어합니다. 별칭은 고객 마스터 키와 연결할 수 있는 선택적인 기억하기 쉬운 이름입니다.	List			
ListGrants	고객 마스터 키를 위한 모든 권한 부여를 볼 수 있는 권한을 제어합니다.	List	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:GrantIsForAWSResource (p. 1304) kms:ViaService (p. 1305)	
ListKeyPolicies	고객 마스터 키에 대한 키 정책의 이름을 볼 수 있는 권한을 제어합니다.	List	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
ListKeys	계정 내 모든 고객 마스터 키의 키 ID 및 Amazon 리소스 이름(ARN)을 볼 수 있는 권한을 제어합니다.	List			
ListResourceTags	고객 마스터 키에 연결된 모든 태그를 볼 수 있는 권한을 제어합니다.	Read	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
ListRetirableGrants	지정된 보안 주체가 사용 중지 보안 주체인 권한 부여를 볼 수 있는 권한을 제어합니다. 다른 보안 주체는 이 권한 부여를 사용 중지할 수 있고 이 보안 주체는 다른 권한 부여를 사용 중지할 수 있습니다.	List	key* (p. 1303)		
PutKeyPolicy	지정된 고객 마스터 키에 대한 키 정책을 교체할 수 있는 권한을 제어합니다.	권한 관리	key* (p. 1303)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				kms:BypassPolicyLockoutSafetyCheck (p. 1304) kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
ReEncryptFrom	AWS KMS 내에서 데이터를 암호화 해제하고 재암호화하는 프로세스의 일부로서 데이터의 암호화를 해제할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:EncryptionAlgorithm (p. 1304) kms:EncryptionContextKeys (p. 1304) kms:ReEncryptOnSameKey (p. 1305) kms:ViaService (p. 1305)	
ReEncryptTo	AWS KMS 내에서 데이터를 암호화 해제하고 재암호화하는 프로세스의 일부로서 데이터를 암호화할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:EncryptionAlgorithm (p. 1304) kms:EncryptionContextKeys (p. 1304) kms:ReEncryptOnSameKey (p. 1305) kms:ViaService (p. 1305)	
RetireGrant	권한 부여의 사용을 중지할 수 있는 권한을 제어합니다. RetireGrant 작업은 일반적으로 권한 부여에 의해 사용자가 수행하도록 허용된 작업을 완료한 후 권한 부여 사용자에 의해 호출됩니다.	권한 관리	key* (p. 1303)		
RevokeGrant	권한 부여를 취소(권한 부여를 사용하는 모든 작업에 대한 권한을 거부함)할 수 있는 권한을 제어합니다.	권한 관리	key* (p. 1303)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				kms:CallerAccount (p. 1304) kms:GrantIsForAWSResource (p. 1304) kms:ViaService (p. 1305)	
ScheduleKeyDeletion	고객 마스터 키의 삭제를 예약할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
Sign	메시지에 대한 디지털 서명을 생성할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:MessageType (p. 1304) kms:SigningAlgorithm (p. 1305) kms:ViaService (p. 1305)	
TagResource	고객 마스터 키에 연결되는 모든 태그를 생성하거나 업데이트할 수 있는 권한을 제어합니다.	태그 지정	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
UntagResource	고객 마스터 키에 연결된 태그를 삭제할 수 있는 권한을 제어합니다.	태그 지정	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
UpdateAlias	별칭을 다른 고객 마스터 키와 연결할 수 있는 권한을 제어합니다. 별칭은 고객 마스터 키와 연결할 수 있는 선택적인 표시 이름입니다.	쓰기	alias* (p. 1303)		
			key* (p. 1303)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
UpdateCustomKeyStore	사용자 지정 키 스토어의 속성을 변경할 수 있는 권한을 제어합니다.	쓰기			
UpdateKeyDescription	고객 마스터 키의 설명을 삭제하거나 변경할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:ViaService (p. 1305)	
Verify	지정된 고객 마스터 키를 사용하여 디지털 서명을 확인할 수 있는 권한을 제어합니다.	쓰기	key* (p. 1303)		
				kms:CallerAccount (p. 1304) kms:MessageType (p. 1304) kms:SigningAlgorithm (p. 1305) kms:ViaService (p. 1305)	

AWS Key Management Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1294)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
alias	`arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}`	
key	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	

AWS Key Management Service에 사용되는 조건 키

AWS Key Management Service는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
kms:BypassPolicyLockoutSafetyCheck	요청의 BypassPolicyLockoutSafetyCheck 파라미터 값에 따라 CreateKey 및 PutKeyPolicy 작업에 대한 액세스를 제어합니다.	Bool
kms:CallerAccount	호출자의 AWS 계정 ID에 따라 지정된 AWS KMS 작업에 대한 액세스를 제어합니다. 이 조건 키를 사용하여 단일 정책 설명으로 AWS 계정의 모든 IAM 사용자 및 역할에 대한 액세스를 허용하거나 거부할 수 있습니다.	문자열
kms:CustomerMasterKeySpec	생성되었거나 작업에서 사용된 CMK의 CustomerMasterKeySpec 속성을 기반으로 API 작업에 대한 액세스를 제어합니다. 이를 사용하여 CreateKey 작업 또는 CMK 리소스에 대해 승인된 모든 작업의 권한을 검증할 수 있습니다.	문자열
kms:CustomerMasterKeyUsage	생성되었거나 작업에서 사용된 CMK의 KeyUsage 속성을 기반으로 API 작업에 대한 액세스를 제어합니다. 이를 사용하여 CreateKey 작업 또는 CMK 리소스에 대해 승인된 모든 작업의 권한을 검증할 수 있습니다.	문자열
kms:DataKeyPairSpec	요청의 DataKeyPairSpec 파라미터 값을 기반으로 GenerateDataKeyPair 및 GenerateDataKeyPairWithoutPlaintext 작업에 대한 액세스를 제어합니다.	문자열
kms:EncryptionAlgorithm	요청의 암호화 알고리즘 값을 기반으로 암호화 작업에 대한 액세스를 제어합니다.	문자열
kms:EncryptionContext:*key*	암호화 컨텍스트에서 지정된 키의 유무에 따라 액세스를 제어합니다. 암호화 컨텍스트는 암호화 작업의 선택적 요소입니다.	문자열
kms:ExpirationModel	요청의 ExpirationModel 파라미터 값에 따라 ImportKeyMaterial 작업에 대한 액세스를 제어합니다.	문자열
kms:GrantConstraintType	요청의 권한 부여 제약에 따라 CreateGrant 작업에 대한 액세스를 제어합니다.	문자열
kms:GrantIsForAWSResource	요청의 출처가 지정된 AWS 서비스인 경우 CreateGrant 작업에 대한 액세스를 제어합니다.	Bool
kms:GrantOperations	권한 부여의 작업에 따라 CreateGrant 작업에 대한 액세스를 제어합니다.	문자열
kms:GranteePrincipal	권한 부여의 피부여자 보안 주체에 따라 CreateGrant 작업에 대한 액세스를 제어합니다.	문자열
kms:KeyOrigin	생성되었거나 작업에서 사용된 CMK의 Origin 속성을 기반으로 API 작업에 대한 액세스를 제어합니다. 이를 사용하여 CreateKey 작업 또는 CMK 리소스에 대해 승인된 모든 작업의 권한을 검증할 수 있습니다.	문자열
kms:MessageType	요청의 MessageType 파라미터 값에 따라 Sign 및 Verify 작업에 대한 액세스를 제어합니다.	문자열

조건 키	설명	유형
kms:ReEncryptOnSameKey	Encrypt 작업에 사용된 것과 동일한 고객 마스터 키를 사용하는 경우 ReEncrypt 작업에 대한 액세스를 제어합니다.	Bool
kms:RetiringPrincipal	권한 부여의 사용 중지 보안 주체에 따라 CreateGrant 작업에 대한 액세스를 제어합니다.	문자열
kms:SigningAlgorithm	요청의 서명 알고리즘을 기반으로 Sign 및 Verify 작업에 대한 액세스를 제어합니다.	문자열
kms:ValidTo	요청의 ValidTo 파라미터 값에 따라 ImportKeyMaterial 작업에 대한 액세스를 제어합니다. 이 조건 키를 사용하여 지정된 날짜에 만료되는 경우에만 사용자가 키 구성 요소를 가져오도록 허용할 수 있습니다.	숫자
kms:ViaService	보안 주체를 대신하여 수행된 요청의 출처가 지정된 AWS 서비스인 경우 액세스를 제어합니다.	문자열
kms:WrappingAlgorithm	요청의 WrappingAlgorithm 파라미터 값에 따라 GetParametersForImport 작업에 대한 액세스를 제어합니다.	문자열
kms:WrappingKeySpec	요청의 WrappingKeySpec 파라미터 값에 따라 GetParametersForImport 작업에 대한 액세스를 제어합니다.	문자열

Amazon Kinesis에 사용되는 작업, 리소스 및 조건 키

Amazon Kinesis(서비스 접두사: `kinesis`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Kinesis에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTagsToStream	지정된 Amazon Kinesis 스트림에 대한 태그를 추가하거나 업데이트합니다. 각 스트림은 최대 10개의 태그를 보유할 수 있습니다.	태그 지정	stream* (p. 1308)		
CreateStream	Amazon Kinesis 스트림을 생성합니다.	쓰기	stream* (p. 1308)		
DecreaseStreamRetentionPeriod	스트림의 보존 기간(데이터 레코드를 스트림에 추가한 후 데이터 레코드에 액세스할 수 있는 기간)을 줄입니다.	쓰기	stream* (p. 1308)		
DeleteStream	스트림 및 해당되는 샤드 및 데이터를 모두 삭제합니다.	쓰기	stream* (p. 1308)		
DeregisterStreamConsumer	Kinesis 데이터 스트림에서 스트림 소비자를 등록 취소합니다.	쓰기	consumer* (p. 1308)		
			stream* (p. 1308)		
DescribeLimits	계정에 대한 샤드 제한 및 사용량을 설명합니다.	Read			
DescribeStream	지정된 스트림을 설명합니다.	Read	stream* (p. 1308)		
DescribeStreamConsumer	등록된 스트림 소비자에 대한 설명을 가져옵니다.	Read	consumer* (p. 1308)		
			stream* (p. 1308)		
DescribeStreamSummary	지정된 Kinesis 데이터 스트림에 대한 요약 설명을 제공합니다(샤드 목록 없음).	Read	stream* (p. 1308)		
DisableEnhancedMonitoring	확장 모니터링을 비활성화합니다.	쓰기			
EnableEnhancedMonitoring	API_EnableEnhancedMonitoring.html	쓰기			
GetRecords	샤드에서 데이터 레코드를 가져옵니다.	Read	stream* (p. 1308)		
GetShardIterator	샤드 반복자를 가져옵니다. 샤드 반복자는 요청자에게 반환되고 5분 후에 만료됩니다.	Read	stream* (p. 1308)		
IncreaseStreamRetentionPeriod	스트림의 보존 기간(데이터 레코드를 스트림에 추가한 후 데이터 레코드에 액세스할 수 있는 기간)을 늘립니다.	쓰기	stream* (p. 1308)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListShards	스트림의 샤드를 나열하고 각 샤드에 대한 정보를 제공합니다.	List			
ListStreamConsumers	향상된 팬아웃을 사용하여 Kinesis 스트림으로부터 데이터를 수신하도록 등록된 스트림 소비자를 나열하고 각 소비자에 대한 정보를 제공합니다.	List			
ListStreams	스트림을 나열합니다.	List			
ListTagsForStream	지정된 Amazon Kinesis 스트림에 대한 태그를 나열합니다.	Read	stream* (p. 1308)		
MergeShards	스트림에서 두 인접 샤드를 병합하고 단일 샤드로 결합하여 데이터를 수집하고 전송하기 위한 스트림의 용량을 줄입니다.	쓰기	stream* (p. 1308)		
PutRecord	생산자의 단일 데이터 레코드를 Amazon Kinesis 스트림에 씁니다.	쓰기	stream* (p. 1308)		
PutRecords	생산자의 여러 데이터 레코드를 단일 호출(PutRecords 요청이라고도 일컬어짐)로 Amazon Kinesis 스트림에 씁니다.	쓰기	stream* (p. 1308)		
RegisterStreamConsumer	Kinesis 데이터 스트림에 스트림 소비자를 등록합니다.	쓰기	consumer* (p. 1308)		
			stream* (p. 1308)		
RemoveTagsFromStream	SplitShard에 대한 설명	태그 지정	stream* (p. 1308)		
SplitShard	SplitShard에 대한 설명	쓰기	stream* (p. 1308)		
SubscribeToShard	향상된 팬아웃으로 특정 샤드를 수신 대기합니다.	Read	consumer* (p. 1308)		
			stream* (p. 1308)		
UpdateShardCount	지정된 스트림의 샤드 수를 지정된 샤드 수로 업데이트합니다.	쓰기			

Amazon Kinesis에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1305)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
stream	`arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}`	
consumer	`arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}`	

Amazon Kinesis에 사용되는 조건 키

Kinesis에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Kinesis Analytics에 사용되는 작업, 리소스 및 조건 키

Amazon Kinesis Analytics(서비스 접두사: `kinesisanalytics`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Kinesis Analytics에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddApplicationInput	입력을 애플리케이션에 추가합니다.	쓰기	application* (p. 1310)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddApplicationOutput	출력을 애플리케이션에 추가합니다.	쓰기	application* (p. 1310)		
AddApplicationReferenceDataSource	참조 데이터 원본을 애플리케이션에 추가합니다.	쓰기	application* (p. 1310)		
CreateApplication	애플리케이션을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1310) aws:TagKeys (p. 1310)	
DeleteApplication	애플리케이션을 삭제합니다.	쓰기	application* (p. 1310)		
DeleteApplicationOutput	애플리케이션의 지정된 출력을 삭제합니다.	쓰기	application* (p. 1310)		
DeleteApplicationReferenceDataSource	애플리케이션의 지정된 참조 데이터 원본을 삭제합니다.	쓰기	application* (p. 1310)		
DescribeApplication	지정된 애플리케이션을 설명합니다.	Read	application* (p. 1310)		
DiscoverInputSchema	애플리케이션에 대한 입력 스키마를 검색합니다.	Read			
GetApplicationState [권한만 해당]	Kinesis Data Analytics 콘솔에 Kinesis Data Analytics SQL 실행 시간 애플리케이션의 스트림 결과를 표시할 수 있는 권한을 부여합니다.	Read	application* (p. 1310)		
ListApplications	계정에 대한 애플리케이션을 나열합니다.	List			
ListTagsForResource	애플리케이션과 연결된 태그를 가져옵니다.	Read	application* (p. 1310)		
StartApplication	애플리케이션을 시작합니다.	쓰기	application* (p. 1310)		
StopApplication	애플리케이션을 중지합니다.	쓰기	application* (p. 1310)		
TagResource	애플리케이션에 태그를 추가합니다.	태그 지정	application* (p. 1310)		
				aws:RequestTag/${TagKey} (p. 1310) aws:TagKeys (p. 1310)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UntagResource	애플리케이션에서 지정된 태그를 제거합니다.	태그 지정	application* (p. 1310)		
				aws:TagKeys (p. 1310)	
UpdateApplication	애플리케이션을 업데이트합니다.	쓰기	application* (p. 1310)		

Amazon Kinesis Analytics에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1308)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey} (p. 1310)

Amazon Kinesis Analytics의 조건 키

Amazon Kinesis Analytics는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon Kinesis Analytics V2에 사용되는 작업, 리소스 및 조건 키

Amazon Kinesis Analytics V2(서비스 접두사: `kinesisanalytics`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Kinesis Analytics V2에서 정의한 작업 (p. 1311)
- Amazon Kinesis Analytics V2에서 정의한 리소스 유형 (p. 1313)
- Amazon Kinesis Analytics V2에 사용되는 조건 키 (p. 1313)

Amazon Kinesis Analytics V2에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddApplicationCloudWatchLoggingOption	CloudWatch 로깅 옵션을 애플리케이션에 추가합니다.	쓰기	application* (p. 1313)		
AddApplicationInput	입력을 애플리케이션에 추가합니다.	쓰기	application* (p. 1313)		
AddApplicationInputProcessingConfiguration	입력 처리 구성을 애플리케이션에 추가합니다.	쓰기	application* (p. 1313)		
AddApplicationOutput	출력을 애플리케이션에 추가합니다.	쓰기	application* (p. 1313)		
AddApplicationReferenceDataSource	참조 데이터 원본을 애플리케이션에 추가합니다.	쓰기	application* (p. 1313)		
AddApplicationVpcConfiguration	VPC 구성을 애플리케이션에 추가합니다.	쓰기	application* (p. 1313)		
CreateApplication	애플리케이션을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1313) aws:TagKeys (p. 1313)	
CreateApplicationSnapshot	애플리케이션에 대한 스냅샷을 생성합니다.	쓰기	application* (p. 1313)		
DeleteApplication	애플리케이션을 삭제합니다.	쓰기	application* (p. 1313)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteApplicationCloudWatchLoggingOption	애플리케이션의 지정된 CloudWatch 로깅 옵션을 삭제합니다.	쓰기	application* (p. 1313)		
DeleteApplicationInputProcessingConfiguration	애플리케이션의 지정된 입력 처리 구성을 삭제합니다.	쓰기	application* (p. 1313)		
DeleteApplicationOutput	애플리케이션의 지정된 출력을 삭제합니다.	쓰기	application* (p. 1313)		
DeleteApplicationReferenceDataSource	애플리케이션의 지정된 참조 데이터 원본을 삭제합니다.	쓰기	application* (p. 1313)		
DeleteApplicationSnapshot	애플리케이션에 대한 스냅샷을 삭제합니다.	쓰기	application* (p. 1313)		
DeleteApplicationVpcConfiguration	애플리케이션의 지정된 VPC 구성을 삭제합니다.	쓰기	application* (p. 1313)		
DescribeApplication	지정된 애플리케이션을 설명합니다.	Read	application* (p. 1313)		
DescribeApplicationSnapshot	애플리케이션 스냅샷을 설명합니다.	Read	application* (p. 1313)		
DiscoverInputSchema	애플리케이션에 대한 입력 스키마를 검색합니다.	Read			
ListApplicationSnapshots	애플리케이션에 대한 스냅샷을 나열합니다.	Read	application* (p. 1313)		
ListApplications	계정에 대한 애플리케이션을 나열합니다.	List			
ListTagsForResource	애플리케이션과 연결된 태그를 가져옵니다.	Read	application* (p. 1313)		
StartApplication	애플리케이션을 시작합니다.	쓰기	application* (p. 1313)		
StopApplication	애플리케이션을 중지합니다.	쓰기	application* (p. 1313)		
TagResource	애플리케이션에 태그를 추가합니다.	태그 지정	application* (p. 1313)		
				aws:RequestTag/${TagKey} (p. 1313) aws:TagKeys (p. 1313)	
UntagResource	애플리케이션에서 지정된 태그를 제거합니다.	태그 지정	application* (p. 1313)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1313)	
UpdateApplication	애플리케이션을 업데이트합니다.	쓰기	application* (p. 1313)		

Amazon Kinesis Analytics V2에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1311)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey} (p. 1313)

Amazon Kinesis Analytics V2에 사용되는 조건 키

Amazon Kinesis Analytics V2는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon Kinesis Firehose에 사용되는 작업, 리소스 및 조건 키

Amazon Kinesis Firehose(서비스 접두사: `firehose`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Kinesis Firehose에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateDeliveryStream	전송 스트림을 생성합니다.	쓰기	deliverystream* (p. 1315)		
				aws:RequestTag/${TagKey} (p. 1315) aws:TagKeys (p. 1316)	
DeleteDeliveryStream	전송 스트림 및 해당 데이터를 삭제합니다.	쓰기	deliverystream* (p. 1315)		
DescribeDeliveryStream	지정된 전송 스트림을 설명하고 상태를 가져옵니다.	List	deliverystream* (p. 1315)		
ListDeliveryStreams	전송 스트림을 나열합니다.	List			
ListTagsForDeliveryStream	지정된 전송 스트림에 대한 태그를 나열합니다.	List	deliverystream* (p. 1315)		
PutRecord	단일 데이터 레코드를 Amazon Kinesis Firehose 전송 스트림에 씁니다.	쓰기	deliverystream* (p. 1315)		
PutRecordBatch	여러 데이터 레코드를 단일 호출로 전송 스트림에 씁니다(그러면 단일 레코드를 쓸 때보다 생산자당 더 높은 처리량을 달성할 수 있음).	쓰기	deliverystream* (p. 1315)		
StartDeliveryStreamEncryption	전송 스트림에 대해 서버 측 암호화(SSE)를 활성화합니다.	쓰기	deliverystream* (p. 1315)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StopDeliveryStream...	지정된 전송 스트림의 지정된 대상을 비활성화합니다.	쓰기	deliverystream* (p. 1315)		
TagDeliveryStream	지정된 전송 스트림에 대한 태그를 추가 또는 업데이트합니다.	쓰기	deliverystream* (p. 1315)		
				aws:RequestTag/${TagKey} (p. 1315) aws:TagKeys (p. 1316)	
UntagDeliveryStream	지정된 전송 스트림에 대한 태그를 제거합니다.	쓰기	deliverystream* (p. 1315)		
				aws:TagKeys (p. 1316)	
UpdateDestination	지정된 전송 스트림의 지정된 대상을 업데이트합니다.	쓰기	deliverystream* (p. 1315)		

Amazon Kinesis Firehose에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1314)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
deliverystream	`arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}`	aws:ResourceTag/${TagKey} (p. 1315)

Amazon Kinesis Firehose에 사용되는 조건 키

Amazon Kinesis Firehose는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열

Amazon Kinesis Video Streams에 사용되는 작업, 리소스 및 조건 키

Amazon Kinesis Video Streams(서비스 접두사: `kinesisvideo`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Kinesis Video Streams에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ConnectAsMaster	엔드포인트에서 지정한 신호 채널에 마스터로 연결할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1319)		
ConnectAsViewer	엔드포인트에서 지정한 신호 채널에 뷰어로 연결할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1319)		
CreateSignalingChannel	신호 채널을 생성할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1319)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1320) aws:TagKeys (p. 1320)	
CreateStream	Kinesis 비디오 스트림을 생성할 수 있는 권한을 부여합니다.	쓰기	stream* (p. 1319)		
				aws:RequestTag/${TagKey} (p. 1320) aws:TagKeys (p. 1320)	
DeleteSignalingChannel	기존 신호 채널을 삭제할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1319)		
DeleteStream	기존 Kinesis 비디오 스트림을 삭제할 수 있는 권한을 부여합니다.	쓰기	stream* (p. 1319)		
DescribeSignalingChannel	지정된 신호 채널을 설명할 수 있는 권한을 부여합니다.	List	channel* (p. 1319)		
DescribeStream	지정된 Kinesis 비디오 스트림을 설명할 수 있는 권한을 부여합니다.	List	stream* (p. 1319)		
GetDASHStreamingSessionURL	MPEG-DASH 비디오 스트리밍용 URL을 생성할 수 있는 권한을 부여합니다.	Read	stream* (p. 1319)		
GetDataEndpoint	Kinesis 비디오 스트림에 대한 미디어 데이터를 읽거나 쓰기 위해 지정된 스트림의 엔드포인트를 가져올 수 있는 권한을 부여합니다.	Read	stream* (p. 1319)		
GetHLSStreamingSessionURL	HLS 비디오 스트리밍용 URL을 생성할 수 있는 권한을 부여합니다.	Read	stream* (p. 1319)		
GetIceServerConfig	ICE 서버 구성을 가져올 수 있는 권한을 부여합니다.	Read	channel* (p. 1319)		
GetMedia	Kinesis 비디오 스트림의 미디어 콘텐츠를 반환할 수 있는 권한을 부여합니다.	Read	stream* (p. 1319)		
GetMediaForFragmentList	영구 스토리지에서만 미디어 데이터를 읽고 반환할 수 있는 권한을 부여합니다.	Read	stream* (p. 1319)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetSignalingChannelEndpoint	신호 채널에서 지정된 프로토콜 및 역할 조합에 대한 엔드포인트를 가져올 수 있는 권한을 부여합니다.	Read	channel* (p. 1319)		
ListFragments	범위가 지정된 페이지 매김 토큰 또는 선택기 유형에 따라 아카이브 스토리지의 조각을 나열할 수 있는 권한을 부여합니다.	List	stream* (p. 1319)		
ListSignalingChannels	신호 채널을 나열할 수 있는 권한을 부여합니다.	List			
ListStreams	Kinesis 비디오 스트림을 나열할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	리소스와 연결된 태그를 가져올 수 있는 권한을 부여합니다.	Read	channel (p. 1319)		
			stream (p. 1319)		
ListTagsForStream	Kinesis 비디오 스트림과 연결된 태그를 가져올 수 있는 권한을 부여합니다.	Read	stream* (p. 1319)		
PutMedia	Kinesis 비디오 스트림에 미디어 데이터를 보낼 수 있는 권한을 부여합니다.	쓰기	stream* (p. 1319)		
SendAlexaOfferToMaster	마스터에게 Alexa SDP 제안을 보낼 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1319)		
TagResource	리소스에 태그 세트를 첨부할 수 있는 권한을 부여합니다.	태그 지정	channel (p. 1319)		
			stream (p. 1319)		
				aws:RequestTag/${TagKey} (p. 1320) aws:TagKeys (p. 1320)	
TagStream	Kinesis 비디오 스트림에 태그 세트를 첨부할 수 있는 권한을 부여합니다.	태그 지정	stream* (p. 1319)		
				aws:RequestTag/${TagKey} (p. 1320) aws:TagKeys (p. 1320)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UntagResource	리소스에서 태그를 1개 이상 제거할 수 있는 권한을 부여합니다.	태그 지정	channel (p. 1319)		
			stream (p. 1319)		
				aws:TagKeys (p. 1320)	
UntagStream	Kinesis 비디오 스트림에서 태그를 하나 이상 제거할 수 있는 권한을 부여합니다.	태그 지정	stream* (p. 1319)		
				aws:TagKeys (p. 1320)	
UpdateDataRetention	Kinesis 비디오 스트림의 데이터 보존 기간을 업데이트할 수 있는 권한을 부여합니다.	쓰기	stream* (p. 1319)		
UpdateSignalingChannel	기존 신호 채널을 업데이트할 수 있는 권한을 부여합니다.	쓰기	channel* (p. 1319)		
UpdateStream	기존 Kinesis 비디오 스트림을 업데이트할 수 있는 권한을 부여합니다.	쓰기	stream* (p. 1319)		

Amazon Kinesis Video Streams에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1316)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
stream	`arn:${Partition}:kinesisvideo:${Region}:${Account}:stream/${StreamName}/${CreationTime}`	aws:ResourceTag/${TagKey} (p. 1320)
channel	`arn:${Partition}:kinesisvideo:${Region}:${Account}:channel/${ChannelName}/${CreationTime}`	aws:ResourceTag/${TagKey} (p. 1320)

Amazon Kinesis Video Streams의 조건 키

Amazon Kinesis Video Streams는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	스트림과 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그 키가 있는지 여부를 기준으로 요청을 필터링합니다.	문자열

AWS Lake Formation에 사용되는 작업, 리소스 및 조건 키

AWS Lake Formation(서비스 접두사: `lakeformation`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Lake Formation에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchGrantPermissions	데이터 레이크 권한을 보안 주체 1개 이상에서 일괄적으로 부여합니다.	권한 관리			
BatchRevokePermissions	보안 주체 1개 이상에서 데이터 레이크 권한을 일괄적으로 취소합니다.	권한 관리			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeregisterResource	등록된 위치를 등록 해제합니다.	쓰기			
DescribeResource	등록된 위치에 대해 설명합니다.	Read			
GetDataAccess	가상 데이터 레이크 액세스 권한을 부여합니다.	쓰기			
GetDataLakeSettings	데이터 레이크 관리자 및 데이터베이스와 테이블 기본 권한 목록 같은 데이터 레이크 설정을 가져옵니다.	Read			
GetEffectivePermissionsForPath	지정된 경로로 리소스에 연결된 권한을 가져옵니다.	Read			
GrantPermissions	데이터 레이크 권한을 보안 주체에게 부여합니다.	권한 관리			
ListPermissions	보안 주체 또는 리소스를 기준으로 필터링된 권한을 나열합니다.	List			
ListResources	등록된 위치를 나열합니다.	List			
PutDataLakeSettings	데이터 레이크 관리자 및 데이터베이스와 테이블 기본 권한 목록 같은 데이터 레이크 설정을 덮어씁니다.	권한 관리			
RegisterResource	Lake Formation에서 새롭게 관리할 위치를 등록합니다.	쓰기			
RevokePermissions	보안 주체에게서 데이터 레이크 권한을 취소합니다.	권한 관리			
UpdateResource	등록된 위치를 업데이트합니다.	쓰기			

AWS Lake Formation에서 정의한 리소스 유형

AWS Lake Formation은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Lake Formation에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Lake Formation의 조건 키

Lake Formation에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Lambda에 사용되는 작업, 리소스 및 조건 키

AWS Lambda(서비스 접두사: `lambda`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Lambda에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddLayerVersionPermission	함수 계층의 버전에 권한 정책을 추가합니다.	권한 관리	layerVersion* (p. 1326)		
AddPermission	지정된 AWS Lambda 함수와 연결된 리소스 정책에 권한을 추가합니다.	권한 관리	function* (p. 1326)		
				lambda:Principal (p. 1327)	
CreateAlias	지정된 Lambda 함수 버전을 가리키는 별칭을 생성합니다.	쓰기	function* (p. 1326)		
CreateEventSourceMapping	스트림을 Lambda 함수에 대한 이벤트 소스로 식별합니다.	쓰기		lambda:FunctionArn (p. 1326)	
CreateFunction	새 Lambda 함수를 생성합니다.	쓰기	function* (p. 1326)		
				lambda:Layer (p. 1327)	
DeleteAlias	지정된 Lambda 함수 별칭을 삭제합니다.	쓰기	function* (p. 1326)		
DeleteEventSourceMapping	이벤트 소스 매핑을 제거합니다.	쓰기	eventSourceMapping* (p. 1326)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				lambda:FunctionArn (p. 1326)	
DeleteFunction	지정된 Lambda 함수 코드 및 구성을 삭제합니다.	쓰기	function* (p. 1326)		
DeleteFunctionConcurrency	Lambda 함수에 설정된 동시성 한도를 제거합니다.	쓰기	function* (p. 1326)		
DeleteFunctionEventInvokeConfig	지정된 Lambda 함수에 대한 이벤트 호출 구성 파라미터를 삭제합니다.	쓰기	function* (p. 1326)		
DeleteLayerVersion	함수 계층의 버전을 삭제합니다.	쓰기	layerVersion* (p. 1326)		
DeleteProvisionedConcurrencyConfig	함수에 대해 프로비저닝된 동시성 구성을 삭제합니다.	쓰기	function alias (p. 1326)		
			function version (p. 1326)		
DisableReplication [권한만 해당]	Lambda 복제 서비스가 함수 코드 및 구성을 검색할 수 있도록 허용하는 리소스 정책 권한을 제거합니다.	권한 관리	function* (p. 1326)		
EnableReplication [권한만 해당]	함수 코드 및 구성을 가져올 수 있는 Lambda 복제 서비스 권한을 부여하는 리소스 정책에 권한을 추가합니다.	권한 관리	function* (p. 1326)		
GetAccountSettings	동시성과 코드 스토리지 등의 계정 제한 및 사용 통계를 반환합니다.	Read			
GetAlias	별칭 ARN, 설명 및 별칭이 가리키는 함수 버전 등 지정된 별칭 정보를 반환합니다.	Read	function* (p. 1326)		
GetEventSourceMapping	지정된 이벤트 소스 매핑에 대한 구성 정보를 반환합니다.	Read	eventSourceMapping* (p. 1326)		
				lambda:FunctionArn (p. 1326)	
GetFunction	.zip 파일을 다운로드할 수 있도록 CreateFunction을 사용하여 업로드한 .zip 파일에 대한 미리 서명된 URL 링크와 Lambda 함수의 구성 정보를 반환합니다.	Read	function* (p. 1326)		
GetFunctionConcurrency	함수의 동시성 구성에 대한 세부 정보를 반환합니다.	Read	function* (p. 1326)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetFunctionConfiguration	Lambda 함수의 구성 정보를 반환합니다.	Read	function* (p. 1326)		
GetFunctionEventInvokeConfig	지정된 Lambda 함수에 대한 이벤트 호출 구성 파라미터를 반환합니다.	Read	function* (p. 1326)		
GetLayerVersion	10분간 유효한 계층 아카이브 다운로드 링크를 사용하여 함수 계층의 버전에 대한 정보를 반환합니다.	Read	layerVersion* (p. 1326)		
GetLayerVersionPolicy	계층 버전에 대한 권한 정책을 반환합니다.	Read	layerVersion* (p. 1326)		
GetPolicy	지정된 Lambda 함수와 연결된 리소스 정책을 반환합니다.	Read	function* (p. 1326)		
GetProvisionedConcurrencyConfig	함수의 별칭 또는 버전에 대해 프로비저닝된 동시성 구성을 검색합니다.	Read	function alias (p. 1326)		
			function version (p. 1326)		
InvokeAsync	호출 요청을 AWS Lambda에 제출합니다. 더 이상 사용되지 않습니다.	쓰기	function* (p. 1326)		
InvokeFunction [권한만 해당]	특정 Lambda 함수를 호출합니다.	쓰기	function* (p. 1326)		
ListAliases	Lambda 함수에 대해 생성된 별칭 목록을 반환합니다.	List	function* (p. 1326)		
ListEventSourceMappings	CreateEventSourceMapping을 사용하여 생성한 이벤트 소스 매핑 목록을 반환합니다.	List			
ListFunctionEventInvokeConfigs	Lambda 함수, 별칭 및 버전에 대한 모든 이벤트 호출 구성 파라미터의 목록을 반환합니다.	List	function* (p. 1326)		
ListFunctions	Lambda 함수 목록을 반환합니다.	List			
ListLayerVersions	Lambda 계층 버전의 목록을 반환합니다.	List			
ListLayers	함수 계층을 나열하고 각각 최신 버전에 대한 정보를 표시합니다.	List			
ListProvisionedConcurrencyConfigs	함수에 대해 프로비저닝된 동시성 구성 목록을 검색합니다.	List	function* (p. 1326)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTags	Lambda 함수에 대한 태그를 나열합니다.	Read	function* (p. 1326)		
ListVersionsByFunction	함수의 모든 버전을 나열합니다.	List	function* (p. 1326)		
PublishLayerVersion	ZIP 아카이브에서 함수 계층을 생성합니다. 동일한 버전 이름으로 PublishLayerVersion을 호출할 때마다 새 버전이 생성됩니다.	쓰기	layer* (p. 1326)		
PublishVersion	$LATEST의 현재 스냅샷에서 함수의 버전을 게시합니다.	쓰기	function* (p. 1326)		
PutFunctionConcurrency	Lambda 함수에 동시성 한도를 추가합니다.	쓰기	function* (p. 1326)		
PutFunctionEventInvokeConfig	요청에 제공된 값을 사용하여 지정된 Lambda 함수에 대한 이벤트 호출 구성 파라미터를 추가합니다.	쓰기	function* (p. 1326)		
PutProvisionedConcurrencyConfig	함수의 별칭 또는 버전에 대해 프로비저닝된 동시성 구성을 추가합니다.	쓰기	function alias (p. 1326)		
			function version (p. 1326)		
RemoveLayerVersionPermission	계층 버전에 대한 권한 정책에서 설명을 제거합니다.	권한 관리	layerVersion* (p. 1326)		
RemovePermission	권한을 추가했을 때 제공한 문 ID를 제공하여 Lambda 함수와 연결된 리소스 정책에서 개별 권한을 제거할 수 있습니다.	권한 관리	function* (p. 1326)		
				lambda:Principal (p. 1327)	
TagResource	Lambda 함수에 태그를 추가합니다.	쓰기	function* (p. 1326)		
UntagResource	Lambda 함수에서 태그를 제거합니다.	쓰기	function* (p. 1326)		
UpdateAlias	이 API를 사용하여 별칭이 가리키는 함수 버전과 별칭 설명을 업데이트할 수 있습니다.	쓰기	function* (p. 1326)		
UpdateEventSourceMapping	이벤트 소스 매핑을 업데이트할 수 있습니다.	쓰기	eventSourceMapping* (p. 1326)		
				lambda:FunctionArn (p. 1326)	
UpdateFunctionCode	지정된 Lambda 함수에 대한 코드를 업데이트합니다.	쓰기	function* (p. 1326)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateFunctionConfiguration	요청에 제공된 값을 사용하여 지정된 Lambda 함수에 대한 구성 파라미터를 업데이트합니다.	쓰기	function* (p. 1326)		
				lambda:Layer (p. 1327)	
UpdateFunctionEventInvokeConfig	요청에 제공된 값을 사용하여 지정된 Lambda 함수에 대한 이벤트 호출 구성 파라미터를 업데이트합니다.	쓰기	function* (p. 1326)		

AWS Lambda에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1322)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
function	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}`	
function version	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}`	
function alias	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Alias}`	
layer	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}`	
layerVersion	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}:${LayerVersion}`	
eventSourceMapping	`arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}`	

AWS Lambda의 조건 키

AWS Lambda는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
lambda:FunctionArn	Lambda 함수의 ARN입니다.	ARN

조건 키	설명	유형
lambda:Layer	Lambda 계층의 ARN입니다.	문자열
lambda:Principal	AWS 보안 주체입니다.	문자열

Launch Wizard에 사용되는 작업, 리소스 및 조건 키

Launch Wizard(서비스 접두사: `launchwizard`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

주제

Launch Wizard에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteApp [권한만 해당]	애플리케이션을 삭제합니다.	쓰기			
DescribeProvisionedApp [권한만 해당]	프로비저닝 애플리케이션을 설명합니다.	Read			
DescribeProvisioningEvents [권한만 해당]	프로비저닝 이벤트를 설명합니다.	Read			
GetInfrastructureSuggestion [권한만 해당]	인프라 제안을 받습니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetIpAddress [권한만 해당]	고객의 IP 주소를 가져옵니다.	Read			
GetResourceCostEstimate [권한만 해당]	리소스 비용 예측을 가져옵니다.	Read			
ListProvisionedApps [권한만 해당]	프로비저닝 애플리케이션을 나열합니다.	List			
StartProvisioning [권한만 해당]	프로비저닝을 시작합니다.	쓰기			

Launch Wizard에서 정의한 리소스 유형

Launch Wizard는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Launch Wizard에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Launch Wizard에 사용되는 조건 키

Launch Wizard에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Lex에 사용되는 작업, 리소스 및 조건 키

Amazon Lex(서비스 접두사: `lex`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Lex에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시

됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateBotVersion	지정된 봇의 $LATEST 버전을 기반으로 새 버전을 생성합니다.	쓰기	bot* (p. 1331)		
CreateIntentVersion	지정된 의도의 $LATEST 버전을 기반으로 새 버전을 생성합니다.	쓰기	intent* (p. 1331)		
CreateSlotTypeVersion	지정된 슬롯 유형의 $LATEST 버전을 기반으로 새 버전을 생성합니다.	쓰기	slottype* (p. 1331)		
DeleteBot	봇의 모든 버전을 삭제합니다.	쓰기	bot* (p. 1331)		
DeleteBotAlias	지정된 봇의 별칭을 삭제합니다.	쓰기	bot* (p. 1331)		
DeleteBotChannelAssociation	Amazon Lex 봇 별칭과 메시징 플랫폼 간의 연결을 삭제합니다.	쓰기	channel* (p. 1331)		
DeleteBotVersion	봇의 특정 버전을 삭제합니다.	쓰기	bot* (p. 1331)		
DeleteIntent	의도의 모든 버전을 삭제합니다.	쓰기	intent* (p. 1331)		
DeleteIntentVersion	의도의 특정 버전을 삭제합니다.	쓰기	intent* (p. 1331)		
DeleteSlotType	슬롯 유형의 모든 버전을 삭제합니다.	쓰기	slottype* (p. 1331)		
DeleteSlotTypeVersion	슬롯 유형의 특정 버전을 삭제합니다.	쓰기	slottype* (p. 1331)		
DeleteUtterances	Amazon Lex가 특정 봇 및 userId에서 utterances를 위해 유지하는 정보를 삭제합니다.	쓰기	bot* (p. 1331)		
GetBot	특정 봇에 대한 정보를 반환합니다. 봇 이름 뿐만 아니라 봇 버전 또는 별칭도 필요합니다.	Read	bot* (p. 1331)		
GetBotAlias	Amazon Lex 봇 별칭에 대한 정보를 반환합니다.	Read	bot* (p. 1331)		
GetBotAliases	지정된 Amazon Lex 봇에 대한 별칭 목록을 반환합니다.	List	bot* (p. 1331)		
GetBotChannelAssociation	Amazon Lex 봇과 메시징 플랫폼 간의 연결에 대한 정보를 반환합니다.	Read	channel* (p. 1331)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetBotChannelAssociations	단일 봇과 연결된 모든 채널의 목록을 반환합니다.	List	channel* (p. 1331)		
GetBotVersions	특정 봇의 모든 버전에 대한 정보를 반환합니다.	List	bot* (p. 1331)		
GetBots	클라이언트에서 제공하는 필터에 따라 모든 봇의 $LATEST 버전에 대한 정보를 반환합니다.	List			
GetBuiltinIntent	기본 제공 의도에 관한 정보를 반환합니다.	Read			
GetBuiltinIntents	지정된 기준에 맞는 기본 제공 의도의 목록을 가져옵니다.	Read			
GetBuiltinSlotTypes	지정된 기준에 맞는 기본 제공 슬롯 유형을 가져옵니다.	Read			
GetIntent	특정 의도에 대한 정보를 반환합니다. 의도 이름 뿐만 아니라 의도 버전 또한 지정해야 합니다.	Read	intent* (p. 1331)		
GetIntentVersions	특정 의도의 모든 버전에 대한 정보를 반환합니다.	List	intent* (p. 1331)		
GetIntents	클라이언트에서 제공하는 필터에 따라 모든 의도의 $LATEST 버전에 대한 정보를 반환합니다.	List			
GetSlotType	슬롯 유형의 특정 버전에 대한 정보를 반환합니다. 슬롯 유형 이름을 지정할 뿐만 아니라 슬롯 유형 버전 또한 지정해야 합니다.	Read	slottype* (p. 1331)		
GetSlotTypeVersions	특정 슬롯 유형의 모든 버전에 대한 정보를 반환합니다.	List	slottype* (p. 1331)		
GetSlotTypes	클라이언트에서 제공하는 필터에 따라 모든 슬롯 유형의 $LATEST 버전에 대한 정보를 반환합니다.	List			
GetUtterancesView	최근 기간 동안 봇의 버전에 대한 집계 utterance 데이터의 보기를 반환합니다.	List	bot* (p. 1331)		
PostContent	Amazon Lex에 사용자 입력(텍스트 또는 스피치)을 전송합니다.	쓰기	bot* (p. 1331)		
PostText	Amazon Lex에 사용자 입력(텍스트만)을 전송합니다.	쓰기	bot* (p. 1331)		
PutBot	Amazon Lex 대화형 봇의 $LATEST 버전을 생성하거나 업데이트합니다.	쓰기	bot* (p. 1331)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutBotAlias	특정 봇의 별칭을 생성하거나 업데이트합니다.	쓰기	bot* (p. 1331)		
PutIntent	의도의 $LATEST 버전을 생성하거나 업데이트합니다.	쓰기	intent* (p. 1331)		
PutSlotType	슬롯 유형의 $LATEST 버전을 생성하거나 업데이트합니다.	쓰기	slottype* (p. 1331)		

Amazon Lex에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1328)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
bot	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotVersionOrAlias}`	
channel	`arn:${Partition}:lex:${Region}:${Account}:bot-channel:${BotName}:${BotAlias}:${ChannelName}`	
intent	`arn:${Partition}:lex:${Region}:${Account}:intent:${IntentName}:${IntentVersion}`	
slottype	`arn:${Partition}:lex:${Region}:${Account}:slottype:${SlotName}:${SlotVersion}`	

Amazon Lex에 사용되는 조건 키

Amazon Lex는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
lex:associatedIntents	요청에 포함된 의도를 기반으로 액세스를 제어할 수 있습니다.	문자열
lex:associatedSlotTypes	요청에 포함된 슬롯 유형을 기반으로 액세스를 제어할 수 있습니다.	문자열
lex:channelType	요청에 포함된 채널 유형을 기반으로 액세스를 제어할 수 있습니다.	문자열

AWS License Manager에 사용되는 작업, 리소스 및 조건 키

AWS License Manager(서비스 접두사: `license-manager`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS License Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateLicenseConfiguration	새 라이선스 구성을 생성합니다.	태그 지정		aws:RequestTag/${TagKey} (p. 1334) aws:TagKeys (p. 1334)	
DeleteLicenseConfiguration	라이선스 구성을 영구적으로 삭제합니다.	쓰기	license-configuration* (p. 1333)		
GetLicenseConfiguration	라이선스 구성을 가져옵니다.	List	license-configuration* (p. 1333)		
GetServiceSettings	서비스 설정을 가져옵니다.	List			
ListAssociationsForLicenseConfiguration	선택된 라이선스 구성에 대한 연결을 나열합니다.	List	license-configuration* (p. 1333)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListLicenseConfigurations	라이선스 구성을 나열합니다.	List			
ListLicenseSpecificationsForResource	선택된 리소스와 연결된 라이선스 사양을 나열합니다.	List			
ListResourceInventory	리소스 인벤토리를 나열합니다.	List			
ListTagsForResource	선택된 리소스에 대한 태그를 나열합니다.	List	license-configuration* (p. 1333)		
ListUsageForLicenseConfiguration	선택된 라이선스 구성의 사용 레코드를 나열합니다.	List	license-configuration* (p. 1333)		
TagResource	선택된 리소스에 태그를 지정합니다.	태그 지정	license-configuration* (p. 1333)		
				aws:RequestTag/${TagKey} (p. 1334) aws:TagKeys (p. 1334)	
UntagResource	선택된 리소스에서 태그를 제거합니다.	태그 지정	license-configuration* (p. 1333)		
UpdateLicenseConfiguration	기존 라이선스 구성을 업데이트합니다.	쓰기	license-configuration* (p. 1333)		
UpdateLicenseSpecificationsForResource	선택된 라이선스의 라이선스 사양을 업데이트합니다.	쓰기	license-configuration* (p. 1333)		
UpdateServiceSettings	서비스 설정을 업데이트합니다.	권한 관리			

AWS License Manager에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1332)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
license-configuration	`arn:${Partition}:license-manager:${Region}:${Account}:license-configuration/${LicenseConfigurationId}`	license-manager:ResourceTag/${TagKey} (p. 1334)

AWS License Manager에 사용되는 조건 키

AWS License Manager는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 필수 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:TagKeys	요청에서 사용되는 태그 키를 강제 적용합니다.	문자열
license-manager:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열

Amazon Lightsail에 사용되는 작업, 리소스 및 조건 키

Amazon Lightsail(서비스 접두사: `lightsail`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Lightsail에서 정의한 작업 (p. 1334)
- Amazon Lightsail에서 정의한 리소스 유형 (p. 1344)
- Amazon Lightsail의 조건 키 (p. 1345)

Amazon Lightsail에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AllocateStaticIp	인스턴스에 연결할 수 있는 고정 IP 주소를 생성합니다.	쓰기	StaticIp* (p. 1345)		
AttachDisk	인스턴스에 디스크를 연결합니다.	쓰기	Disk* (p. 1345)		
			Instance* (p. 1345)		
AttachInstancesToLoadBalancer	로드 밸런서에 하나 이상의 인스턴스를 연결합니다.	쓰기	Instance* (p. 1345)		
			LoadBalancer* (p. 1345)		
AttachLoadBalancerTlsCertificate	로드 밸런서에 TLS 인증서를 연결합니다.	쓰기	LoadBalancer* (p. 1345)		
AttachStaticIp	인스턴스에 고정 IP 주소를 연결합니다.	쓰기	Instance* (p. 1345)		
			StaticIp* (p. 1345)		
CloseInstancePublicPorts	인스턴스의 퍼블릭 포트를 닫습니다.	쓰기	Instance* (p. 1345)		
CopySnapshot	Amazon Lightsail의 한 AWS 리전에서 다른 AWS 리전으로 스냅샷을 복사합니다.	쓰기			
CreateCloudFormationStack	내보낸 Amazon Lightsail 스냅샷에서 새 Amazon EC2 인스턴스를 생성합니다.	쓰기	ExportSnapshotRecord* (p. 1345)		
CreateDisk	디스크를 생성합니다.	쓰기	Disk* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateDiskFromSnapshot	스냅샷에서 디스크를 생성합니다.	쓰기	Disk* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateDiskSnapshot	디스크 스냅샷을 생성합니다.	쓰기	Disk* (p. 1345)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateDomain	지정된 도메인 이름에 대한 도메인 리소스를 생성합니다.	쓰기	Domain* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateDomainEntry	주소(A), 정식 이름(CNAME), 메일 교환기(MX), 이름 서버(NS), 권한 시작(SOA), 서비스 로케이터(SRV) 또는 텍스트(TXT) 등 도메인 리소스에 대한 하나 이상의 DNS 레코드 항목을 생성합니다.	쓰기	Domain* (p. 1345)		
CreateInstanceSnapshot	인스턴스 스냅샷을 생성합니다.	쓰기	Instance* (p. 1345)		
			InstanceSnapshot* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateInstances	하나 이상의 인스턴스를 생성합니다.	쓰기	KeyPair* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateInstancesFromSnapshot	인스턴스 스냅샷을 기반으로 하나 이상의 인스턴스를 생성합니다.	쓰기	Instance* (p. 1345)		
			InstanceSnapshot* (p. 1345)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateKeyPair	인스턴스를 인증하고 연결하는 데 사용되는 키 페어를 생성합니다.	쓰기	KeyPair* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateLoadBalancer	로드 밸런서를 생성합니다.	쓰기	LoadBalancer* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateLoadBalancerTlsCertificate	로드 밸런서 TLS 인증서를 생성합니다.	쓰기	LoadBalancer* (p. 1345)		
CreateRelationalDatabase	새 관계형 데이터베이스를 생성합니다.	쓰기	RelationalDatabase* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateRelationalDatabaseFromSnapshot	스냅샷에서 새 관계형 데이터베이스를 생성합니다.	쓰기	RelationalDatabase* (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
CreateRelationalDatabaseSnapshot	관계형 데이터베이스 스냅샷을 생성합니다.	쓰기	RelationalDatabaseSnapshot* (p. 1345)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
DeleteDisk	디스크를 삭제합니다.	쓰기	Disk* (p. 1345)		
DeleteDiskSnapshot	디스크 스냅샷을 삭제합니다.	쓰기	Disk* (p. 1345)		
DeleteDomain	도메인 리소스와 모든 DNS 레코드를 삭제합니다.	쓰기	Domain* (p. 1345)		
DeleteDomainEntry	도메인 리소스에 대한 DNS 레코드 항목을 삭제합니다.	쓰기	Domain* (p. 1345)		
DeleteInstance	인스턴스를 삭제합니다.	쓰기	Instance* (p. 1345)		
DeleteInstanceSnapshot	인스턴스 스냅샷을 삭제합니다.	쓰기	InstanceSnapshot* (p. 1345)		
DeleteKeyPair	인스턴스를 인증하고 연결하는 데 사용되는 키 페어를 삭제합니다.	쓰기	KeyPair* (p. 1345)		
DeleteKnownHostKeys	Amazon Lightsail 브라우저 기반 SSH 또는 RDP 클라이언트가 인스턴스를 인증하는 데 사용하는 알려진 호스트 키 또는 인증서를 삭제합니다.	쓰기	Instance* (p. 1345)		
DeleteLoadBalancer	로드 밸런서를 삭제합니다.	쓰기	LoadBalancer* (p. 1345)		
DeleteLoadBalancerTlsCertificate	로드 밸런서 TLS 인증서를 삭제합니다.	쓰기	LoadBalancer* (p. 1345)		
DeleteRelationalDatabase	관계형 데이터베이스를 삭제합니다.	쓰기	RelationalDatabase* (p. 1345)		
DeleteRelationalDatabaseSnapshot	관계형 데이터베이스 스냅샷을 삭제합니다.	쓰기	RelationalDatabaseSnapshot* (p. 1345)		
DetachDisk	인스턴스에서 디스크를 분리합니다.	쓰기	Disk* (p. 1345)		
DetachInstancesFromLoadBalancer	로드 밸런서에서 하나 이상의 인스턴스를 분리합니다.	쓰기	Instance* (p. 1345)		
			LoadBalancer* (p. 1345)		
DetachStaticIp	연결된 인스턴스에서 고정 IP를 분리합니다.	쓰기	Instance* (p. 1345)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			StaticIp* (p. 1345)		
DownloadDefaultKeyPair	특정 AWS 리전의 인스턴스를 인증하고 연결하는 데 사용되는 기본 키 페어를 다운로드합니다.	쓰기	KeyPair* (p. 1345)		
ExportSnapshot	Amazon Lightsail 스냅샷을 Amazon EC2로 내보냅니다.	쓰기			
GetActiveNames	모든 활성(삭제되지 않음) 리소스의 이름을 반환합니다.	Read			
GetBlueprints	인스턴스 이미지 또는 블루프린트의 목록을 반환합니다. 블루프린트를 사용하여 특정 운영 체제뿐만 아니라 사전 설치된 애플리케이션 또는 개발 스택이 이미 실행 중인 새 인스턴스를 생성할 수 있습니다. 인스턴스에서 실행되는 소프트웨어는 인스턴스 생성 시 정의한 블루프린트에 따라 달라집니다.	List			
GetBundles	인스턴스 번들의 목록을 반환합니다. 번들을 사용하여 CPU 수, 디스크 크기, RAM 크기 및 네트워크 전송 허용량과 같은 일련의 성능 사양을 가진 새 인스턴스를 생성할 수 있습니다. 인스턴스 비용은 인스턴스 생성 시 정의한 번들에 따라 달라집니다.	List			
GetCloudFormationStackRecords	내보낸 Amazon Lightsail 스냅샷에서 Amazon EC2 리소스를 생성하는 데 사용된 모든 CloudFormation 스택에 대한 정보를 반환합니다.	List	CloudFormationStackRecord* (p. 1345)		
GetDisk	디스크에 대한 정보를 반환합니다.	Read	Disk* (p. 1345)		
GetDiskSnapshot	디스크 스냅샷에 대한 정보를 반환합니다.	Read	Disk* (p. 1345)		
GetDiskSnapshots	모든 디스크 스냅샷에 대한 정보를 반환합니다.	List	Disk* (p. 1345)		
GetDisks	모든 디스크에 대한 정보를 반환합니다.	List			
GetDomain	도메인 리소스에 대한 DNS 레코드를 반환합니다.	Read	Domain* (p. 1345)		
GetDomains	모든 도메인 리소스에 대한 DNS 레코드를 반환합니다.	Read	Domain* (p. 1345)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetExportSnapshotRecords	Amazon Lightsail 스냅샷을 Amazon EC2로 내보낼 모든 레코드에 대한 정보를 반환합니다.	List	ExportSnapshotRecord* (p. 1345)		
GetInstance	인스턴스에 대한 정보를 반환합니다.	Read	Instance* (p. 1345)		
GetInstanceAccessDetails	인스턴스를 인증하고 연결하는 데 사용할 수 있는 임시 키를 반환합니다.	쓰기	Instance* (p. 1345)		
GetInstanceMetricData	인스턴스의 지정된 지표에 대한 데이터 포인트를 반환합니다.	Read	Instance* (p. 1345)		
GetInstancePortStates	인스턴스의 포트 상태를 반환합니다.	Read	Instance* (p. 1345)		
GetInstanceSnapshot	인스턴스 스냅샷에 대한 정보를 반환합니다.	Read	InstanceSnapshot* (p. 1345)		
GetInstanceSnapshots	모든 인스턴스 스냅샷에 대한 정보를 반환합니다.	List	InstanceSnapshot* (p. 1345)		
GetInstanceState	인스턴스의 상태를 반환합니다.	Read	Instance* (p. 1345)		
GetInstances	모든 인스턴스에 대한 정보를 반환합니다.	Read	Instance* (p. 1345)		
GetKeyPair	키 페어에 대한 정보를 반환합니다.	List	KeyPair* (p. 1345)		
GetKeyPairs	모든 키 페어에 대한 정보를 반환합니다.	Read	KeyPair* (p. 1345)		
GetLoadBalancer	로드 밸런서에 대한 정보를 반환합니다.	Read	LoadBalancer* (p. 1345)		
GetLoadBalancerMetricData	로드 밸런서의 지정된 지표에 대한 데이터 포인트를 반환합니다.	Read	LoadBalancer* (p. 1345)		
GetLoadBalancerTlsCertificates	로드 밸런서 TLS 인증서에 대한 정보를 반환합니다.	Read	LoadBalancer* (p. 1345)		
GetLoadBalancers	로드 밸런서에 대한 정보를 반환합니다.	Read	LoadBalancer* (p. 1345)		
GetOperation	작업에 대한 정보를 반환합니다. 작업에는 인스턴스를 생성하고 고정 IP를 할당하며 고정 IP를 연결하는 등의 경우와 같은 이벤트가 포함됩니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetOperations	모든 작업에 대한 정보를 반환합니다. 작업에는 인스턴스를 생성하고 고정 IP를 할당하며 고정 IP를 연결하는 등의 경우와 같은 이벤트가 포함됩니다.	Read			
GetOperationsForResource	리소스에 대한 작업을 반환합니다.	Read	Domain (p. 1345)		
			Instance (p. 1345)		
			InstanceSnapshot (p. 1345)		
			KeyPair (p. 1345)		
			StaticIp (p. 1345)		
GetRegions	Amazon Lightsail에 대해 유효한 모든 AWS 리전의 목록을 반환합니다.	List			
GetRelationalDatabase	관계형 데이터베이스에 대한 정보를 반환합니다.	List	RelationalDatabase* (p. 1345)		
GetRelationalDatabaseBlueprints	관계형 데이터베이스 이미지 또는 블루프린트 목록을 반환합니다. 블루프린트를 사용하여 특정 데이터베이스 엔진을 실행하는 새 데이터베이스를 생성할 수 있습니다. 데이터베이스에서 실행되는 데이터베이스 엔진은 관계형 데이터베이스를 생성할 때 정의하는 블루프린트에 따라 달라집니다.	List			
GetRelationalDatabaseBundles	관계형 데이터베이스 번들의 목록을 반환합니다. 번들을 사용하여 CPU 수, 디스크 크기, RAM 크기, 네트워크 전송 허용량 및 고가용성 표준과 같은 일련의 성능 사양을 가진 새 데이터베이스를 생성할 수 있습니다. 데이터베이스 비용은 관계형 데이터베이스를 생성할 때 정의한 번들에 따라 달라집니다.	List			
GetRelationalDatabaseEvents	관계형 데이터베이스에 대한 이벤트를 반환합니다.	Read			
GetRelationalDatabaseLogEvents	관계형 데이터베이스의 지정된 로그 스트림에 대한 이벤트를 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetRelationalDatabaseBlueprints	관계형 데이터베이스에 사용할 수 있는 블루프린트를 반환합니다.	Read			
GetRelationalDatabaseMasterUserPassword	관계형 데이터베이스의 마스터 사용자 암호를 반환합니다.	쓰기			
GetRelationalDatabaseMetricData	관계형 데이터베이스의 지정된 지표에 대한 데이터 포인트를 반환합니다.	Read			
GetRelationalDatabaseParameters	관계형 데이터베이스의 파라미터를 반환합니다.	List			
GetRelationalDatabaseSnapshot	관계형 데이터베이스 스냅샷에 대한 정보를 반환합니다.	List	RelationalDatabase* (p. 1345)		
GetRelationalDatabaseSnapshots	모든 관계형 데이터베이스 스냅샷에 대한 정보를 반환합니다.	List	RelationalDatabase* (p. 1345)		
GetRelationalDatabase	모든 관계형 데이터베이스에 대한 정보를 반환합니다.	Read	RelationalDatabase* (p. 1345)		
GetStaticIp	고정 IP에 대한 정보를 반환합니다.	Read	StaticIp* (p. 1345)		
GetStaticIps	모든 고정 IP에 대한 정보를 반환합니다.	Read	StaticIp* (p. 1345)		
ImportKeyPair	키 페어에서 퍼블릭 키를 가져옵니다.	쓰기	KeyPair* (p. 1345)		
IsVpcPeered	Amazon Lightsail Virtual Private Cloud(VPC)가 피어링되는지 여부를 나타내는 부울 값을 반환합니다.	Read			
OpenInstancePublicPorts	인스턴스의 퍼블릭 포트를 추가하기 위해 엽니다.	쓰기	Instance* (p. 1345)		
PeerVpc	Amazon Lightsail Virtual Private Cloud(VPC)를 기본 VPC로 피어링하려고 시도합니다.	쓰기			
PutInstancePublicPorts	인스턴스에 대해 지정된 개방 포트를 설정하고 요청에 포함되지 않은 모든 프로토콜의 모든 포트를 닫습니다.	쓰기	Instance* (p. 1345)		
RebootInstance	실행 중인 상태의 인스턴스를 재부팅합니다.	쓰기	Instance* (p. 1345)		
RebootRelationalDatabase	실행 중인 상태의 관계형 데이터베이스를 재부팅합니다.	쓰기	RelationalDatabase* (p. 1345)		
ReleaseStaticIp	고정 IP를 삭제합니다.	쓰기	StaticIp* (p. 1345)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartInstance	중지된 상태의 인스턴스를 시작합니다.	쓰기	Instance* (p. 1345)		
StartRelationalDatabase	중지된 상태의 관계형 데이터베이스를 시작합니다.	쓰기	RelationalDatabase* (p. 1345)		
StopInstance	실행 중인 상태의 인스턴스를 중지합니다.	쓰기	Instance* (p. 1345)		
StopRelationalDatabase	실행 중인 상태의 관계형 데이터베이스를 중지합니다.	쓰기	RelationalDatabase* (p. 1345)		
TagResource	리소스에 태그를 지정합니다.	쓰기	Disk (p. 1345)		
			DiskSnapshot (p. 1345)		
			Domain (p. 1345)		
			Instance (p. 1345)		
			InstanceSnapshot (p. 1345)		
			KeyPair (p. 1345)		
			LoadBalancer (p. 1345)		
			RelationalDatabase (p. 1345)		
			RelationalDatabaseSnapshot (p. 1345)		
			StaticIp (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
UnpeerVpc	Amazon Lightsail Virtual Private Cloud(VPC)를 기본 VPC에서 피어링 해제하려고 시도합니다.	쓰기			
UntagResource	리소스에서 태그를 제거합니다.	쓰기	Disk (p. 1345)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			DiskSnapshot (p. 1345)		
			Domain (p. 1345)		
			Instance (p. 1345)		
			InstanceSnapshot (p. 1345)		
			KeyPair (p. 1345)		
			LoadBalancer (p. 1345)		
			RelationalDatabase (p. 1345)		
			RelationalDatabaseSnapshot (p. 1345)		
			StaticIp (p. 1345)		
				aws:RequestTag/${TagKey} (p. 1345) aws:TagKeys (p. 1346)	
UpdateDomainEntry	생성된 도메인 RecordSet를 업데이트합니다.	쓰기	Domain* (p. 1345)		
UpdateLoadBalancerAttribute	상태 확인 경로 및 세션 고정성과 같은 로드 밸런서 속성을 업데이트합니다.	쓰기	LoadBalancer* (p. 1345)		
UpdateRelationalDatabase	관계형 데이터베이스를 업데이트합니다.	쓰기	RelationalDatabase* (p. 1345)		
UpdateRelationalDatabaseParameters	관계형 데이터베이스의 파라미터를 업데이트합니다.	쓰기			

Amazon Lightsail에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1334)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Domain	`arn:${Partition}:lightsail:${Region}:${Account}:Domain/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
Instance	`arn:${Partition}:lightsail:${Region}:${Account}:Instance/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
InstanceSnapshot	`arn:${Partition}:lightsail:${Region}:${Account}:InstanceSnapshot/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
KeyPair	`arn:${Partition}:lightsail:${Region}:${Account}:KeyPair/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
StaticIp	`arn:${Partition}:lightsail:${Region}:${Account}:StaticIp/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
Disk	`arn:${Partition}:lightsail:${Region}:${Account}:Disk/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
DiskSnapshot	`arn:${Partition}:lightsail:${Region}:${Account}:DiskSnapshot/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
LoadBalancer	`arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancer/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
PeeredVpc	`arn:${Partition}:lightsail:${Region}:${Account}:PeeredVpc/${Id}`	
LoadBalancerTlsCertificate	`arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancerTlsCertificate/${Id}`	
ExportSnapshotRecord	`arn:${Partition}:lightsail:${Region}:${Account}:ExportSnapshotRecord/${Id}`	
CloudFormationStackRecord	`arn:${Partition}:lightsail:${Region}:${Account}:CloudFormationStackRecord/${Id}`	
RelationalDatabase	`arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabase/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)
RelationalDatabaseSnapshot	`arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabaseSnapshot/${Id}`	aws:ResourceTag/${TagKey} (p. 1346)

Amazon Lightsail의 조건 키

Amazon Lightsail은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon Machine Learning에 사용되는 작업, 리소스 및 조건 키

Amazon Machine Learning(서비스 접두사: `machinelearning`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Machine Learning에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTags	객체에 하나 이상의 태그를 추가합니다(최대 10개까지). 각 태그는 키와 값(선택 사항)으로 구성됩니다	태그 지정	batchprediction (p. 1349)		
			datasource (p. 1349)		
			evaluation (p. 1349)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			mlmodel (p. 1349)		
CreateBatchPrediction	관측치 그룹에 대한 예측을 생성합니다.	쓰기	batchprediction* (p. 1349)		
			datasource* (p. 1349)		
			mlmodel* (p. 1349)		
CreateDataSourceFromRDS	Amazon RDS에서 DataSource 객체를 생성합니다.	쓰기	datasource* (p. 1349)		
CreateDataSourceFromRedshift	Amazon Redshift 클러스터에 호스팅된 데이터베이스에서 DataSource 객체를 생성합니다.	쓰기	datasource* (p. 1349)		
CreateDataSourceFromS3	S3에서 DataSource 객체를 생성합니다.	쓰기	datasource* (p. 1349)		
CreateEvaluation	MLModel의 새 평가를 생성합니다.	쓰기	datasource* (p. 1349)		
			evaluation* (p. 1349)		
			mlmodel* (p. 1349)		
CreateMLModel	새 MLModel을 생성합니다.	쓰기	datasource* (p. 1349)		
			mlmodel* (p. 1349)		
CreateRealtimeEndpoint	MLModel에 대한 실시간 엔드포인트를 생성합니다.	쓰기	mlmodel* (p. 1349)		
DeleteBatchPrediction	BatchPrediction에 DELETED 상태를 할당하여 사용 불가 상태로 만듭니다.	쓰기	batchprediction* (p. 1349)		
DeleteDataSource	DataSource에 DELETED 상태를 할당하여 사용 불가 상태로 만듭니다.	쓰기	datasource* (p. 1349)		
DeleteEvaluation	Evaluation에 DELETED 상태를 할당하여 사용 불가 상태로 만듭니다.	쓰기	evaluation* (p. 1349)		
DeleteMLModel	MLModel에 DELETED 상태를 할당하여 사용 불가 상태로 만듭니다.	쓰기	mlmodel* (p. 1349)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteRealtimeEndpoint	MLModel의 실시간 엔드포인트를 삭제합니다.	쓰기	mlmodel* (p. 1349)		
DeleteTags	ML 객체와 연결된 지정된 태그를 삭제합니다. 이 작업이 완료된 후에는 삭제된 태그를 복구할 수 없습니다.	태그 지정	batchprediction (p. 1349)		
			datasource (p. 1349)		
			evaluation (p. 1349)		
			mlmodel (p. 1349)		
DescribeBatchPredictions	요청의 검색 기준과 일치하는 BatchPrediction 작업의 목록을 반환합니다.	List			
DescribeDataSources	요청의 검색 기준과 일치하는 DataSource의 목록을 반환합니다.	List			
DescribeEvaluations	요청의 검색 기준과 일치하는 DescribeEvaluations의 목록을 반환합니다.	List			
DescribeMLModels	요청의 검색 기준과 일치하는 MLModel의 목록을 반환합니다.	List			
DescribeTags	Amazon ML 객체에 대한 하나 이상의 태그를 설명합니다.	List	batchprediction (p. 1349)		
			datasource (p. 1349)		
			evaluation (p. 1349)		
			mlmodel (p. 1349)		
GetBatchPrediction	상세 메타데이터, 상태 및 데이터 파일 정보가 포함된 BatchPrediction를 반환합니다.	Read	batchprediction* (p. 1349)		
GetDataSource	메타데이터 및 데이터 파일 정보가 포함된 DataSource 뿐만 아니라 DataSource의 현재 상태를 반환합니다.	Read	datasource* (p. 1349)		
GetEvaluation	메타데이터가 포함된 Evaluation 뿐만 아니라 Evaluation의 현재 상태를 반환합니다.	Read	datasource* (p. 1349)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetMLModel	상세 메타데이터 및 데이터 원본 정보가 포함된 MLModel 뿐만 아니라 MLModel의 현재 상태를 반환합니다.	Read	mlmodel* (p. 1349)		
Predict	지정된 ML Model을 사용하여 관측치에 대한 예측을 생성합니다.	쓰기	mlmodel* (p. 1349)		
UpdateBatchPrediction	BatchPrediction의 BatchPredictionName을 업데이트합니다.	쓰기	batchprediction* (p. 1349)		
UpdateDataSource	DataSource의 DataSourceName을 업데이트합니다.	쓰기	datasource* (p. 1349)		
UpdateEvaluation	Evaluation의 EvaluationName을 업데이트합니다.	쓰기	evaluation* (p. 1349)		
UpdateMLModel	MLModel의 MLModelName 및 ScoreThreshold를 업데이트합니다.	쓰기	mlmodel* (p. 1349)		

Amazon Machine Learning에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1346)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
batchprediction	`arn:${Partition}:machinelearning:${Region}:${Account}:batchprediction/${BatchPredictionId}`	
datasource	`arn:${Partition}:machinelearning:${Region}:${Account}:datasource/${DatasourceId}`	
evaluation	`arn:${Partition}:machinelearning:${Region}:${Account}:evaluation/${EvaluationId}`	
mlmodel	`arn:${Partition}:machinelearning:${Region}:${Account}:mlmodel/${MlModelId}`	

Amazon Machine Learning에 사용되는 조건 키

기계 학습에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Macie에 사용되는 작업, 리소스 및 조건 키

Amazon Macie(서비스 접두사: `macie`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Macie에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateMemberAccount	사용자가 지정된 AWS 계정을 멤버 계정으로 Amazon Macie와 연결할 수 있습니다.	쓰기			
AssociateS3Resources	사용자가 모니터링 및 데이터 분류를 위해 S3 리소스를 Amazon Macie와 연결할 수 있습니다.	쓰기		aws:SourceArn (p. 1351)	
DisassociateMemberAccount	사용자가 Amazon Macie에서 지정된 멤버 계정을 제거할 수 있습니다.	쓰기			
DisassociateS3Resources	사용자가 Amazon Macie에 의해 모니터링되는 지정된 S3 리소스를 제거할 수 있습니다.	쓰기		aws:SourceArn (p. 1351)	
ListMemberAccounts	사용자가 현재 Amazon Macie 마스터 계정의 모든 Macie 멤버 계정을 나열할 수 있습니다.	List			
ListS3Resources	사용자가 Amazon Macie와 연결된 모든 S3 리소스를 나열할 수 있습니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateS3Resources	사용자가 지정된 S3 리소스의 분류유형을 업데이트할 수 있습니다.	쓰기		aws:SourceArn (p. 1351)	

Amazon Macie에서 정의한 리소스 유형

Amazon Macie는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Macie에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Macie에 사용되는 조건 키

Amazon Macie는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:SourceArn	요청이 지정된 AWS 리소스에 대해 작동하는 경우에만 지정된 작업에 대한 액세스를 허용합니다.	Arn

Manage Amazon API Gateway에 사용되는 작업, 리소스 및 조건 키

Manage Amazon API Gateway(서비스 접두사: `apigateway`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Manage Amazon API Gateway에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DELETE	리소스를 삭제하는 데 사용됩니다.	쓰기	apigateway-general* (p. 1353)		
				aws:RequestTag/${TagKey} (p. 1353) aws:TagKeys (p. 1353)	
GET	리소스에 대한 정보를 가져오는 데 사용됩니다.	Read	apigateway-general* (p. 1353)		
PATCH	리소스를 업데이트하는 데 사용됩니다.	쓰기	apigateway-general* (p. 1353)		
				aws:RequestTag/${TagKey} (p. 1353) aws:TagKeys (p. 1353)	
POST	하위 리소스를 생성하는 데 사용됩니다.	쓰기	apigateway-general* (p. 1353)		
				aws:RequestTag/${TagKey} (p. 1353) aws:TagKeys (p. 1353)	
PUT	리소스를 업데이트하는 데 사용됩니다(권장되지는 않지만 하위 리소스를 생성하는 데에도 사용될 수 있습니다).	쓰기	apigateway-general* (p. 1353)		
				aws:RequestTag/${TagKey} (p. 1353) aws:TagKeys (p. 1353)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SetWebACL	WAF에 WebAcl 권한을 부여합니다.	쓰기	apigateway-general* (p. 1353)		
UpdateRestApiPolicy	지정된 API에 대한 리소스 정책을 업데이트하는 데 사용됩니다.	쓰기	apigateway-general* (p. 1353)		

Manage Amazon API Gateway에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1351)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
apigateway-general	`arn:${Partition}:apigateway:${Region}::${ApiGatewayResourcePath}`	aws:ResourceTag/${TagKey} (p. 1353)

Manage Amazon API Gateway에 사용되는 조건 키

Manage Amazon API Gateway는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}		문자열
aws:ResourceTag/${TagKey}		문자열
aws:TagKeys		문자열

AWS Managed Apache Cassandra Service에 사용되는 작업, 리소스 및 조건 키

AWS Managed Apache Cassandra Service(서비스 접두사: `cassandra`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS Managed Apache Cassandra Service에서 정의한 작업 (p. 1354)
- AWS Managed Apache Cassandra Service에서 정의한 리소스 유형 (p. 1354)
- AWS Managed Apache Cassandra Service의 조건 키 (p. 1355)

AWS Managed Apache Cassandra Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Alter	키스페이스 또는 테이블을 변경할 수 있는 권한을 부여합니다.	쓰기	keyspace (p. 1355)		
			table (p. 1355)		
Create	키스페이스 또는 테이블을 생성할 수 있는 권한을 부여합니다.	쓰기	keyspace (p. 1355)		
			table (p. 1355)		
Drop	키스페이스 또는 테이블을 삭제할 수 있는 권한을 부여합니다.	쓰기	keyspace (p. 1355)		
			table (p. 1355)		
Modify	테이블에서 데이터를 삽입, 업데이트 또는 삭제할 수 있는 권한을 부여합니다.	쓰기	table* (p. 1355)		
Select	테이블에서 데이터를 선택할 수 있는 권한을 부여합니다.	Read	table* (p. 1355)		

AWS Managed Apache Cassandra Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1354)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니

다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
keyspace	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/`	
table	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${tableName}`	

AWS Managed Apache Cassandra Service의 조건 키

MCS에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Managed Blockchain에 사용되는 작업, 리소스 및 조건 키

Amazon Managed Blockchain(서비스 접두사: `managedblockchain`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Managed Blockchain에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateMember	Amazon Managed Blockchain 네트워크의 멤버를 생성할 수 있는 권한을 부여합니다.	쓰기	network* (p. 1357)		
CreateNetwork	Amazon Managed Blockchain 네트워크를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateNode	Amazon Managed Blockchain 네트워크의 멤버 내 노드를 생성할 수 있는 권한을 부여합니다.	쓰기	member* (p. 1357)		
CreateProposal	다른 블록체인 네트워크 멤버가 투표할 수 있도록 Amazon Managed Blockchain 네트워크에서 멤버를 추가 또는 제거하는 제안을 생성할 수 있는 권한을 부여합니다.	쓰기	network* (p. 1357)		
DeleteMember	Amazon Managed Blockchain 네트워크에서 멤버 및 모든 연결된 리소스를 삭제할 수 있는 권한을 부여합니다.	쓰기	member* (p. 1357)		
DeleteNode	Amazon Managed Blockchain 네트워크의 멤버에서 노드를 삭제할 수 있는 권한을 부여합니다.	쓰기	node* (p. 1357)		
GetMember	Amazon Managed Blockchain 네트워크의 멤버에 대한 세부 정보를 반환할 수 있는 권한을 부여합니다.	Read	member* (p. 1357)		
GetNetwork	Amazon Managed Blockchain 네트워크에 대한 세부 정보를 반환할 수 있는 권한을 부여합니다.	Read	network* (p. 1357)		
GetNode	Amazon Managed Blockchain 네트워크의 멤버 내 노드에 대한 세부 정보를 반환할 수 있는 권한을 부여합니다.	Read	node* (p. 1357)		
GetProposal	Amazon Managed Blockchain 네트워크의 제안에 대한 세부 정보를 반환할 수 있는 권한을 부여합니다.	Read	proposal* (p. 1357)		
ListInvitations	모든 Managed Blockchain 네트워크에서 활성 AWS 계정으로 보낸 초대를 나열할 수 있는 권한을 부여합니다.	List			
ListMembers	Amazon Managed Blockchain 네트워크의 멤버 및 해당 멤버십의 속성을 나열할 수 있는 권한을 부여합니다.	List	network* (p. 1357)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListNetworks	현재 AWS 계정이 멤버를 갖는 Amazon Managed Blockchain 네트워크에 대한 정보를 반환할 수 있는 권한을 부여합니다.	List			
ListNodes	Amazon Managed Blockchain 네트워크의 멤버 내 노드를 나열할 수 있는 권한을 부여합니다.	List	member* (p. 1357)		
ListProposalVotes	제안에 대한 모든 투표를 나열할 수 있는 권한을 부여합니다(투표 값, 지정된 Amazon Managed Blockchain 네트워크에 대해 투표할 수 있는 멤버의 고유 식별자 등).	List	proposal* (p. 1357)		
ListProposals	지정된 Amazon Managed Blockchain 네트워크에 대한 제안을 나열할 수 있는 권한을 부여합니다.	List	network* (p. 1357)		
RejectInvitation	블록체인 네트워크에 가입하라는 초대를 거부할 수 있는 권한을 부여합니다.	쓰기	invitation* (p. 1357)		
VoteOnProposal	지정된 블록체인 네트워크 멤버를 대신하여 제안에 투표할 수 있는 권한을 부여합니다.	쓰기	proposal* (p. 1357)		

Amazon Managed Blockchain에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1355)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
network	`arn:${Partition}:managedblockchain:${Region}::networks/${NetworkId}`	
member	`arn:${Partition}:managedblockchain:${Region}:${Account}:members/${MemberId}`	
node	`arn:${Partition}:managedblockchain:${Region}:${Account}:nodes/${NodeId}`	
proposal	`arn:${Partition}:managedblockchain:${Region}::proposals/${ProposalId}`	
invitation	`arn:${Partition}:managedblockchain:${Region}:${Account}:invitations/${InvitationId}`	

Amazon Managed Blockchain에 사용되는 조건 키

Managed Blockchain에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Managed Streaming for Kafka에 사용되는 작업, 리소스 및 조건 키

Amazon Managed Streaming for Kafka(서비스 접두사: `kafka`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

Amazon Managed Streaming for Kafka에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCluster	클러스터를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1360) aws:TagKeys (p. 1360)	ec2:DescribeSecurityGrou ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedI iam:PutRolePolicy kms:CreateGrant kms:DescribeKey

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateConfiguration	구성을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteCluster	클러스터를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DescribeCluster	클러스터를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeClusterOperation	ARN으로 지정된 클러스터 작업에 대한 설명을 반환합니다.	Read			
DescribeConfiguration	구성을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeConfigurationRevision	구성 개정을 설명할 수 있는 권한을 부여합니다.	Read			
GetBootstrapBrokers	클러스터의 브로커 노드에 대한 연결 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
ListClusterOperations	지정된 MSK 클러스터에서 수행된 모든 작업의 목록을 반환합니다.	Read			
ListClusters	현재 계정에 있는 모든 클러스터의 목록을 반환할 수 있는 권한을 부여합니다.	List			
ListConfigurations	현재 계정 내 모든 구성의 목록을 반환할 수 있는 권한을 부여합니다.	List			
ListNodes	클러스터의 노드 목록을 반환할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	MSK 리소스의 태그를 나열할 수 있는 권한을 부여합니다.	Read	cluster (p. 1360)		
TagResource	MSK 리소스에 태그를 지정할 수 있는 권한을 부여합니다.	태그 지정	cluster (p. 1360)		
				aws:RequestTag/${TagKey} (p. 1360) aws:TagKeys (p. 1360)	
UntagResource	MSK 리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	cluster (p. 1360)		
				aws:TagKeys (p. 1360)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateBrokerStorage	클러스터의 브로커 노드의 스토리지 크기를 업데이트합니다.	쓰기			
UpdateClusterConfiguration	클러스터에서 실행 중인 Kafka 구성을 업데이트합니다.	쓰기			

Amazon Managed Streaming for Kafka에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1358)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${UUID}`	aws:ResourceTag/${TagKey} (p. 1360)

Amazon Managed Streaming for Kafka에서 사용되는 조건 키

Amazon Managed Streaming for Kafka는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	MSK 리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그 키가 있는지 여부를 기준으로 요청을 필터링합니다.	문자열

AWS Marketplace에 사용되는 작업, 리소스 및 조건 키

AWS Marketplace(서비스 접두사: `aws-marketplace`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Marketplace에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptAgreementApprovalRequest	사용자가 수신 구독 요청을 승인할 수 있습니다(구독 확인이 필요한 제품을 제공하는 공급자의 경우).	쓰기			
CancelAgreementRequest	사용자가 구독 확인이 필요한 제품에 대해 보류 중인 구독 요청을 취소할 수 있습니다.	쓰기			
GetAgreementApprovalRequest	사용자가 수신 구독 요청의 세부 정보를 볼 수 있도록 허용합니다(구독 확인이 필요한 제품을 제공하는 공급자의 경우).	Read			
GetAgreementRequest	사용자가 구독 확인이 필요한 데이터 제품에 대한 구독 요청의 세부 정보를 볼 수 있습니다.	Read			
ListAgreementApprovalRequests	사용자가 수신 구독 요청을 나열할 수 있습니다(구독 확인이 필요한 제품을 제공하는 공급자의 경우).	List			
ListAgreementRequests	사용자가 구독 확인이 필요한 제품에 대한 구독 요청을 나열할 수 있습니다.	List			
RejectAgreementApprovalRequest	사용자가 수신 구독 요청을 거부할 수 있습니다(구독 확인이 필요한 제품을 제공하는 공급자의 경우).	쓰기			
Subscribe	사용자가 AWS Marketplace 제품을 구독할 수 있습니다. 구독 확인	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	이 필요한 제품에 대한 구독 요청을 보낼 수 있는 기능이 포함되어 있습니다. 기존 구독에 대해 자동 갱신을 활성화하는 기능이 포함되어 있습니다.				
Unsubscribe	사용자가 AWS Marketplace 제품에 대한 구독을 제거할 수 있습니다. 기존 구독에 대한 자동 갱신을 비활성화하는 기능이 포함되어 있습니다.	쓰기			
UpdateAgreementApprovalRequest	사용자가 잠재 구독자의 정보를 수정하는 기능을 포함하여 수신 구독 요청을 변경할 수 있습니다(구독 확인이 필요한 제품을 제공하는 공급자의 경우).	쓰기			
ViewSubscriptions	사용자가 계정의 구독을 볼 수 있습니다.	List			

AWS Marketplace에서 정의한 리소스 유형

AWS Marketplace는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Marketplace에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Marketplace의 조건 키

Marketplace에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Marketplace Catalog에 사용되는 작업, 리소스 및 조건 키

AWS Marketplace Catalog(서비스 접두사: `aws-marketplace`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Marketplace Catalog에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelChangeSet	실행 중인 변경 세트를 취소합니다.	쓰기			
CompleteTask	기존 작업을 완료하고 관련 변경 사항에 내용을 제출합니다.	쓰기			
DescribeChangeSet	기존 변경 세트의 세부 정보를 반환합니다.	Read			
DescribeEntity	기존 엔터티의 세부 정보를 반환합니다.	Read			
DescribeTask	기존 작업의 세부 정보를 반환합니다.	Read			
ListChangeSets	기존 변경 세트를 나열합니다.	Read			
ListEntities	기존 엔터티를 나열합니다.	Read			
ListTasks	기존 작업을 나열합니다.	List			
StartChangeSet	새 변경 세트를 요청합니다.	쓰기		catalog:ChangeType (p. 1364)	
UpdateTask	기존 작업의 내용을 업데이트합니다.	쓰기			

AWS Marketplace Catalog에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1362)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Entity	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/${EntityType}/${ResourceId}`	

리소스 유형	ARN	조건 키
ChangeSet	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/ChangeSet/${ResourceId}`	

AWS Marketplace Catalog에 사용되는 조건 키

AWS Marketplace Catalog는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
catalog:ChangeType	StartChangeSet 요청에서 변경 유형을 확인할 수 있습니다.	문자열

AWS Marketplace Entitlement Service에 사용되는 작업, 리소스 및 조건 키

AWS Marketplace Entitlement Service(서비스 접두사: `aws-marketplace`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

주제

- AWS Marketplace Entitlement Service에서 정의한 작업 (p. 1364)
- AWS Marketplace Entitlement Service에서 정의한 리소스 유형 (p. 1365)
- AWS Marketplace Entitlement Service에 사용되는 조건 키 (p. 1365)

AWS Marketplace Entitlement Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetEntitlements	지정된 제품에 대한 권한 부여 값을 검색합니다. 결과는 고객 식별	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	자 또는 제품 치수를 기준으로 필터링할 수 있습니다.				

AWS Marketplace Entitlement Service에서 정의한 리소스 유형

AWS Marketplace Entitlement Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Marketplace Entitlement Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Marketplace Entitlement Service에 사용되는 조건 키

Marketplace Entitlement에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Marketplace Image Building Service에 사용되는 작업, 리소스 및 조건 키

AWS Marketplace Image Building Service(서비스 접두사: `aws-marketplace`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Marketplace Image Building Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeBuilds [권한만 해당]	빌드 ID로 식별되는 이미지 빌드를 설명합니다.	Read			
ListBuilds [권한만 해당]	이미지 빌드를 나열합니다.	Read			
StartBuild [권한만 해당]	이미지 빌드를 시작합니다.	쓰기			

AWS Marketplace Image Building Service에서 정의한 리소스 유형

AWS Marketplace Image Building Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Marketplace Image Building Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Marketplace Image Building Service에 사용되는 조건 키

Marketplace Image Build에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Marketplace Management Portal에 사용되는 작업, 리소스 및 조건 키

AWS Marketplace Management Portal(서비스 접두사: `aws-marketplace-management`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Marketplace Management Portal에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
uploadFiles	사용자가 AWS Marketplace Management Portal에 있는 File Upload 페이지에 액세스하도록 허용합니다.	쓰기			
viewMarketing	사용자가 AWS Marketplace Management Portal에 있는 Marketing 페이지에 액세스하도록 허용합니다.	List			
viewReports	사용자가 AWS Marketplace Management Portal에 있는 Reports 페이지에 액세스하도록 허용합니다.	List			
viewSettings	사용자가 AWS Marketplace Management Portal에 있는 설정 페이지에 액세스하도록 허용합니다.	List			
viewSupport	사용자가 AWS Marketplace Management Portal에 있는 Customer Support Eligibility 페이지에 액세스하도록 허용합니다.	List			

AWS Marketplace Management Portal에서 정의한 리소스 유형

AWS Marketplace Management Portal은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Marketplace Management Portal에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Marketplace Management Portal에 사용되는 조건 키

Marketplace Portal에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Marketplace Metering Service에 사용되는 작업, 리소스 및 조건 키

AWS Marketplace Metering Service(서비스 접두사: `aws-marketplace`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Marketplace Metering Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchMeterUsage	AWS Marketplace에 나열된 SaaS 애플리케이션에서 호출되어 일련의 고객에 대한 측정 레코드를 게시합니다.	쓰기			
MeterUsage	측정 레코드를 방출합니다.	쓰기			
RegisterUsage	유료 소프트웨어를 실행하는 고객이 AWS Marketplace에서 제품을 구독하고 있는지 확인할 수 있으며, 이를 통해 무단 사용을 방지할 수도 있습니다. ECS 작업마다 시간당 소프트웨어 사용을 측정하며, 이때 사용량은 초 단위로 비례 할당되어 계산됩니다.	쓰기			
ResolveCustomer	등록 토큰을 확인하여 고객 식별자 및 제품 코드를 가져옵니다.	쓰기			

AWS Marketplace Metering Service에서 정의한 리소스 유형

AWS Marketplace Metering Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Marketplace Metering Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Marketplace Metering Service의 조건 키

Marketplace Metering에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Marketplace Procurement Systems Integration에 사용되는 작업, 리소스 및 조건 키

AWS Marketplace Procurement Systems Integration(서비스 접두사: `aws-marketplace`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Marketplace Procurement Systems Integration에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeProcurementSystemConfiguration [권한만 해당]	개별 계정 또는 전체 AWS Organization(있을 경우)에 대한 Procurement System integration 구성(예: Coupa)을 설명합니다. 이 작업은 AWS Organization을 사용하는 경우에만 마스터 계정이 수행합니다.	Read			
PutProcurementSystemConfiguration [권한만 해당]	개별 계정 또는 전체 AWS Organization(있을 경우)에 대한 Procurement System integration 구성(예: Coupa)을 생성하거나 업데이트합니다. 이 작업은 AWS Organization을 사용하는 경우에만 마스터 계정이 수행합니다.	쓰기			

AWS Marketplace Procurement Systems Integration에서 정의한 리소스 유형

AWS Marketplace Procurement Systems Integration은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Marketplace Procurement Systems Integration에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Marketplace Procurement Systems Integration에 사용되는 조건 키

Marketplace Procurement Integration에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Mechanical Turk에 사용되는 작업, 리소스 및 조건 키

Amazon Mechanical Turk(서비스 접두사: `mechanicalturk`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Mechanical Turk에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptQualificationRequest	AcceptQualificationRequest 작업은 자격에 대한 작업자의 요청을 허용합니다.	쓰기			
ApproveAssignment	ApproveAssignment 작업은 완료된 배정의 결과를 승인합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateQualificationWithWorker	AssociateQualificationWithWorker 작업은 작업자에게 자격을 부여합니다.	쓰기			
CreateAdditionalAssignmentsForHIT	CreateAdditionalAssignmentsForHIT 작업은 기존 HIT의 최대 배정 수를 늘립니다.	쓰기			
CreateHIT	CreateHIT 작업은 새로운 HIT(인간 지능 작업)를 생성합니다.	쓰기			
CreateHITType	CreateHITType 작업은 새 HIT 유형을 생성합니다.	쓰기			
CreateHITWithHITType	CreateHITWithHITType 작업은 CreateHITType 작업에 의해 생성된 기존 HITTypeID를 사용하여 새로운 HIT(인간 지능 작업)를 생성합니다.	쓰기			
CreateQualificationType	CreateQualificationType 작업은 QualificationType 데이터 구조에 의해 표현되는 새로운 자격 유형을 생성합니다.	쓰기			
CreateWorkerBlock	CreateWorkerBlock 작업은 작업자가 HIT에서 작업을 못하게 할 수 있습니다.	쓰기			
DeleteHIT	DeleteHIT 작업은 더 이상 필요하지 않은 HIT를 폐기합니다.	쓰기			
DeleteQualificationType	DeleteQualificationType 작업은 자격 유형을 폐기하고 해당 자격 유형과 연결된 모든 HIT 유형을 폐기합니다.	쓰기			
DeleteWorkerBlock	DeleteWorkerBlock 작업은 HIT에서 작업이 차단된 작업자를 복구시킵니다.	쓰기			
DisassociateQualificationFromWorker	DisassociateQualificationFromWorker 작업은 사용자에게 이전에 부여된 자격을 취소합니다.	쓰기			
GetAccountBalance	GetAccountBalance 작업은 Amazon Mechanical Turk 계정에서 금액을 검색합니다.	Read			
GetAssignment	GetAssignment는 배정의 ID를 사용하여 AssignmentStatus 값(Submitted(제출), Approved(승인) 또는 Rejected(거부))을 가진 배정을 검색합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetFileUploadURL	GetFileUploadURL 작업은 임시 URL을 생성하고 반환합니다.	Read			
GetHIT	GetHIT 작업은 지정된 HIT에 관한 세부 정보를 검색합니다.	Read			
GetQualificationScore	GetQualificationScore 작업은 주어진 자격 유형을 위한 작업자의 자격 값을 반환합니다.	Read			
GetQualificationType	GetQualificationType 작업은 ID를 사용하여 자격 유형에 대한 정보를 검색합니다.	Read			
ListAssignmentsForHIT	ListAssignmentsForHIT 작업은 HIT에 대해 완료된 배정을 검색합니다.	List			
ListBonusPayments	ListBonusPayments 작업은 주어진 HIT 또는 배정에 대해 작업자에게 지불한 보상 금액을 검색합니다.	List			
ListHITs	ListHITs 작업은 요청자의 HIT를 모두 반환합니다.	List			
ListHITsForQualificationType	ListHITsForQualificationType 작업은 QualificationRequirement에 대해 지정된 QualififcationType을 사용하는 HIT를 반환합니다.	List			
ListQualificationRequests	ListQualificationRequests 작업은 특정 자격 유형의 자격에 대한 요청을 검색합니다.	List			
ListQualificationTypes	ListQualificationTypes 작업은 지정된 검색 쿼리를 사용하여 자격 유형을 검색하고 자격 유형의 목록을 반환합니다.	List			
ListReviewPolicyResultsForHIT	ListReviewPolicyResultsForHIT 작업은 CreateHIT 작업 동안 검토 정책을 실행하는 중에 취해진 작업 및 계산된 결과를 검색합니다.	List			
ListReviewableHITs	ListReviewableHITs 작업은 승인 또는 거부되지 않은 요청자의 모든 HIT를 반환합니다.	List			
ListWorkerBlocks	ListWorkersBlocks 작업은 HIT에서의 작업이 차단된 작업자의 목록을 검색합니다.	List			
ListWorkersWithQualificationType	ListWorkersWithQualificationType 작업은 지정된 자격 유형을 가진 모든 작업자를 반환합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
NotifyWorkers	NotifyWorkers 작업은 Worker ID로 지정하는 한 명 이상의 작업자에게 이메일을 보냅니다.	쓰기			
RejectAssignment	RejectAssignment 작업은 완료된 배정의 결과를 거부합니다.	쓰기			
RejectQualificationRequest	RejectQualificationRequest 작업은 자격에 대한 사용자의 요청을 거부합니다.	쓰기			
SendBonus	SendBonus 작업은 계정으로부터 금액의 결제를 작업자에게 발급합니다.	쓰기			
SendTestEventNotification	SendTestEventNotification 작업은 대신 제공된 알림 지정에 따라 HIT 이벤트가 발생한 것처럼, Amazon Mechanical Turk가 알림 메시지를 보내도록 합니다.	쓰기			
UpdateExpirationForHIT	UpdateExpirationForHIT 작업을 사용하면 HIT의 만료 시간을 현재 만료 이상으로 연장하거나 HIT를 즉시 만료할 수 있습니다.	쓰기			
UpdateHITReviewStatus	UpdateHITReviewStatus 작업은 HIT의 상태를 토글합니다.	쓰기			
UpdateHITTypeOfHIT	UpdateHITTypeOfHIT 작업을 통해 HIT의 HITType 속성을 변경할 수 있습니다.	쓰기			
UpdateNotificationSettings	UpdateNotificationSettings 작업은 HIT 유형에 대한 알림을 생성, 업데이트, 비활성화 또는 재활성화합니다.	쓰기			
UpdateQualificationType	UpdateQualificationType 작업은 QualificationType 데이터 구조로 표현되는 기존 자격 유형의 속성을 수정합니다.	쓰기			

Amazon Mechanical Turk에서 정의한 리소스 유형

Amazon Mechanical Turk는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Mechanical Turk에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Mechanical Turk에 사용되는 조건 키

MechanicalTurk에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Message Delivery Service에 사용되는 작업, 리소스 및 조건 키

Amazon Message Delivery Service(서비스 접두사: `ec2messages`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

주제

Amazon Message Delivery Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcknowledgeMessage	메시지가 다시 전달되지 않도록 메시지를 확인합니다.	쓰기			
DeleteMessage	메시지를 삭제합니다.	쓰기			
FailMessage	메시지 전송을 실패하게 하여(메시지를 성공적으로 처리할 수 없음을 의미함), 회신하거나 다시 전달할 수 없게 합니다.	쓰기			
GetEndpoint	트래픽을 메시지에 대하여 주어진 목적지를 기반으로 정확한 엔드포인트로 라우팅합니다.	Read			
GetMessages	긴 폴링을 사용하여 메시지를 클라이언트/인스턴스에 전달합니다.	Read			
SendReply	답변을 클라이언트/인스턴스에서 업스트림 서비스로 전송합니다.	쓰기			

Amazon Message Delivery Service에서 정의한 리소스 유형

Amazon 메시지 전송 서비스는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon 메시지 전송 서비스에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Message Delivery Service에 사용되는 조건 키

EC2 Messages에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Migration Hub에 사용되는 작업, 리소스 및 조건 키

AWS Migration Hub(서비스 접두사: `mgh`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Migration Hub에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateCreatedArtifact	MigrationTask에 지정된 AWS 결과물 연결	쓰기	migrationTask* (p. 1377)		
AssociateDiscoveredResource	MigrationTask에 지정된 ADS 리소스 연결	쓰기	migrationTask* (p. 1377)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateHomeRegionControl	Migration Hub 홈 리전 제어 생성	쓰기			
CreateProgressUpdateStream	ProgressUpdateStream 생성	쓰기	progressUpdateStream* (p. 1377)		
DeleteProgressUpdateStream	ProgressUpdateStream 삭제	쓰기	progressUpdateStream* (p. 1377)		
DescribeApplicationState	Application Discovery Service 애플리케이션의 상태 가져오기	Read			
DescribeHomeRegionControls	홈 리전 제어 나열	List			
DescribeMigrationTask	MigrationTask 설명	Read	migrationTask* (p. 1377)		
DisassociateCreatedArtifact	MigrationTask에서 지정된 AWS 결과물 연결 해제	쓰기	migrationTask* (p. 1377)		
DisassociateDiscoveredResource	MigrationTask에서 지정된 ADS 리소스 연결 해제	쓰기	migrationTask* (p. 1377)		
GetHomeRegion	Migration Hub 홈 리전 가져오기	Read			
ImportMigrationTask	MigrationTask 가져오기	쓰기	migrationTask* (p. 1377)		
ListCreatedArtifacts	MigrationTask에 대해 연결된 생성 결과물 나열	List	migrationTask* (p. 1377)		
ListDiscoveredResources	MigrationTask에서 연결된 ADS 리소스 나열	List	migrationTask* (p. 1377)		
ListMigrationTasks	MigrationTasks 나열	List			
ListProgressUpdateStreams	ProgressUpdateStreams 나열	List			
NotifyApplicationState	Application Discovery Service 애플리케이션의 상태 업데이트	쓰기			
NotifyMigrationTaskState	최신 MigrationTask 상태 알림	쓰기	migrationTask* (p. 1377)		
PutResourceAttributes	ResourceAttributes 적용	쓰기	migrationTask* (p. 1377)		

AWS Migration Hub에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1375)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유

형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
progressUpdateStream	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}`	
migrationTask	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}/migrationTask/${Task}`	

AWS Migration Hub의 조건 키

Migration Hub에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Mobile Analytics에 사용되는 작업, 리소스 및 조건 키

Amazon Mobile Analytics(서비스 접두사: `mobileanalytics`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Mobile Analytics에서 정의한 작업 (p. 1377)
- Amazon Mobile Analytics에서 정의한 리소스 유형 (p. 1378)
- Amazon Mobile Analytics의 조건 키 (p. 1378)

Amazon Mobile Analytics에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetFinancialReports	앱의 재무 지표에 대한 액세스 권한 부여	Read			
GetReports	앱의 표준 지표에 대한 액세스 권한 부여	Read			
PutEvents	PutEvents 작업은 하나 이상의 이벤트를 기록합니다	쓰기			

Amazon Mobile Analytics에서 정의한 리소스 유형

Amazon Mobile Analytics는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Mobile Analytics에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Mobile Analytics의 조건 키

Mobile Analytics에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Mobile Hub에 사용되는 작업, 리소스 및 조건 키

AWS Mobile Hub(서비스 접두사: `mobilehub`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Mobile Hub에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateProject	프로젝트 생성	쓰기			
CreateServiceRole	필요한 서비스 역할을 만들어 계정에서 AWS Mobile Hub를 활성화합니다.	쓰기			
DeleteProject	지정된 프로젝트를 삭제합니다.	쓰기	project* (p. 1380)		
DeleteProjectSnapshot	프로젝트 구성의 저장된 스냅샷을 삭제합니다.	쓰기			
DeployToStage	변경 사항을 지정된 단계에 배포합니다.	쓰기			
DescribeBundle	다운로드 번들을 설명합니다.	Read			
ExportBundle	다운로드 번들을 내보냅니다.	Read			
ExportProject	프로젝트 구성을 내보냅니다.	Read	project* (p. 1380)		
GenerateProjectParameters	코드 생성에 필요한 프로젝트 파라미터를 생성합니다.	쓰기	project* (p. 1380)		
GetProject	프로젝트 구성 및 리소스를 가져옵니다.	Read	project* (p. 1380)		
GetProjectSnapshot	이전에 내보낸 프로젝트 구성 스냅샷을 가져옵니다.	Read			
ImportProject	이전에 내보낸 프로젝트 구성에서 프로젝트를 새로 만듭니다.	쓰기			
InstallBundle	프로젝트 배포 S3 버킷에 번들을 설치합니다.	쓰기			
ListAvailableConnectors	사용 가능한 SaaS(Software as a Service) 커넥터를 나열합니다.	List			
ListAvailableFeatures	사용 가능한 기능을 나열합니다.	List			
ListAvailableRegions	프로젝트에 사용 가능한 리전을 나열합니다.	List			
ListBundles	사용 가능한 다운로드 번들을 나열합니다.	List			
ListProjectSnapshots	프로젝트 구성의 저장된 스냅샷을 나열합니다.	List			
ListProjects	프로젝트를 나열합니다.	List			
SynchronizeProject	리소스의 상태를 프로젝트에 동기화합니다.	쓰기	project* (p. 1380)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateProject	프로젝트 업데이트	쓰기	project* (p. 1380)		
ValidateProject	모바일 허브 프로젝트의 유효성을 검사합니다.	Read			
VerifyServiceRole	계정에서 AWS Mobile Hub가 활성화되어 있는지 확인합니다.	Read			

AWS Mobile Hub에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1378)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
project	`arn:${Partition}:mobilehub:${Region}:${Account}:project/${ProjectId}`	

AWS Mobile Hub에 사용되는 조건 키

Mobile Hub에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon MQ에 사용되는 작업, 리소스 및 조건 키

Amazon MQ(서비스 접두사: `mq`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

- Amazon MQ에서 정의한 작업 (p. 1380)
- Amazon MQ에서 정의한 리소스 유형 (p. 1382)
- Amazon MQ에 사용되는 조건 키 (p. 1383)

Amazon MQ에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시

됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateBroker	브로커를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1383) aws:TagKeys (p. 1383)	
CreateConfiguration	지정된 구성 이름에 대한 새 구성을 생성할 수 있는 권한을 부여합니다. Amazon MQ는 기본 구성(엔진 유형 및 엔진 버전)을 사용합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1383) aws:TagKeys (p. 1383)	
CreateTags	태그를 생성할 수 있는 권한을 부여합니다.	쓰기	brokers (p. 1383)		
			configurations (p. 1383)		
				aws:RequestTag/${TagKey} (p. 1383) aws:TagKeys (p. 1383)	
CreateUser	ActiveMQ 사용자를 생성할 수 있는 권한을 부여합니다.	쓰기	brokers* (p. 1383)		
DeleteBroker	브로커를 삭제할 수 있는 권한을 부여합니다.	쓰기	brokers* (p. 1383)		
DeleteTags	태그를 삭제할 수 있는 권한을 부여합니다.	쓰기	brokers (p. 1383)		
			configurations (p. 1383)		
				aws:TagKeys (p. 1383)	
DeleteUser	ActiveMQ 사용자를 삭제할 수 있는 권한을 부여합니다.	쓰기	brokers* (p. 1383)		
DescribeBroker	지정된 브로커에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read	brokers* (p. 1383)		
DescribeBrokerEngineTypes	브로커 엔진에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeBrokerInstanceOptions	브로커 인스턴스 옵션에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read			
DescribeConfiguration	지정된 구성에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read	configurations* (p. 1383)		
DescribeConfigurationRevision	지정된 구성에 대한 지정된 구성 개정을 반환할 수 있는 권한을 부여합니다.	Read	configurations* (p. 1383)		
DescribeUser	ActiveMQ 사용자에 대한 정보를 반환할 수 있는 권한을 부여합니다.	Read	brokers* (p. 1383)		
ListBrokers	모든 브로커의 목록을 반환할 수 있는 권한을 부여합니다.	List			
ListConfigurationRevisions	지정된 구성에 대한 모든 기존 개정 목록을 반환할 수 있는 권한을 부여합니다.	List	configurations* (p. 1383)		
ListConfigurations	모든 구성의 목록을 반환할 수 있는 권한을 부여합니다.	List			
ListTags	태그 목록을 반환할 수 있는 권한을 부여합니다.	List	brokers (p. 1383)		
			configurations (p. 1383)		
ListUsers	모든 ActiveMQ 사용자의 목록을 반환할 수 있는 권한을 부여합니다.	List	brokers* (p. 1383)		
RebootBroker	브로커를 재부팅할 수 있는 권한을 부여합니다.	쓰기	brokers* (p. 1383)		
UpdateBroker	브로커에 대기 중인 구성 변경을 추가할 수 있는 권한을 부여합니다.	쓰기	brokers* (p. 1383)		
UpdateConfiguration	지정된 구성을 업데이트할 수 있는 권한을 부여합니다.	쓰기	configurations* (p. 1383)		
UpdateUser	ActiveMQ 사용자에 대한 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기	brokers* (p. 1383)		

Amazon MQ에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1380)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
brokers	`arn:${Partition}:mq:${Region}:${Account}:broker:${broker-id}`	aws:ResourceTag/${TagKey} (p. 1383)
configurations	`arn:${Partition}:mq:${Region}:${Account}:configuration:${configuration-id}`	aws:ResourceTag/${TagKey} (p. 1383)

Amazon MQ에 사용되는 조건 키

Amazon MQ는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}		문자열
aws:ResourceTag/${TagKey}		문자열
aws:TagKeys		문자열

Amazon Neptune에 사용되는 작업, 리소스 및 조건 키

Amazon Neptune(서비스 접두사: `neptune-db`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Neptune에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있

으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
connect	데이터베이스에 연결	쓰기	database* (p. 1384)		

Amazon Neptune에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1383)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
database	`arn:${Partition}:neptune-db:${Region}:${Account}:${RelativeId}/database`	

Amazon Neptune에 사용되는 조건 키

Neptune에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Network Manager에 사용되는 작업, 리소스 및 조건 키

Network Manager(서비스 접두사: `networkmanager`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Network Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateCustomerGateway	고객 게이트웨이를 디바이스에 연결할 수 있는 권한을 부여합니다.	쓰기	device* (p. 1389)		
			global-network* (p. 1389)		
			link (p. 1389)		
				networkmanager:cgwArn (p. 1390)	
AssociateLink	링크를 디바이스에 연결할 수 있는 권한을 부여합니다.	쓰기	device* (p. 1389)		
			global-network* (p. 1389)		
			link* (p. 1389)		
CreateDevice	새 역할을 생성할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
				aws:RequestTag/${TagKey} (p. 1390) aws:TagKeys (p. 1390)	
CreateGlobalNetwork	새 글로벌 네트워크를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1390) aws:TagKeys (p. 1390)	iam:CreateServiceLinkedI
CreateLink	새 링크를 생성할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
			site (p. 1389)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1390) aws:TagKeys (p. 1390)	
CreateSite	새 사이트를 생성할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
				aws:RequestTag/${TagKey} (p. 1390) aws:TagKeys (p. 1390)	
DeleteDevice	디바이스를 삭제할 수 있는 권한을 부여합니다.	쓰기	device* (p. 1389)		
			global-network* (p. 1389)		
DeleteGlobalNetwork	글로벌 네트워크를 삭제할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
DeleteLink	링크를 삭제할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
			link* (p. 1389)		
DeleteSite	사이트를 삭제할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
			site* (p. 1389)		
DeregisterTransitGateway	글로벌 네트워크에서 전송 게이트웨이 등록을 취소할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
				networkmanager:tgwArn (p. 1390)	
DescribeGlobalNetworks	글로벌 네트워크를 설명할 수 있는 권한을 부여합니다.	List	global-network (p. 1389)		
DisassociateCustomerGateway	디바이스에서 고객 게이트웨이의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				networkmanager:cgwArn (p. 1390)	
DisassociateLink	디바이스에서 링크의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기	device* (p. 1389)		
			global-network* (p. 1389)		
			link* (p. 1389)		
GetCustomerGatewayAssociations	고객 게이트웨이 연결을 설명할 수 있는 권한을 부여합니다.	List	global-network* (p. 1389)		
GetDevices	디바이스를 설명할 수 있는 권한을 부여합니다.	List	global-network* (p. 1389)		
			device (p. 1389)		
GetLinkAssociations	링크 연결을 설명할 수 있는 권한을 부여합니다.	List	global-network* (p. 1389)		
			device (p. 1389)		
			link (p. 1389)		
GetLinks	링크를 설명할 수 있는 권한을 부여합니다.	List	global-network* (p. 1389)		
			link (p. 1389)		
GetSites	글로벌 네트워크를 설명할 수 있는 권한을 부여합니다.	List	global-network* (p. 1389)		
			site (p. 1389)		
GetTransitGatewayRegistrations	전송 게이트웨이 등록을 설명할 수 있는 권한을 부여합니다.	List	global-network* (p. 1389)		
ListTagsForResource	Network Manager 리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	device (p. 1389)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			global-network (p. 1389)		
			link (p. 1389)		
			site (p. 1389)		
				aws:ResourceTag/${TagKey} (p. 1390)	
RegisterTransitGateway	글로벌 네트워크에 전송 게이트웨이를 등록할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
				networkmanager:tgwArn (p. 1390)	
TagResource	Network Manager 리소스에 태그를 지정할 수 있는 권한을 부여합니다.	태그 지정	device (p. 1389)		
			global-network (p. 1389)		
			link (p. 1389)		
			site (p. 1389)		
				aws:TagKeys (p. 1390) aws:RequestTag/${TagKey} (p. 1390) aws:ResourceTag/${TagKey} (p. 1390)	
UntagResource	Network Manager 리소스의 태그를 해제할 수 있는 권한을 부여합니다.	태그 지정	device (p. 1389)		
			global-network (p. 1389)		
			link (p. 1389)		
			site (p. 1389)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1390)	
UpdateDevice	디바이스를 업데이트할 수 있는 권한을 부여합니다.	쓰기	device* (p. 1389)		
			global-network* (p. 1389)		
UpdateGlobalNetwork	글로벌 네트워크를 업데이트할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
UpdateLink	링크를 업데이트할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
			link* (p. 1389)		
UpdateSite	사이트를 업데이트할 수 있는 권한을 부여합니다.	쓰기	global-network* (p. 1389)		
			site* (p. 1389)		

Network Manager에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1384)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
global-network	`arn:${Partition}:networkmanager::${Account}:global-network/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1390)
site	`arn:${Partition}:networkmanager::${Account}:site/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1390)
link	`arn:${Partition}:networkmanager::${Account}:link/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1390)
device	`arn:${Partition}:networkmanager::${Account}:device/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1390)

Network Manager용 조건 키

Network Manager는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
networkmanager:cgwArn	연결 또는 연결 해제할 수 있는 고객 게이트웨이를 제어합니다.	문자열
networkmanager:tgwArn	등록 또는 등록 해제할 수 있는 전송 게이트웨이를 제어합니다.	문자열

AWS OpsWorks에 사용되는 작업, 리소스 및 조건 키

AWS OpsWorks(서비스 접두사: `opsworks`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS OpsWorks에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssignInstance	등록된 인스턴스를 계층에 할당합니다.	쓰기	stack (p. 1395)		
AssignVolume	스택의 등록된 Amazon EBS 볼륨 중 하나를 지정된 인스턴스에 할당합니다.	쓰기	stack (p. 1395)		
AssociateElasticIp	스택의 등록된 탄력적 IP 주소 중 하나를 지정된 인스턴스와 연결합니다.	쓰기	stack (p. 1395)		
AttachElasticLoadBalancer	Elastic Load Balancing 로드 밸런서를 지정된 계층에 연결합니다.	쓰기	stack (p. 1395)		
CloneStack	지정된 스택의 복제를 만듭니다.	쓰기	stack (p. 1395)		
CreateApp	지정된 스택에 대한 앱을 만듭니다.	쓰기	stack (p. 1395)		
CreateDeployment	배포 또는 스택 명령을 실행합니다.	쓰기	stack (p. 1395)		
CreateInstance	지정된 스택에 인스턴스를 만듭니다.	쓰기	stack (p. 1395)		
CreateLayer	계층을 만듭니다.	쓰기	stack (p. 1395)		
CreateStack	새로운 스택을 만듭니다.	쓰기			
CreateUserProfile	새 사용자 프로필을 생성합니다.	쓰기			
DeleteApp	지정된 앱을 삭제합니다.	쓰기	stack (p. 1395)		
DeleteInstance	지정된 인스턴스를 삭제합니다(그러면 연결된 Amazon EC2 인스턴스가 종료됩니다).	쓰기	stack (p. 1395)		
DeleteLayer	지정된 계층을 삭제합니다.	쓰기	stack (p. 1395)		
DeleteStack	지정된 스택을 삭제합니다.	쓰기	stack (p. 1395)		
DeleteUserProfile	사용자 프로필을 삭제합니다.	쓰기			
DeregisterEcsCluster	사용자 프로필을 삭제합니다.	쓰기	stack (p. 1395)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeregisterElasticIp	지정된 탄력적 IP 주소를 등록 취소합니다.	쓰기	stack (p. 1395)		
DeregisterInstance	등록된 Amazon EC2 또는 온프레미스 인스턴스를 등록 취소합니다.	쓰기	stack (p. 1395)		
DeregisterRdsDbInstance	Amazon RDS 인스턴스를 등록 취소합니다.	쓰기	stack (p. 1395)		
DeregisterVolume	Amazon EBS 볼륨을 등록 취소합니다.	쓰기	stack (p. 1395)		
DescribeAgentVersions	사용 가능한 AWS OpsWorks 에이전트 버전을 설명합니다.	List	stack (p. 1395)		
DescribeApps	지정된 앱 집합의 설명을 요청합니다.	List	stack (p. 1395)		
DescribeCommands	지정된 명령의 결과를 설명합니다.	List	stack (p. 1395)		
DescribeDeployments	지정된 배포 집합의 설명을 요청합니다.	List	stack (p. 1395)		
DescribeEcsClusters	스택에 등록된 Describes Amazon ECS 클러스터를 설명합니다.	List	stack (p. 1395)		
DescribeElasticIps	탄력적 IP 주소를 설명합니다.	List	stack (p. 1395)		
DescribeElasticLoadBalancers	스택의 Elastic Load Balancing 인스턴스를 설명합니다.	List	stack (p. 1395)		
DescribeInstances	인스턴스 집합의 설명을 요청합니다.	List	stack (p. 1395)		
DescribeLayers	지정된 스택에서 하나 이상의 계층에 대한 설명을 요청합니다.	List	stack (p. 1395)		
DescribeLoadBasedAutoScaling	지정된 계층에 대한 로드 기반 Auto Scaling 구성을 설명합니다.	List	stack (p. 1395)		
DescribeMyUserProfile	사용자의 SSH 정보를 설명합니다.	List			
DescribePermissions	지정된 스택에 대한 권한을 설명합니다.	List	stack (p. 1395)		
DescribeRaidArrays	인스턴스의 RAID 어레이를 설명합니다.	List	stack (p. 1395)		
DescribeRdsDbInstances	Amazon RDS 인스턴스를 설명합니다.	List	stack (p. 1395)		
DescribeServiceErrors	AWS OpsWorks 서비스 오류를 설명합니다.	List	stack (p. 1395)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeStackProvisioningParameters	스택의 프로비저닝 파라미터의 설명을 요청합니다.	List	stack (p. 1395)		
DescribeStackSummary	지정된 스택에 계층 및 앱의 수, running_setup 또는 online과 같은 각 상태에서 인스턴스의 수를 설명합니다.	List	stack (p. 1395)		
DescribeStacks	하나 이상의 스택에 대한 설명을 요청합니다.	List	stack (p. 1395)		
DescribeTimeBasedAutoScaling	지정된 인스턴스에 대한 시간 기반 Auto Scaling 구성을 설명합니다.	List	stack (p. 1395)		
DescribeUserProfiles	지정된 사용자를 설명합니다.	List			
DescribeVolumes	인스턴스의 Amazon EBS 볼륨을 설명합니다.	List	stack (p. 1395)		
DetachElasticLoadBalancing	계층에서 지정된 Elastic Load Balancing 인스턴스를 분리합니다.	쓰기	stack (p. 1395)		
DisassociateElasticIp	인스턴스에서 탄력적 IP 주소를 연결 해제합니다.	쓰기	stack (p. 1395)		
GetHostnameSuggestion	현재 호스트 이름 주제에 기반하여 지정된 계층을 위해 생성된 호스트 이름을 가져옵니다.	Read	stack (p. 1395)		
GrantAccess	지정된 기간 동안 Windows 인스턴스에 대한 RDP 액세스를 허용합니다.	쓰기	stack (p. 1395)		
ListTags	지정된 스택 또는 계층에 적용되는 태그 목록을 반환합니다.	List	stack (p. 1395)		
RebootInstance	지정된 인스턴스를 재부팅합니다.	쓰기	stack (p. 1395)		
RegisterEcsCluster	지정된 Amazon ECS 클러스터를 스택에 등록합니다.	쓰기	stack (p. 1395)		
RegisterElasticIp	탄력적 IP 주소를 지정된 스택에 등록합니다.	쓰기	stack (p. 1395)		
RegisterInstance	AWS OpsWorks 외부에서 생성된 인스턴스를 지정된 스택에 등록합니다.	쓰기	stack (p. 1395)		
RegisterRdsDbInstance	Amazon RDS 인스턴스를 스택에 등록합니다.	쓰기	stack (p. 1395)		
RegisterVolume	Amazon EBS 볼륨을 지정된 스택에 등록합니다.	쓰기	stack (p. 1395)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SetLoadBasedAutoScaling	지정된 계층에 대한 로드 기반 Auto Scaling 구성을 지정합니다.	쓰기	stack (p. 1395)		
SetPermission	사용자의 권한을 지정합니다.	권한 관리	stack (p. 1395)		
SetTimeBasedAutoScaling	지정된 인스턴스에 대한 시간 기반 Auto Scaling 구성을 지정합니다.	쓰기	stack (p. 1395)		
StartInstance	지정된 인스턴스를 시작합니다.	쓰기	stack (p. 1395)		
StartStack	스택의 인스턴스를 시작합니다.	쓰기	stack (p. 1395)		
StopInstance	지정된 인스턴스를 중지합니다.	쓰기	stack (p. 1395)		
StopStack	지정된 스택을 중지합니다	쓰기	stack (p. 1395)		
TagResource	지정된 스택 또는 계층에 태그를 적용합니다.	쓰기	stack (p. 1395)		
UnassignInstance	모든 해당 계층에서 등록된 인스턴스를 할당 해제합니다.	쓰기	stack (p. 1395)		
UnassignVolume	할당된 Amazon EBS 볼륨을 할당 해제합니다.	쓰기	stack (p. 1395)		
UntagResource	지정된 스택 또는 계층에서 태그를 제거합니다.	쓰기	stack (p. 1395)		
UpdateApp	지정된 앱을 업데이트합니다.	쓰기	stack (p. 1395)		
UpdateElasticIp	등록된 탄력적 IP 주소의 이름을 업데이트합니다.	쓰기	stack (p. 1395)		
UpdateInstance	지정된 인스턴스를 업데이트합니다.	쓰기	stack (p. 1395)		
UpdateLayer	지정된 계층을 업데이트합니다.	쓰기	stack (p. 1395)		
UpdateMyUserProfile	사용자의 SSH 퍼블릭 키를 업데이트합니다.	쓰기			
UpdateRdsDbInstance	Amazon RDS 인스턴스를 업데이트합니다.	쓰기	stack (p. 1395)		
UpdateStack	지정된 스택을 업데이트합니다.	쓰기	stack (p. 1395)		
UpdateUserProfile	지정된 사용자 프로필을 업데이트합니다.	권한 관리			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateVolume	Amazon EBS 볼륨의 이름 또는 탑재 지점을 업데이트합니다.	쓰기	stack (p. 1395)		

AWS OpsWorks에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1390)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
stack	`arn:${Partition}:opsworks:${Region}:${Account}:stack/${StackId}/`	

AWS OpsWorks에 사용되는 조건 키

OpsWorks에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS OpsWorks Configuration Management에 사용되는 작업, 리소스 및 조건 키

AWS OpsWorks Configuration Management(서비스 접두사: `opsworks-cm`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS OpsWorks Configuration Management에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateNode	노드를 구성 관리 서버에 연결합니다.	쓰기			
CreateBackup	지정된 서버에 대한 백업을 생성합니다.	쓰기			
CreateServer	새 서버를 만듭니다.	쓰기			
DeleteBackup	지정된 백업 및 가능한 경우 해당 S3 버킷을 삭제합니다.	쓰기			
DeleteServer	지정된 서버와 그에 해당되는 CF 스택 및 가능한 경우 S3 버킷을 삭제합니다.	쓰기			
DescribeAccountAttributes	사용자의 계정에 대한 서비스 제한을 설명합니다.	List			
DescribeBackups	단일 백업, 지정된 서버의 모든 백업 또는 사용자 계정의 모든 백업을 설명합니다.	List			
DescribeEvents	지정된 서버의 모든 이벤트를 설명합니다.	List			
DescribeNodeAssociationStatus	지정된 노드 토큰 및 지정된 서버에 대한 연결 상태를 설명합니다.	List			
DescribeServers	지정된 서버 또는 사용자 계정의 모든 서버를 설명합니다.	List			
DisassociateNode	서버에서 지정된 노드를 연결 해제합니다.	쓰기			
RestoreServer	지정된 서버에 백업을 적용합니다. 지정된 경우 ec2 인스턴스를 가능한 대로 스왑 아웃합니다.	쓰기			
StartMaintenance	서버 유지 관리를 즉시 시작합니다.	쓰기			
UpdateServer	일반 서버 설정을 업데이트합니다.	쓰기			
UpdateServerEngineAttributes	구성 관리 유형에 고유한 서버 설정을 업데이트합니다.	쓰기			

AWS OpsWorks Configuration Management에서 정의한 리소스 유형

AWS OpsWorks Configuration Management는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS OpsWorks Configuration Management에 대한 액세스를 허용하려면 정책에 `"Resource": "*"`를 지정합니다.

AWS OpsWorks Configuration Management에 사용되는 조건 키

OpsworksCM에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Organizations에 사용되는 작업, 리소스 및 조건 키

AWS Organizations(서비스 접두사: `organizations`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Organizations에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptHandshake	핸드셰이크 요청에 의해 제안된 작업에 동의하는 핸드셰이크의 전송 위치로 응답을 전송할 수 있는 권한을 부여합니다.	쓰기	handshake* (p. 1402)		
AttachPolicy	정책을 루트, 조직 단위 또는 개인 계정에 연결할 수 있는 권한을 부여합니다.	쓰기	policy* (p. 1402)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			account (p. 1402)		
			organizationalunit (p. 1402)		
			root (p. 1402)		
CancelHandshake	핸드셰이크를 취소할 수 있는 권한을 부여합니다.	쓰기	handshake* (p. 1402)		
CreateAccount	요청을 하는 자격 증명이 있는 조직의 멤버가 자동으로 되는 AWS 계정을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateGovCloudAccount	AWS GovCloud(US) 계정을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateOrganization	조직을 생성할 수 있는 권한을 부여합니다. CreateOrganization 작업을 호출하는 자격 증명이 있는 계정은 자동으로 새 조직의 마스터 계정이 됩니다.	쓰기			
CreateOrganizationalUnit	루트 또는 상위 OU 내에 조직 단위(OU)를 생성할 수 있는 권한을 부여합니다.	쓰기	organizationalunit (p. 1402)		
			root (p. 1402)		
CreatePolicy	루트, 조직 단위(OU) 또는 개인 AWS 계정에 연결할 수 있는 정책을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeclineHandshake	핸드셰이크 요청을 거부할 수 있는 권한을 부여합니다. 그러면 핸드셰이크 상태가 DECLINED(거부됨)으로 설정되고 요청을 효율적으로 비활성화합니다.	쓰기	handshake* (p. 1402)		
DeleteOrganization	조직을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteOrganizationalUnit	루트 또는 다른 OU에서 조직 단위를 삭제할 수 있는 권한을 부여합니다.	쓰기	organizationalunit* (p. 1402)		
DeletePolicy	조직에서 정책을 삭제할 수 있는 권한을 부여합니다.	쓰기	policy* (p. 1402)		
DescribeAccount	특정 계정에 대한 조직 관련 상세 정보를 검색할 수 있는 권한을 부여합니다.	Read	account* (p. 1402)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeCreateAccountStatus	계정을 생성하기 위한 비동기식 요청의 현재 상태를 검색할 수 있는 권한을 부여합니다.	Read			
DescribeEffectivePolicy	계정에 대한 유효 정책을 검색할 수 있는 권한을 부여합니다.	Read	account* (p. 1402)		
DescribeHandshake	이전에 요청한 핸드셰이크에 대한 상세 정보를 검색할 수 있는 권한을 부여합니다.	Read	handshake* (p. 1402)		
DescribeOrganization	호출 자격 증명이 속하는 조직에 대한 상세 정보를 검색할 수 있는 권한을 부여합니다.	Read			
DescribeOrganizationalUnit	조직 단위(OU)에 대한 상세 정보를 검색할 수 있는 권한을 부여합니다.	Read	organizationalunit* (p. 1402)		
DescribePolicy	정책에 대한 상세 정보를 검색할 수 있는 권한을 부여합니다.	Read	policy* (p. 1402)		
DetachPolicy	대상 루트, 조직 단위 또는 계정에서 정책을 분리할 수 있는 권한을 부여합니다.	쓰기	policy* (p. 1402)		
			account (p. 1402)		
			organizationalunit (p. 1402)		
			root (p. 1402)		
DisableAWSServiceAccess	AWS Organizations에 AWS 서비스(ServicePrincipal에 의해 지정되는 서비스)의 통합을 비활성화할 수 있는 권한을 부여합니다.	쓰기		organizations:ServicePrincipal (p. 1402)	
DisablePolicyType	루트에서 조직 정책 유형을 비활성화할 수 있는 권한을 부여합니다.	쓰기	root* (p. 1402)		
EnableAWSServiceAccess	AWS Organizations에 AWS 서비스(ServicePrincipal에 의해 지정되는 서비스)의 통합을 활성화할 수 있는 권한을 부여합니다.	쓰기		organizations:ServicePrincipal (p. 1402)	
EnableAllFeatures	통합 결제 기능만 지원으로부터 업그레이드하여 조직의 모든 기능을 활성화하는 프로세스를 시작할 수 있는 권한을 부여합니다.	쓰기			
EnablePolicyType	루트에서 정책 유형을 활성화할 수 있는 권한을 부여합니다.	쓰기	root* (p. 1402)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
InviteAccountToOrganization	멤버 계정으로 조직에 가입하도록 요청하여 다른 AWS 계정에 초대장을 발송할 수 있는 권한을 부여합니다.	쓰기	account (p. 1402)		
LeaveOrganization	상위 조직에서 멤버 계정을 제거할 수 있는 권한을 부여합니다.	쓰기			
ListAWSServiceAccessForOrganization	조직과의 통합을 활성화한 AWS 서비스의 목록을 검색할 수 있는 권한을 부여합니다.	List			
ListAccounts	조직의 모든 계정을 나열할 수 있는 권한을 부여합니다.	List			
ListAccountsForParent	루트 또는 조직 단위(OU)가 포함된 조직의 계정을 나열할 수 있는 권한을 부여합니다.	List	organizationalunit (p. 1402)		
			root (p. 1402)		
ListChildren	상위 OU 또는 루트에 포함된 OU 또는 계정을 모두 나열할 수 있는 권한을 부여합니다.	List	organizationalunit (p. 1402)		
			root (p. 1402)		
ListCreateAccountStatus	조직에 대해 현재 추적 중인 비동기식 계정 생성 요청을 나열할 수 있는 권한을 부여합니다.	List			
ListHandshakesForAccount	계정과 연결된 모든 핸드셰이크를 나열할 수 있는 권한을 부여합니다.	List			
ListHandshakesForOrganization	조직과 연결된 핸드셰이크를 나열할 수 있는 권한을 부여합니다.	List			
ListOrganizationalUnitsForParent	상위 조직 단위 또는 루트의 모든 조직 단위(OU)를 나열할 수 있는 권한을 부여합니다.	List	organizationalunit (p. 1402)		
			root (p. 1402)		
ListParents	하위 OU 또는 계정의 직속 상위 역할을 하는 루트 또는 조직 단위(OU)를 나열할 수 있는 권한을 부여합니다.	List	account (p. 1402)		
			organizationalunit (p. 1402)		
ListPolicies	조직의 모든 정책을 나열할 수 있는 권한을 부여합니다.	List			
ListPoliciesForTarget	루트, 조직 단위(OU) 또는 계정에 직접 연결된 모든 정책을 나열할 수 있는 권한을 부여합니다.	List	account (p. 1402)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			organizationalunit (p. 1402)		
			root (p. 1402)		
ListRoots	조직에 정의되어 있는 모든 루트를 나열할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	지정된 리소스에 대한 모든 태그를 나열할 수 있는 권한을 부여합니다.	List			
ListTargetsForPolicy	정책이 연결된 모든 루트, OU 및 계정을 나열할 수 있는 권한을 부여합니다.	List	policy* (p. 1402)		
MoveAccount	현재 루트 또는 OU의 계정을 다른 상위 루트 또는 OU로 이동할 수 있는 권한을 부여합니다.	쓰기	account* (p. 1402)		
			organizationalunit (p. 1402)		
			root (p. 1402)		
RemoveAccountFromOrganization	조직에서 지정된 계정을 제거할 수 있는 권한을 부여합니다.	쓰기	account* (p. 1402)		
TagResource	지정된 리소스에 하나 이상의 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정			
UntagResource	지정된 리소스에서 하나 이상의 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정			
UpdateOrganizationalUnit	조직 단위(OU)의 이름을 변경할 수 있는 권한을 부여합니다.	쓰기	organizationalunit* (p. 1402)		
UpdatePolicy	기존의 정책을 새로운 이름, 설명 또는 내용으로 업데이트할 수 있는 권한을 부여합니다.	쓰기	policy* (p. 1402)		

AWS Organizations에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1397)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
account	`arn:${Partition}:organizations::${MasterAccountId}:account/o-${OrganizationId}/${AccountId}`	
handshake	`arn:${Partition}:organizations::${MasterAccountId}:handshake/o-${OrganizationId}/${HandshakeType}/h-${HandshakeId}`	
organization	`arn:${Partition}:organizations::${MasterAccountId}:organization/o-${OrganizationId}`	
organizationalunit	`arn:${Partition}:organizations::${MasterAccountId}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}`	
policy	`arn:${Partition}:organizations::${MasterAccountId}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}`	
awspolicy	`arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}`	
root	`arn:${Partition}:organizations::${MasterAccountId}:root/o-${OrganizationId}/r-${RootId}`	

AWS Organizations에 사용되는 조건 키

AWS Organizations는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
organizations:ServicePrincipal	지정된 서비스 보안 주체 이름으로만 요청을 필터링할 수 있습니다	문자열

AWS Outposts에 사용되는 작업, 리소스 및 조건 키

AWS Outposts(서비스 접두사: `outposts`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Outposts에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateOutpost	Outpost를 생성합니다.	쓰기			
GetOutpost	지정된 Outpost에 대한 정보를 가져옵니다.	Read			
GetOutpostInstanceTypes	지정된 Outpost를 위한 인스턴스 유형을 나열합니다.	Read			
ListOutposts	AWS 계정의 Outposts를 나열합니다.	List			
ListSites	지정된 AWS 계정의 사이트를 나열합니다.	List			

AWS Outposts에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1403)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Outpost	`arn:${Partition}:outposts:${Region}:${Account}:outpost/${OutpostId}`	
Site	`arn:${Partition}:outposts:${Region}:${Account}:site/${SiteId}`	
Order	`arn:${Partition}:outposts:${Region}:${Account}:order/${OrderId}`	

AWS Outpostss에 사용되는 조건 키

Outposts에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Performance Insights에 사용되는 작업, 리소스 및 조건 키

AWS Performance Insights(서비스 접두사: `pi`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

주제

AWS Performance Insights에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeDimensionKeys	특정 기간에 대해, 지표의 상위 N 개 차원 키를 검색합니다.	Read	metric-resource* (p. 1404)		
GetResourceMetrics	일정 기간 동안 데이터 소스 집합에 대한 PI 지표를 검색합니다.	Read	metric-resource* (p. 1404)		

AWS Performance Insights에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1404)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
metric-resource	`arn:${Partition}:pi:${Region}:${Account}:metrics/${ServiceType}/${Identifier}`	

AWS Performance Insights에 사용되는 조건 키

Performance Insights에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Personalize에 사용되는 작업, 리소스 및 조건 키

Amazon Personalize(서비스 접두사: `personalize`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

Amazon Personalize에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCampaign	캠페인을 생성합니다.	쓰기	campaign* (p. 1408)		
CreateDataset	데이터 세트를 생성합니다.	쓰기	dataset* (p. 1408)		
CreateDatasetGroup	데이터 세트 그룹을 생성합니다.	쓰기	datasetGroup* (p. 1408)		
CreateDatasetImportJob	데이터 세트 가져오기 작업을 생성합니다.	쓰기	datasetImportJob* (p. 1408)		
CreateEventTracker	이벤트 추적기를 생성합니다.	쓰기	eventTracker* (p. 1408)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateSchema	스키마를 생성합니다.	쓰기	schema* (p. 1407)		
CreateSolution	솔루션을 생성합니다.	쓰기	solution* (p. 1408)		
CreateSolutionVersion	솔루션 버전을 생성합니다.	쓰기	solution* (p. 1408)		
DeleteCampaign	캠페인을 삭제합니다.	쓰기	campaign* (p. 1408)		
DeleteDataset	데이터 세트를 삭제합니다.	쓰기	dataset* (p. 1408)		
DeleteDatasetGroup	데이터 세트 그룹을 삭제합니다.	쓰기	datasetGroup* (p. 1408)		
DeleteEventTracker	이벤트 추적기를 삭제합니다.	쓰기	eventTracker* (p. 1408)		
DeleteSchema	스키마를 삭제합니다.	쓰기	schema* (p. 1407)		
DeleteSolution	솔루션의 모든 버전을 포함하여 솔루션을 삭제합니다.	쓰기	solution* (p. 1408)		
DescribeAlgorithm	알고리즘을 설명합니다.	Read	algorithm* (p. 1408)		
DescribeCampaign	캠페인을 설명합니다.	Read	campaign* (p. 1408)		
DescribeDataset	데이터 세트를 설명합니다.	Read	dataset* (p. 1408)		
DescribeDatasetGroup	데이터 세트 그룹을 설명합니다.	Read	datasetGroup* (p. 1408)		
DescribeDatasetImportJob	데이터 세트 가져오기 작업을 설명합니다.	Read	datasetImportJob* (p. 1408)		
DescribeEventTracker	이벤트 추적기를 설명합니다.	Read	eventTracker* (p. 1408)		
DescribeFeatureTransformation	기능 변환을 설명합니다.	Read	featureTransformation* (p. 1407)		
DescribeRecipe	레시피를 설명합니다.	Read	recipe* (p. 1408)		
DescribeSchema	스키마를 설명합니다.	Read	schema* (p. 1407)		
DescribeSolution	솔루션을 설명합니다.	Read	solution* (p. 1408)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeSolutionVersion	솔루션의 버전을 설명합니다.	Read	solution* (p. 1408)		
GetPersonalizedRanking	순위가 다시 지정된 추천 항목 목록을 가져옵니다.	쓰기	campaign* (p. 1408)		
GetRecommendations	캠페인에서 추천 항목 목록을 가져옵니다.	Read	campaign* (p. 1408)		
GetSolutionMetrics	솔루션 버전에 대한 지표를 가져옵니다.	Read	solution* (p. 1408)		
ListCampaigns	캠페인을 나열합니다.	List			
ListDatasetGroups	데이터 세트 그룹을 나열합니다.	List			
ListDatasetImportJobs	데이터 세트 가져오기 작업을 나열합니다.	List			
ListDatasets	데이터 세트를 나열합니다.	List			
ListEventTrackers	이벤트 추적기를 나열합니다.	List			
ListRecipes	레시피를 나열합니다.	List			
ListSchemas	스키마를 나열합니다.	List			
ListSolutionVersions	솔루션의 버전을 나열합니다.	List			
ListSolutions	솔루션을 나열합니다.	List			
PutEvents	실시간 이벤트 데이터를 기록합니다.	쓰기	eventTracker* (p. 1408)		
UpdateCampaign	캠페인을 업데이트합니다.	쓰기	campaign* (p. 1408)		

Amazon Personalize에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1405)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
schema	`arn:${Partition}:personalize:${Region}:${Account}:schema/${ResourceId}`	
featureTransformation	`arn:${Partition}:personalize:${Region}:${Account}:feature-transformation/${ResourceId}`	

리소스 유형	ARN	조건 키
dataset	`arn:${Partition}:personalize:${Region}:${Account}:dataset/${ResourceId}`	
datasetGroup	`arn:${Partition}:personalize:${Region}:${Account}:dataset-group/${ResourceId}`	
datasetImportJob	`arn:${Partition}:personalize:${Region}:${Account}:dataset-import-job/${ResourceId}`	
solution	`arn:${Partition}:personalize:${Region}:${Account}:solution/${ResourceId}`	
campaign	`arn:${Partition}:personalize:${Region}:${Account}:campaign/${ResourceId}`	
eventTracker	`arn:${Partition}:personalize:${Region}:${Account}:event-tracker/${ResourceId}`	
recipe	`arn:${Partition}:personalize:${Region}:${Account}:recipe/${ResourceId}`	
algorithm	`arn:${Partition}:personalize:${Region}:${Account}:algorithm/${ResourceId}`	

Amazon Personalize에 사용되는 조건 키

Personalize에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Pinpoint에 사용되는 작업, 리소스 및 조건 키

Amazon Pinpoint(서비스 접두사: `mobiletargeting`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Pinpoint에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있

으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateApp	앱을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419) aws:ResourceTag/${TagKey} (p. 1419)	
CreateCampaign	앱 캠페인을 생성합니다.	쓰기	apps* (p. 1418)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419) aws:ResourceTag/${TagKey} (p. 1419)	
CreateEmailTemplate	이메일 템플릿을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419) aws:ResourceTag/${TagKey} (p. 1419)	
CreateExportJob	엔드포인트 정의를 Amazon S3로 내보내는 내보내기 작업을 생성합니다.	쓰기	apps* (p. 1418)		
CreateImportJob	엔드포인트 정의를 가져와 세그먼트를 생성합니다.	쓰기	apps* (p. 1418)		
CreateJourney	앱에 대한 여정을 생성합니다.	쓰기	apps* (p. 1418)		
				aws:RequestTag/${TagKey} (p. 1419)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1419) aws:ResourceTag/${TagKey} (p. 1419)	
CreatePushTemplate	푸시 알림 템플릿을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419) aws:ResourceTag/${TagKey} (p. 1419)	
CreateRecommenderConfiguration	추천 모델에 대한 Amazon Pinpoint 구성을 생성합니다.	쓰기			
CreateSegment	엡이 Pinpoint에 보고하는 엔드포인트 데이터를 기반으로 세그먼트를 생성합니다. 사용자가 Pinpoint 외부에서 엔드포인트 데이터를 가져와 세그먼트를 생성하도록 허용하려면 mobiletargeting:CreateImportJob 작업을 허용합니다.	쓰기	apps* (p. 1418)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419) aws:ResourceTag/${TagKey} (p. 1419)	
CreateSmsTemplate	SMS 메시지 템플릿을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419) aws:ResourceTag/${TagKey} (p. 1419)	
CreateVoiceTemplate	음성 메시지 템플릿을 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419) aws:ResourceTag/${TagKey} (p. 1419)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteAdmChannel	앱의 ADM 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteApnsChannel	앱의 APNs 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteApnsSandboxChannel	앱의 APNs 샌드박스 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteApnsVoipChannel	앱의 APNs VoIP 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteApnsVoipSandboxChannel	앱 APNs VoIP 샌드박스 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteApp	특정 캠페인을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteBaiduChannel	앱의 Baidu 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteCampaign	특정 캠페인을 삭제합니다.	쓰기	apps* (p. 1418)		
			campaigns* (p. 1419)		
DeleteEmailChannel	앱의 이메일 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteEmailTemplate	이메일 템플릿 또는 이메일 템플릿 버전을 삭제합니다.	쓰기	templates* (p. 1419)		
DeleteEndpoint	엔드포인트를 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteEventStream	앱의 이벤트 스트림을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteGcmChannel	앱의 GCM 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteJourney	특정 여정을 삭제합니다.	쓰기	apps* (p. 1418)		
			journeys* (p. 1419)		
DeletePushTemplate	푸시 알림 템플릿 또는 푸시 알림 템플릿 버전을 삭제합니다.	쓰기	templates* (p. 1419)		
DeleteRecommenderConfiguration	추천 모델에 대한 Amazon Pinpoint 구성을 삭제합니다.	쓰기	recommenders* (p. 1419)		
DeleteSegment	특정 세그먼트를 삭제합니다.	쓰기	apps* (p. 1418)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			segments* (p. 1419)		
DeleteSmsChannel	앱의 SMS 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteSmsTemplate	SMS 메시지 템플릿 또는 SMS 메시지 템플릿 버전을 삭제합니다.	쓰기	templates* (p. 1419)		
DeleteUserEndpoints	사용자 ID와 연결된 모든 정책을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteVoiceChannel	앱의 음성 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
DeleteVoiceTemplate	음성 메시지 템플릿 또는 음성 메시지 템플릿 버전을 삭제합니다.	쓰기	templates* (p. 1419)		
GetAdmChannel	앱의 Amazon Device Messaging(ADM) 채널에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetApnsChannel	앱의 APNs 채널에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetApnsSandboxChannel	앱의 APNs 샌드박스 채널에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetApnsVoipChannel	앱의 APNs VoIP 채널에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetApnsVoipSandboxChannel	앱의 APNs VoIP 샌드박스 채널에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetApp	Amazon Pinpoint 계정의 특정 앱에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetApplicationSettings	앱의 기본 설정을 검색합니다.	List	apps* (p. 1418)		
GetApps	Amazon Pinpoint 계정의 앱 목록을 검색합니다.	List	apps* (p. 1418)		
GetBaiduChannel	앱의 Baidu 채널에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetCampaign	특정 캠페인에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
			campaigns* (p. 1419)		
GetCampaignActivities	캠페인이 수행하는 활동에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
			campaigns* (p. 1419)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetCampaignVersion	특정 캠페인 버전에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
			campaigns* (p. 1419)		
GetCampaignVersions	캠페인의 현재 및 이전 버전에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
			campaigns* (p. 1419)		
GetCampaigns	앱의 모든 캠페인에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
GetChannels	앱의 모든 채널 정보를 가져옵니다.	List	apps* (p. 1418)		
GetEmailChannel	앱의 이메일 채널에 대한 정보를 가져옵니다.	Read	apps* (p. 1418)		
GetEmailTemplate	이메일 템플릿의 특정 버전 또는 활성 버전에 대한 정보를 검색합니다.	Read	templates* (p. 1419)		
GetEndpoint	특정 엔드포인트에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetEventStream	앱의 이벤트 스트림에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetExportJob	특정 내보내기 작업에 대한 정보를 가져옵니다.	Read	apps* (p. 1418)		
GetExportJobs	앱의 모든 내보내기 작업의 목록을 검색합니다.	List	apps* (p. 1418)		
GetGcmChannel	앱의 GCM 채널에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetImportJob	특정 가져오기 작업에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetImportJobs	앱의 모든 가져오기 작업에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
GetJourney	특정 여정에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
			journeys* (p. 1419)		
GetPushTemplate	푸시 알림 템플릿의 특정 버전 또는 활성 버전에 대한 정보를 검색합니다.	Read	templates* (p. 1419)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetRecommenderConfiguration	추천 모델에 대한 Amazon Pinpoint 구성 정보를 검색합니다.	Read	recommenders* (p. 1419)		
GetRecommenderConfigurations	Amazon Pinpoint 계정과 연결된 모든 추천 모델 구성 정보를 검색합니다.	List			
GetSegment	특정 세그먼트에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
			segments* (p. 1419)		
GetSegmentExportJobs	엔드포인트 정의를 세그먼트에서 Amazon S3로 내보내는 작업에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
			segments* (p. 1419)		
GetSegmentImportJobs	에서 엔드포인트 정의를 가져와 세그먼트를 생성하는 작업에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
			segments* (p. 1419)		
GetSegmentVersion	특정 세그먼트 버전에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
			segments* (p. 1419)		
GetSegmentVersions	세그먼트의 현재 및 이전 버전에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
			segments* (p. 1419)		
GetSegments	앱의 세그먼트에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
GetSmsChannel	앱의 SMS 채널에 대한 정보를 가져옵니다.	Read	apps* (p. 1418)		
GetSmsTemplate	SMS 메시지 템플릿의 특정 버전 또는 활성 버전에 대한 정보를 검색합니다.	Read	templates* (p. 1419)		
GetUserEndpoints	사용자 ID와 연결된 엔드포인트에 대한 정보를 검색합니다.	Read	apps* (p. 1418)		
GetVoiceChannel	앱의 음성 채널에 대한 정보를 가져옵니다.	Read	apps* (p. 1418)		
GetVoiceTemplate	음성 메시지 템플릿의 특정 버전 또는 활성 버전에 대한 정보를 검색합니다.	Read	templates* (p. 1419)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListJourneys	앱의 모든 여정에 대한 정보를 검색합니다.	List	apps* (p. 1418)		
ListTagsForResource	리소스에 대한 태그를 나열합니다.	List	apps (p. 1418)		
			campaigns (p. 1419)		
			segments (p. 1419)		
ListTemplateVersions	특정 템플릿에 대한 모든 버전을 검색합니다.	List	templates* (p. 1419)		
ListTemplates	쿼리된 템플릿에 대한 메타데이터를 검색합니다.	List	templates* (p. 1419)		
PhoneNumberValidate	전화 번호에 대한 메타데이터(번호 유형(모바일, 유선 또는 VoIP), 위치 및 공급자 등)를 가져옵니다.	Read	apps* (p. 1418)		
PutEventStream	앱의 이벤트 스트림을 생성 또는 업데이트합니다.	쓰기	apps* (p. 1418)		
PutEvents	앱에 대한 이벤트를 생성 또는 업데이트합니다.	쓰기	apps* (p. 1418)		
RemoveAttributes	앱에 대한 속성을 제거하는 데 사용됩니다.	쓰기	apps* (p. 1418)		
SendMessages	특정 엔드포인트로 SMS 메시지 또는 푸시 알림을 전송합니다.	쓰기	apps* (p. 1418)		
SendUsersMessages	특정 사용자 ID와 연결된 모든 엔드포인트로 SMS 메시지 또는 푸시 알림을 전송합니다.	쓰기	apps* (p. 1418)		
TagResource	태그를 리소스에 추가합니다.	태그 지정	apps (p. 1418)		
			campaigns (p. 1419)		
			segments (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UntagResource	리소스에서 태그를 제거합니다.	태그 지정	apps (p. 1418)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			campaigns (p. 1419)		
			segments (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UpdateAdmChannel	앱의 Amazon Device Messaging(ADM) 채널을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateApnsChannel	앱의 Apple 푸시 알림 서비스(APNs) 채널을 삭제합니다.	쓰기	apps* (p. 1418)		
UpdateApnsSandboxChannel	앱의 Apple 푸시 알림 서비스(APNs) 샌드박스 채널을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateApnsVoipChannel	앱의 Apple 푸시 알림 서비스(APNs) VoIP 채널을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateApnsVoipSandboxChannel	앱의 Apple 푸시 알림 서비스(APNs) VoIP 샌드박스 채널을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateApplicationSettings	앱의 기본 설정을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateBaiduChannel	앱의 Baidu 채널을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateCampaign	특정 캠페인을 업데이트합니다.	쓰기	apps* (p. 1418)		
			campaigns* (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UpdateEmailChannel	앱의 이메일 채널을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateEmailTemplate	동일한 버전의 특정 이메일 템플릿을 업데이트하거나 새 버전을 생성합니다.	쓰기	templates* (p. 1419)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UpdateEndpoint	엔드포인트를 생성하거나 엔드포인트 정보를 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateEndpointsBatch	배치 작업으로 엔드포인트를 생성하거나 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateGcmChannel	푸시 알림을 Android 앱으로 전송하도록 허용하는 Firebase Cloud Messaging(FCM) 또는 Google Cloud Messaging(GCM) API 키를 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateJourney	특정 여정을 업데이트합니다.	쓰기	apps* (p. 1418)		
			journeys* (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UpdateJourneyState	특정 여정 상태를 업데이트합니다.	쓰기	apps* (p. 1418)		
			journeys* (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UpdatePushTemplate	동일한 버전의 특정 푸시 알림 템플릿을 업데이트하거나 새 버전을 생성합니다.	쓰기	templates* (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UpdateRecommenderConfiguration	추천 모델에 대한 Amazon Pinpoint 구성을 업데이트합니다.	쓰기	recommenders* (p. 1419)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateSegment	특정 세그먼트를 업데이트합니다.	쓰기	apps* (p. 1418)		
			segments* (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UpdateSmsChannel	앱의 SMS 채널을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateSmsTemplate	동일한 버전의 특정 SMS 메시지 템플릿을 업데이트하거나 새 버전을 생성합니다.	쓰기	templates* (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	
UpdateTemplateActiveVersion	특정 템플릿의 활성 버전 파라미터를 업데이트합니다.	쓰기	templates* (p. 1419)		
UpdateVoiceChannel	앱의 음성 채널을 업데이트합니다.	쓰기	apps* (p. 1418)		
UpdateVoiceTemplate	동일한 버전의 특정 음성 메시지 템플릿을 업데이트하거나 새 버전을 생성합니다.	쓰기	templates* (p. 1419)		
				aws:RequestTag/${TagKey} (p. 1419) aws:TagKeys (p. 1419)	

Amazon Pinpoint에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1408)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
apps	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey} (p. 1419)

리소스 유형	ARN	조건 키
campaigns	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}`	aws:ResourceTag/${TagKey} (p. 1419)
journeys	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}`	aws:ResourceTag/${TagKey} (p. 1419)
segments	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/segments/${SegmentId}`	aws:ResourceTag/${TagKey} (p. 1419)
templates	`arn:${Partition}:mobiletargeting:${Region}:${Account}:templates/${TemplateName}/${ChannelType}`	aws:ResourceTag/${TagKey} (p. 1419)
recommenders	`arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/${RecommenderId}`	

Amazon Pinpoint에 사용되는 조건 키

Amazon Pinpoint는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	Pinpoint 서비스에 대한 사용자의 요청에 있는 키를 기준으로 액세스를 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	Pinpoint 서비스에 대한 사용자의 요청에 있는 모든 태그 키 이름의 목록을 기준으로 액세스를 필터링합니다.	문자열

Amazon Pinpoint 이메일 서비스에 사용되는 작업, 리소스 및 조건 키

Amazon Pinpoint 이메일 서비스(서비스 접두사: `ses`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

- Amazon Pinpoint 이메일 서비스에서 정의한 작업 (p. 1420)

- Amazon Pinpoint Email Service에서 정의한 리소스 유형 (p. 1424)
- Amazon Pinpoint 이메일 서비스에 사용되는 조건 키 (p. 1425)

Amazon Pinpoint 이메일 서비스에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateConfigurationSet	구성 세트를 생성합니다. 구성 세트는 Amazon Pinpoint를 통해 전송하는 이메일에 적용 가능한 규칙 그룹입니다.	쓰기	configuration-set* (p. 1424)		
				aws:TagKeys (p. 1425) aws:RequestTag/${TagKey} (p. 1425)	
CreateConfigurationSetEventDestination	이벤트 대상을 생성합니다.	쓰기	configuration-set* (p. 1424)		
CreateDedicatedIpPool	전용 IP 주소의 새로운 풀을 생성합니다.	쓰기	dedicated-ip-pool* (p. 1424)		
				aws:TagKeys (p. 1425) aws:RequestTag/${TagKey} (p. 1425)	
CreateDeliverabilityTestReport	새로운 예측적 받은 편지함 배치 테스트를 생성합니다.	쓰기	identity* (p. 1425)		
				aws:TagKeys (p. 1425) aws:RequestTag/${TagKey} (p. 1425)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateEmailIdentity	Amazon Pinpoint에 사용할 이메일 자격 증명을 확인합니다.	쓰기	identity* (p. 1425)		
				aws:TagKeys (p. 1425) aws:RequestTag/${TagKey} (p. 1425)	
DeleteConfigurationSet	기존 구성 세트를 삭제합니다.	쓰기	configuration-set* (p. 1424)		
DeleteConfigurationSetEventDestination	이벤트 대상을 삭제합니다.	쓰기	configuration-set* (p. 1424)		
DeleteDedicatedIpPool	전용 IP 풀을 삭제합니다.	쓰기	dedicated-ip-pool* (p. 1424)		
DeleteEmailIdentity	Amazon Pinpoint에 사용하기 위해 이전에 확인한 이메일 자격 증명을 삭제합니다.	쓰기	identity* (p. 1425)		
GetAccount	이메일 전송 상태 및 용량에 대한 정보를 가져옵니다.	Read			
GetBlacklistReports	전용 IP 주소가 표시되는 블랙리스트의 목록을 검색합니다.	Read			
GetConfigurationSet	기존 구성 세트에 대한 정보를 가져옵니다.	Read	configuration-set* (p. 1424)		
GetConfigurationSetEventDestinations	구성 세트와 연결된 이벤트 대상의 목록을 검색합니다.	Read	configuration-set* (p. 1424)		
GetDedicatedIp	전용 IP 주소에 대한 정보를 가져옵니다.	Read			
GetDedicatedIps	Amazon Pinpoint 계정과 연결된 전용 IP 주소를 나열합니다.	Read	dedicated-ip-pool* (p. 1424)		
GetDeliverabilityDashboardOptions	배달 가능성 대시보드의 상태를 표시합니다.	Read			
GetDeliverabilityTestReport	예측적 받은 편지함 배치 테스트의 결과를 검색합니다.	Read	deliverability-test-report* (p. 1424)		
GetDomainStatisticsReport	이메일을 전송하기 위해 사용하는 도메인의 받은 편지함 배치 및 참여 비율을 검색합니다.	Read	identity* (p. 1425)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetEmailIdentity	Amazon Pinpoint 계정과 연결된 특정 자격 증명에 대한 정보를 제공합니다.	Read	identity* (p. 1425)		
ListConfigurationSets	현재 리전의 Amazon Pinpoint 계정과 연결된 구성 세트의 목록을 반환합니다.	List			
ListDedicatedIpPools	현재 AWS 리전의 Amazon Pinpoint 계정에 있는 모든 전용 IP 풀을 나열합니다.	List			
ListDeliverabilityTestReports	사용자가 수행한 예측적 받은 편지함 배치 테스트의 목록을 상태와 상관없이 표시합니다.	List			
ListEmailIdentities	Amazon Pinpoint 계정과 연결된 모든 이메일 자격 증명의 목록을 반환합니다.	List			
ListTagsForResource	특정 리소스와 연결된 모든 태그(키 및 값)를 검색합니다.	Read	configuration-set (p. 1424)		
			dedicated-ip-pool (p. 1424)		
			deliverability-test-report (p. 1424)		
			identity (p. 1425)		
PutAccountDedicatedIpWarmupAttributes	전용 IP 주소의 자동 워밍업 기능을 활성화 또는 비활성화합니다.	쓰기			
PutAccountSendingAttributes	계정에서 이메일을 전송하는 기능을 활성화 또는 비활성화합니다.	쓰기			
PutConfigurationSetDeliveryOptions	구성 세트를 전용 IP 풀과 연결합니다.	쓰기	configuration-set* (p. 1424)		
PutConfigurationSetReputationOptions	특정 AWS 리전에서 특정 구성 세트를 사용하여 전송하는 이메일에 대한 평판 지표의 모음을 활성화 또는 비활성화합니다.	쓰기	configuration-set* (p. 1424)		
PutConfigurationSetSendingOptions	특정 AWS 리전에서 특정 구성 세트를 사용하는 메시지에 대해 이메일 전송을 활성화 또는 비활성화합니다.	쓰기	configuration-set* (p. 1424)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutConfigurationSetTrackingOptions	Amazon Pinpoint를 사용하여 전송하는 이메일의 확인 및 클릭 추적 요소에 사용할 사용자 지정 도메인을 지정합니다.	쓰기	configuration-set* (p. 1424)		
PutDedicatedIpInPool	전용 IP 주소를 기존 전용 IP 풀로 이동합니다.	쓰기	dedicated-ip-pool* (p. 1424)		
PutDedicatedIpWarmupAttributes	전용 IP 워밍업 속성을 내보냅니다.	쓰기			
PutDeliverabilityDashboardOption	배달 가능성 대시보드를 활성화 또는 비활성화합니다.	쓰기			
PutEmailIdentityDkimAttributes	이메일 자격 증명에 대한 DKIM 인증을 활성화 또는 비활성화하는 데 사용됩니다.	쓰기	identity* (p. 1425)		
PutEmailIdentityFeedbackAttributes	자격 증명에 대한 피드백 전달을 활성화 또는 비활성화하는 데 사용됩니다.	쓰기	identity* (p. 1425)		
PutEmailIdentityMailFromAttributes	이메일 자격 증명에 대한 사용자 지정 MAIL FROM 도메인을 활성화 또는 비활성화하는 데 사용됩니다.	쓰기	identity* (p. 1425)		
SendEmail	이메일 메시지를 전송합니다.	쓰기	identity* (p. 1425)		
				ses:FeedbackAddress (p. 1425) ses:FromAddress (p. 1425) ses:FromDisplayName (p. 1425) ses:Recipients (p. 1425)	
TagResource	지정된 리소스에 하나 이상의 태그(키 및 값)를 추가합니다.	태그 지정	configuration-set (p. 1424)		
			dedicated-ip-pool (p. 1424)		
			deliverability-test-report (p. 1424)		
			identity (p. 1425)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1425) aws:RequestTag/${TagKey} (p. 1425)	
UntagResource	지정된 리소스에서 하나 이상의 태그(키 및 값)를 제거합니다.	태그 지정	configuration-set (p. 1424)		
			dedicated-ip-pool (p. 1424)		
			deliverability-test-report (p. 1424)		
			identity (p. 1425)		
				aws:TagKeys (p. 1425)	
UpdateConfigurationSetEventDestination	구성 세트의 이벤트 대상을 업데이트합니다.	쓰기	configuration-set* (p. 1424)		

Amazon Pinpoint Email Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1420)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey} (p. 1425)
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${CustomVerificationEmailTemplateName}`	aws:ResourceTag/${TagKey} (p. 1425)
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${CustomVerificationEmailTemplateName}`	aws:ResourceTag/${TagKey} (p. 1425)
event-destination	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}:event-destination/${EventDestinationName}`	

리소스 유형	ARN	조건 키
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	aws:ResourceTag/${TagKey} (p. 1425)

Amazon Pinpoint 이메일 서비스에 사용되는 조건 키

Amazon Pinpoint 이메일 서비스는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
ses:FeedbackAddress	반송 메일 및 수신 거부가 이메일 피드백 전달로 전송되는 위치를 지정하는 "Return-Path" 주소.	문자열
ses:FromAddress	메시지의 "From" 주소	문자열
ses:FromDisplayName	메시지의 표시 이름으로 사용되는 "From" 주소.	문자열
ses:Recipients	"To", "CC" 및 "BCC" 주소가 포함된 메시지의 수신자 주소.	문자열

Amazon Pinpoint SMS and Voice Service에 사용되는 작업, 리소스 및 조건 키

Amazon Pinpoint SMS and Voice Service(서비스 접두사: `sms-voice`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Pinpoint SMS and Voice Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateConfigurationSet	새 구성 세트를 생성합니다. 구성 세트를 생성한 후 하나 이상의 이벤트 대상을 여기에 추가할 수 있습니다.	쓰기			
CreateConfigurationSetEventDestination	구성 세트에서 새 이벤트 대상을 생성합니다.	쓰기			iam:PassRole
DeleteConfigurationSet	기존 구성 세트를 삭제합니다.	쓰기			
DeleteConfigurationSetEventDestination	구성 세트에서 이벤트 대상을 삭제합니다.	쓰기			
GetConfigurationSetEventDestinations	이벤트 대상에 대한 정보를 가져옵니다. 이벤트 대상이 보고하는 이벤트 유형, 이벤트 대상의 Amazon 리소스 이름(ARN), 이벤트 대상의 이름 등).	Read			
ListConfigurationSets	구성 세트의 목록을 반환합니다. 이 작업은 현재 AWS 리전의 계정과 연결된 구성 세트만 반환합니다.	Read			
SendVoiceMessage	새 음성 메시지를 생성하여 수신자의 전화 번호로 전송합니다.	쓰기			
UpdateConfigurationSetEventDestination	구성 세트에서 이벤트 대상을 업데이트합니다. 이벤트 대상은 음성 호출에 대한 정보를 게시하는 위치입니다. 예를 들어 호출이 실패하면 Amazon CloudWatch 대상으로 이벤트를 로깅할 수 있습니다.	쓰기			iam:PassRole

Amazon Pinpoint SMS and Voice Service에서 정의한 리소스 유형

Amazon Pinpoint SMS 및 Voice Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Pinpoint SMS 및 Voice Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Pinpoint SMS and Voice Service에 사용되는 조건 키

Pinpoint SMS Voice에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Polly에 사용되는 작업, 리소스 및 조건 키

Amazon Polly(서비스 접두사: `polly`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Polly에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteLexicon	AWS 리전에 저장된 지정된 발음 어휘를 삭제합니다.	쓰기	lexicon* (p. 1428)		
DescribeVoices	스피치 합성을 요청할 때 사용할 수 있는 음성 목록을 반환합니다.	List			
GetLexicon	AWS 리전에 저장된 지정된 발음 어휘의 내용을 반환합니다.	Read	lexicon* (p. 1428)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetSpeechSynthesisTask	사용자가 특정 스피치 합성 작업에 대한 정보를 가져올 수 있습니다.	Read			
ListLexicons	AWS 리전에 저장된 발음 어휘의 목록을 반환합니다.	List			
ListSpeechSynthesisTasks	사용자가 요청된 스피치 합성 작업을 나열할 수 있습니다.	List			
PutLexicon	발음 어휘를 AWS 리전에 저장합니다.	쓰기			
StartSpeechSynthesisTask	사용자가 제공된 S3 위치로 긴 입력을 합성할 수 있습니다.	쓰기	lexicon (p. 1428)		s3:PutObject
SynthesizeSpeech	UTF-8 입력, 일반 텍스트 또는 SSML을 바이트의 스트림으로 합성합니다.	Read	lexicon (p. 1428)		

Amazon Polly에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1427)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
lexicon	`arn:${Partition}:polly:${Region}:${Account}:lexicon/${LexiconName}`	

Amazon Polly에 사용되는 조건 키

Polly에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Price List에 사용되는 작업, 리소스 및 조건 키

AWS Price List(서비스 접두사: `pricing`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS Price List에서 정의한 작업 (p. 1429)
- AWS Price List에서 정의한 리소스 유형 (p. 1429)

- AWS Price List의 조건 키 (p. 1429)

AWS Price List에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeServices	모든 (페이지 매김) 서비스에 대한 서비스 세부 정보(serviceCode가 설정되지 않은 경우) 또는 특정 서비스에 대한 서비스 세부 정보(serviceCode가 지정된 경우)를 반환합니다.	Read			
GetAttributeValues	지정된 속성에 대해 가능한 모든 (페이지 매김) 값을 반환합니다.	Read			
GetProducts	지정된 검색 기준과 일치하는 모든 제품을 반환합니다.	Read			

AWS Price List에서 정의한 리소스 유형

AWS Price List는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Price List에 대한 액세스를 허용하려면 정책에서 `“Resource”: “*”`를 지정합니다.

AWS Price List의 조건 키

Price List에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Private Marketplace에 사용되는 작업, 리소스 및 조건 키

AWS Private Marketplace(서비스 접두사: `aws-marketplace`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Private Marketplace에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateProductsWithPrivateMarketplace [권한만 해당]	새로 승인된 제품을 프라이빗 마켓플레이스에 추가합니다. 또한 Private Marketplace와 연결할 제품에 대한 요청을 승인할 수 있습니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	쓰기			
CreatePrivateMarketplace [권한만 해당]	개별 계정 또는 전체 AWS Organization(있을 경우)에서 프라이빗 마켓플레이스를 생성합니다. 이 작업은 AWS Organization을 사용하는 경우에만 마스터 계정이 수행합니다.	쓰기			
CreatePrivateMarketplaceProfile [권한만 해당]	개별 계정 또는 전체 AWS Organization(있을 경우)에서 AWS Marketplace 웹 사이트에 대한 화이트 레이블 경험을 사용자 지정하는 프라이빗 마켓플레이스 프로필을 생성합니다. 이 작업은 AWS Organization을 사용하는 경우에만 마스터 계정이 수행합니다.	쓰기			
CreatePrivateMarketplaceRequests [권한만 해당]	Private Marketplace와 연결할 제품에 대한 새 요청을 생성합니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책에서 허용할 경우 AWS	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	Organization의 모든 계정에서 수행할 수 있습니다.				
DescribePrivateMarketplaceEntityProduct [권한만 해당]	프라이빗 마켓플레이스의 요청된 제품의 상태를 설명합니다(관리 목적). 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	List			
DescribePrivateMarketplaceProfile [권한만 해당]	프라이빗 마켓플레이스 프로필의 세부 정보를 설명합니다(관리 목적). 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	Read			
DescribePrivateMarketplaceRequests [권한만 해당]	Private Marketplace의 요청 및 관련 제품에 대해 설명합니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	List			
DescribePrivateMarketplaceSettings [권한만 해당]	Private Marketplace 설정을 설명합니다. 여기에는 알림에 대한 기본 설정 및 최종 사용자의 요청을 활성화하는 설정이 포함되어 있습니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	Read			
DescribePrivateMarketplaceStatus [권한만 해당]	프라이빗 마켓플레이스의 상태를 설명합니다(관리 목적). 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	Read			
DisassociateProductFromPrivateMarketplace [권한만 해당]	프라이빗 마켓플레이스에서 승인된 제품을 제거합니다. 또한 Private Marketplace와 연결할 제품에 대한 요청을 거부할 수 있습니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListPrivateMarketplaceProducts [권한만 해당]	프라이빗 마켓플레이스의 제품 및 제품 상태에 대한 쿼리 기능한 목록입니다(관리 목적). 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	List			
ListPrivateMarketplaceRequests [권한만 해당]	Private Marketplace의 요청 및 관련 제품에 대한 쿼리 가능한 목록입니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	List			
StartPrivateMarketplace [권한만 해당]	프라이빗 마켓플레이스를 시작하여 사용자 지정된 AWS Marketplace 경험을 구현하고 프라이빗 마켓플레이스에서 제공되는 제품에 따라 구매 제한을 적용합니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	쓰기			
StopPrivateMarketplace [권한만 해당]	프라이빗 마켓플레이스를 중지하여 사용자 지정된 AWS Marketplace 경험을 비활성화하고 제품에 대한 프라이빗 마켓플레이스 구매 제한을 제거합니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	쓰기			
UpdatePrivateMarketplaceOrganization [권한만 해당]	개별 계정 또는 전체 AWS Organization(있을 경우)에서 AWS Marketplace 웹 사이트에 대한 화이트 레이블 경험을 사용자 지정하는 프라이빗 마켓플레이스 프로필을 업데이트합니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdatePrivateMarketplaceSettings [권한만 해당]	Private Marketplace 설정을 업데이트합니다. 여기에는 알림에 대한 기본 설정 및 최종 사용자의 요청을 활성화하는 설정이 포함되어 있습니다. 이 작업은 사용자에게 해당 권한이 있고 조직의 서비스 제어 정책이 허용할 경우 AWS Organization의 모든 계정에서 수행할 수 있습니다.	쓰기			

AWS Private Marketplace에서 정의한 리소스 유형

AWS Private Marketplace는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Private Marketplace에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Private Marketplace에 사용되는 조건 키

Private Marketplace에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon QLDB에 사용되는 작업, 리소스 및 조건 키

Amazon QLDB(서비스 접두사: `qldb`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon QLDB에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateLedger	원장을 생성할 수 있는 권한을 부여합니다.	쓰기	ledger* (p. 1435)		
				aws:RequestTag/${TagKey} (p. 1436) aws:TagKeys (p. 1436)	
DeleteLedger	원장을 삭제할 수 있는 권한을 부여합니다.	쓰기	ledger* (p. 1435)		
DescribeJournalS3Export	저널 내보내기 작업에 대한 정보를 설명할 수 있는 권한을 부여합니다.	Read	ledger* (p. 1435)		
DescribeLedger	원장을 설명할 수 있는 권한을 부여합니다.	Read	ledger* (p. 1435)		
ExecuteStatement	콘솔을 통해 명령을 원장에 전송할 수 있는 권한을 부여합니다.	쓰기	ledger* (p. 1435)		
ExportJournalToS3	저널 내용을 Amazon S3 버킷에 내보낼 수 있는 권한을 부여합니다.	쓰기	ledger* (p. 1435)		
GetBlock	임의의 BlockAddress에 대해 블록을 원장에서 가져올 수 있는 권한을 부여합니다.	Read	ledger* (p. 1435)		
GetDigest	임의의 BlockAddress에 대해 다이제스트를 원장에서 가져올 수 있는 권한을 부여합니다.	Read	ledger* (p. 1435)		
GetRevision	임의의 문서 ID와 임의의 BlockAddress에 대해 개정을 가져올 수 있는 권한을 부여합니다.	Read	ledger* (p. 1435)		
InsertSampleData	콘솔을 통해 샘플 애플리케이션 데이터를 삽입할 수 있는 권한을 부여합니다.	쓰기	ledger* (p. 1435)		
ListJournalS3Exports	모든 원장에 대해 저널 내보내기 작업을 나열할 수 있는 권한을 부여합니다.	List			
ListJournalS3ExportsForLedger	지정된 원장에 대해 저널 내보내기 작업을 나열할 수 있는 권한을 부여합니다.	List	ledger* (p. 1435)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListLedgers	기존 원장을 나열할 수 있는 권한을 부여합니다.	List			
ListTagsForResource	리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	ledger (p. 1435)		
SendCommand	명령을 원장에 전송할 수 있는 권한을 부여합니다.	쓰기	ledger* (p. 1435)		
ShowCatalog	콘솔을 통해 원장 카탈로그를 볼 수 있는 권한을 부여합니다.	쓰기	ledger* (p. 1435)		
TagResource	리소스에 태그를 1개 이상 추가할 수 있는 권한을 부여합니다.	태그 지정	ledger (p. 1435)		
				aws:RequestTag/${TagKey} (p. 1436) aws:TagKeys (p. 1436)	
UntagResource	리소스에서 태그를 1개 이상 제거할 수 있는 권한을 부여합니다.	태그 지정	ledger (p. 1435)		
				aws:TagKeys (p. 1436)	
UpdateLedger	원장 속성을 업데이트할 수 있는 권한을 부여합니다.	쓰기	ledger* (p. 1435)		

Amazon QLDB에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1433)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
ledger	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}`	aws:ResourceTag/${TagKey} (p. 1436)

Amazon QLDB에 사용되는 조건 키

Amazon QLDB는 `Condition` 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon QuickSight에 사용되는 작업, 리소스 및 조건 키

Amazon QuickSight(서비스 접두사: `quicksight`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon QuickSight에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateAdmin [권한만 해당]	CreateAdmin은 사용자가 Amazon QuickSight 관리자, 작성자 및 독자를 프로비저닝하도록 합니다.	쓰기	user* (p. 1441)		
CreateDashboard	템플릿에서 대시보드 생성	쓰기	dashboard* (p. 1441)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1441) aws:TagKeys (p. 1441)	
CreateGroup	QuickSight 그룹을 생성합니다.	쓰기	group* (p. 1441)		
CreateGroupMembership	QuickSight 사용자를 QuickSight 그룹에 추가합니다.	쓰기	group* (p. 1441)	quicksight:UserName (p. 1442)	
CreateIAMPolicyAssignment	지정된 IAM 정책 ARN을 하나 사용하여 할당을 생성하여 지정된 그룹 또는 QuickSight 사용자에게 할당합니다.	쓰기	assignment* (p. 1441)		
CreateReader [권한만 해당]	CreateReader는 사용자가 Amazon QuickSight 독자를 프로비저닝하도록 합니다.	쓰기	user* (p. 1441)		
CreateTemplate	기존 QuickSight 분석 또는 템플릿에서 템플릿 생성	쓰기	template* (p. 1441)		
				aws:RequestTag/${TagKey} (p. 1441) aws:TagKeys (p. 1441)	
CreateTemplateAlias	템플릿의 템플릿 별칭 생성	쓰기	template* (p. 1441)		
CreateUser [권한만 해당]	CreateUser는 사용자가 Amazon QuickSight 작성자 및 독자를 프로비저닝하도록 합니다.	쓰기	user* (p. 1441)		
DeleteDashboard	대시보드 삭제	쓰기	dashboard* (p. 1441)		
DeleteGroup	QuickSight에서 사용자 그룹을 제거합니다.	쓰기	group* (p. 1441)		
DeleteGroupMembership	사용자 그룹에서 사용자를 제거합니다(그러면 사용자가 더 이상 그룹의 멤버가 아님).	쓰기	group* (p. 1441)	quicksight:UserName (p. 1442)	
DeleteIAMPolicyAssignment	기존 할당 업데이트	쓰기	assignment* (p. 1441)		
DeleteTemplate	템플릿 삭제	쓰기	template* (p. 1441)		
DeleteTemplateAlias	지정된 템플릿 별칭이 가리키는 항목 삭제	쓰기	template* (p. 1441)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteUser	호출을 수행하는 IAM 사용자/역할의 자격 증명과 연결된 QuickSight 사용자를 삭제합니다. 이 호출의 결과로 IAM 사용자는 삭제되지 않습니다.	쓰기	user* (p. 1441)		
DeleteUserByPrincipalId	보안 주체 ID로 식별된 사용자를 삭제합니다.	쓰기	user* (p. 1441)		
DescribeDashboard	대시보드에 대한 요약 제공	Read	dashboard* (p. 1441)		
DescribeDashboardPermissions	대시보드에 대한 읽기 및 쓰기 권한 설명	Read	dashboard* (p. 1441)		
DescribeGroup	QuickSight 그룹의 설명 및 ARN을 반환합니다.	Read	group* (p. 1441)		
DescribeIAMPolicyAssignment	기존 할당 설명	Read	assignment* (p. 1441)		
DescribeTemplate	템플릿의 메타데이터 설명	Read	template* (p. 1441)		
DescribeTemplateAlias	템플릿의 템플릿 별칭 설명	Read	template* (p. 1441)		
DescribeTemplatePermissions	템플릿에 대한 읽기 및 쓰기 권한 설명	Read	template* (p. 1441)		
DescribeUser	사용자 이름이 제공된 경우 사용자에 대한 정보를 반환합니다.	Read	user* (p. 1441)		
GetAuthCode [권한만 해당]	QuickSight 사용자를 나타내는 인증 코드를 반환합니다.	Read	user* (p. 1441)		
GetDashboardEmbedURL	QuickSight 대시보드 임베딩 URL을 반환합니다.	Read	dashboard* (p. 1441)		
GetGroupMapping [권한만 해당]	GetGroupMapping은 Amazon QuickSight 엔터프라이즈 버전 계정에서만 사용됩니다. 사용자는 Amazon QuickSight를 사용하여 Amazon QuickSight의 역할에 매핑되어 있는 Microsoft Active Directory(Microsoft AD) 디렉터리 그룹을 확인하고 표시할 수 있습니다.	Read			
ListDashboardVersions	QuickSight 가입의 모든 대시보드 버전 나열	List	dashboard* (p. 1441)		
ListDashboards	AWS 계정의 대시보드 나열	List	dashboard* (p. 1441)		
ListGroupMemberships	사용자 그룹의 멤버 사용자 목록을 반환합니다.	List	group* (p. 1441)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListGroups	QuickSight의 모든 사용자 그룹의 목록을 가져옵니다.	List	group* (p. 1441)		
ListIAMPolicyAssignments	현재 Amazon QuickSight 계정의 모든 할당 나열	List	assignment* (p. 1441)		
ListIAMPolicyAssignmentsForUser	사용자에게 할당된 모든 할당과 해당 할당이 속한 그룹 나열	List	assignment* (p. 1441)		
ListTagsForResource	QuickSight 리소스의 태그를 나열합니다.	List	dashboard (p. 1441)		
			template (p. 1441)		
ListTemplateAliases	템플릿의 모든 별칭 나열	List	template* (p. 1441)		
ListTemplateVersions	현재 Amazon QuickSight 계정의 모든 템플릿 버전 나열	List	template* (p. 1441)		
ListTemplates	현재 Amazon QuickSight 계정의 모든 템플릿 나열	List	template* (p. 1441)		
ListUserGroups	지정된 사용자가 멤버인 그룹의 목록을 반환합니다.	List	user* (p. 1441)		
ListUsers	이 계정에 속하는 모든 QuickSight 사용자의 목록을 반환합니다.	List	user* (p. 1441)		
RegisterUser	자격 증명이 요청에 지정된 IAM 자격 증명/역할과 연결되는 QuickSight 사용자를 생성합니다.	쓰기	user* (p. 1441)	quicksight:IamArn (p. 1441) quicksight:SessionName (p. 1442)	
SearchDirectoryGroups [권한만 해당]	SearchDirectoryGroups는 Amazon QuickSight 엔터프라이즈 버전 계정에서만 사용됩니다. 이를 통해 사용자는 Amazon QuickSight를 사용하여 Microsoft Active Directory디렉터리 그룹을 표시하고, 그 중에서 Amazon QuickSight의 역할에 매핑할 그룹을 선택할 수 있습니다.	쓰기			
SetGroupMapping [권한만 해당]	SearchDirectoryGroups는 Amazon QuickSight 엔터프라이즈 버전 계정에서만 사용됩니다. 이를 통해 사용자는 Amazon QuickSight를 사용하여 Microsoft Active Directory디렉터리 그룹을 표시하고, 그 중에서 Amazon QuickSight의 역할에 매핑할 그룹을 선택할 수 있습니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Subscribe [권한만 해당]	Subscribe는 사용자가 Amazon QuickSight를 구독하도록 합니다. 이 작업을 활성화 시키면 사용자가 구독을 Enterprise Edition으로 업그레이드 할 수 있습니다.	쓰기			
TagResource	QuickSight 리소스에 태그 추가	태그 지정	dashboard (p. 1441)		
			template (p. 1441)		
				aws:TagKeys (p. 1441) aws:RequestTag/${TagKey} (p. 1441)	
Unsubscribe [권한만 해당]	Unsubscribe는 사용자가 Amazon QuickSight에서 구독을 해지하도록 합니다. 그러면 Amazon QuickSight에서 모든 사용자 및 리소스가 영구적으로 삭제됩니다.	쓰기			
UntagResource	QuickSight 리소스에서 태그 제거	태그 지정	dashboard (p. 1441)		
			template (p. 1441)		
				aws:TagKeys (p. 1441)	
UpdateDashboard	AWS 계정의 대시보드 업데이트	쓰기	dashboard* (p. 1441)		
UpdateDashboardPermissions	대시보드에서 읽기 및 쓰기 권한 업데이트	쓰기	dashboard* (p. 1441)		
UpdateDashboardPublishedVersion	대시보드의 게시된 버전 업데이트	쓰기	dashboard* (p. 1441)		
UpdateGroup	그룹 설명을 변경합니다.	쓰기	group* (p. 1441)		
UpdateIAMPolicyAssignment	기존 할당 업데이트	쓰기	assignment* (p. 1441)		
UpdateTemplate	기존 Amazon QuickSight 분석 또는 다른 템플릿에서 템플릿 업데이트	쓰기	template* (p. 1441)		
UpdateTemplateAlias	템플릿의 템플릿 별칭 업데이트	쓰기	template* (p. 1441)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateTemplatePermissions	템플릿에 대한 리소스 사용 권한 업데이트	쓰기	template* (p. 1441)		
UpdateUser	Amazon QuickSight 사용자를 업데이트합니다.	쓰기	user* (p. 1441)		

Amazon QuickSight에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1436)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
user	`arn:${Partition}:quicksight:${Region}:${Account}:user/${ResourceId}`	
group	`arn:${Partition}:quicksight:${Region}:${Account}:group/${ResourceId}`	
dashboard	`arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1441)
template	`arn:${Partition}:quicksight:${Region}:${Account}:template/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1441)
assignment	`arn:${Partition}:quicksight::${Account}:assignment/${ResourceId}`	

Amazon QuickSight에 사용되는 조건 키

Amazon QuickSight는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
quicksight:IamArn	IAM 사용자 ARN 또는 역할 ARN	문자열

조건 키	설명	유형
quicksight:SessionName	세션 이름	문자열
quicksight:UserName	사용자 이름	문자열

Amazon RDS에 사용되는 작업, 리소스 및 조건 키

Amazon RDS(서비스 접두사: `rds`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon RDS에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddRoleToDBCluster	Aurora DB 클러스터에서 IAM(Identity and Access Management) 역할을 연결합니다.	쓰기	cluster* (p. 1458)		iam:PassRole
AddRoleToDBInstance	AWS Identity and Access Management(IAM) 역할을 DB 인스턴스와 연결합니다.	쓰기	db* (p. 1459)		iam:PassRole
AddSourceIdentifierToSubscription	소스 식별자를 기존 RDS 이벤트 알림 구독에 추가합니다.	쓰기	es* (p. 1459)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTagsToResource	메타데이터 태그를 Amazon RDS 리소스에 추가합니다.	태그 지정	db (p. 1459)		
			es (p. 1459)		
			og (p. 1460)		
			pg (p. 1460)		
			ri (p. 1460)		
			secgrp (p. 1460)		
			snapshot (p. 1460)		
			subgrp (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
ApplyPendingMaintenanceAction	대기 중인 유지 관리 작업을 리소스에 적용합니다.	쓰기	db* (p. 1459)		
AuthorizeDBSecurityGroupIngress	두 가지 권한 부여 형식 중 하나를 사용하여 DBSecurityGroup에 대한 수신을 활성화합니다.	권한 관리	secgrp* (p. 1460)		
BacktrackDBCluster	새 DB 클러스터를 생성하지 않고 특정 시점으로 DB 클러스터를 역추적합니다.	쓰기	cluster* (p. 1458)		
CancelExportTask	진행 중인 내보내기 작업을 취소합니다.	쓰기			
CopyDBClusterParameterGroup	지정된 DB 클러스터 파라미터 그룹을 복사합니다.	쓰기	cluster-pg* (p. 1459)		
CopyDBClusterSnapshot	DB 클러스터의 스냅샷을 생성합니다.	쓰기	cluster-snapshot* (p. 1459)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CopyDBParameterGroup	지정된 DB 파라미터 그룹을 복사합니다.	쓰기	pg* (p. 1460)		
CopyDBSnapshot	지정된 DB 스냅샷을 복사합니다.	쓰기	snapshot* (p. 1460)		
CopyOptionGroup	지정된 옵션 그룹을 복사합니다.	쓰기	og* (p. 1460)		
CreateDBCluster	새 Amazon Aurora DB 클러스터를 생성합니다.	태그 지정	cluster* (p. 1458)		iam:PassRole
			cluster-pg* (p. 1459)		
			og* (p. 1460)		
			subgrp* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462) rds:DatabaseEngine (p. 1461) rds:DatabaseName (p. 1461) rds:StorageEncrypted (p. 1461)	
CreateDBClusterEndpoint	새 사용자 지정 엔드포인트를 생성하여 Amazon Aurora DB 클러스터와 연결합니다.	쓰기	cluster* (p. 1458)		
			cluster-endpoint* (p. 1459)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				rds:EndpointType (p. 1461) aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461)	
CreateDBClusterParameterGroup	새 DB 클러스터 파라미터 그룹을 생성합니다.	태그 지정	cluster-pg* (p. 1459)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateDBClusterSnapshot	DB 클러스터의 스냅샷을 생성합니다.	태그 지정	cluster* (p. 1458)		
			cluster-snapshot* (p. 1459)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateDBInstance	새 DB 인스턴스를 생성합니다.	태그 지정	db* (p. 1459)		iam:PassRole
			og* (p. 1460)		
			pg* (p. 1460)		
			secgrp* (p. 1460)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			subgrp* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateDBInstanceReadReplica	소스 DB 인스턴스의 읽기 전용 복제본 역할을 하는 DB 인스턴스를 생성합니다.	태그 지정	db* (p. 1459)		iam:PassRole
			og* (p. 1460)		
			subgrp* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateDBParameterGroup	새 DB 파라미터 그룹을 생성합니다.	태그 지정	pg* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateDBProxy	데이터베이스 프록시를 생성할 수 있는 권한을 부여합니다.	쓰기			iam:PassRole
CreateDBSecurityGroup	새 DB 보안 그룹을 생성합니다. DB 보안 그룹은 DB 인스턴스에 대한 액세스를 제어합니다.	태그 지정	secgrp* (p. 1460)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateDBSnapshot	DBSnapshot을 생성합니다.	태그 지정	db* (p. 1459)		
			snapshot* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateDBSubnetGroup	새 DB 서브넷 그룹을 생성합니다.	태그 지정	subgrp* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateEventSubscription	RDS 이벤트 알림 구독을 생성합니다	태그 지정	es* (p. 1459)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
CreateGlobalCluster	여러 리전에 분산하여 Aurora 글로벌 데이터베이스를 생성합니다.	쓰기	cluster* (p. 1458)		
			global-cluster* (p. 1459)		
CreateOptionGroup	새 옵션 그룹을 생성합니다.	태그 지정	og* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
DeleteDBCluster	DeleteDBCluster 작업은 이전에 프로비저닝된 DB 클러스터를 삭제합니다.	쓰기	cluster* (p. 1458)		
			cluster-snapshot* (p. 1459)		
DeleteDBClusterEndpoint	사용자 지정 엔드포인트를 삭제하고 Amazon Aurora DB 클러스터에서 제거합니다.	쓰기	cluster-endpoint* (p. 1459)		
DeleteDBClusterParameterGroup	지정된 DB 클러스터 파라미터 그룹을 삭제합니다.	쓰기	cluster-pg* (p. 1459)		
DeleteDBClusterSnapshot	DB 클러스터 스냅샷을 삭제합니다.	쓰기	cluster-snapshot* (p. 1459)		
DeleteDBInstance	DeleteDBInstance 작업은 이전에 프로비저닝된 DB 인스턴스를 삭제합니다.	쓰기	db* (p. 1459)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteDBInstanceAutomatedBackup	소스 인스턴스의 DbiResourceId 값 또는 복구 가능 인스턴스의 리소스 ID를 기준으로 자동 백업을 삭제합니다.	쓰기			
DeleteDBParameterGroup	지정된 DBParameterGroup을 삭제합니다.	쓰기	pg* (p. 1460)		
DeleteDBProxy	데이터베이스 프록시를 삭제할 수 있는 권한을 부여합니다.	쓰기	proxy* (p. 1460)		
DeleteDBSecurityGroup	DB 보안 그룹을 삭제합니다.	쓰기	secgrp* (p. 1460)		
DeleteDBSnapshot	DBSnapshot을 삭제합니다.	쓰기	snapshot* (p. 1460)		
DeleteDBSubnetGroup	DB 서브넷 그룹을 삭제합니다.	쓰기	subgrp* (p. 1460)		
DeleteEventSubscription	RDS 이벤트 알림 구독을 삭제합니다.	쓰기	es* (p. 1459)		
DeleteGlobalCluster	글로벌 데이터베이스 클러스터를 삭제합니다.	쓰기	global-cluster* (p. 1459)		
DeleteOptionGroup	기존 옵션 그룹을 삭제합니다.	쓰기	og* (p. 1460)		
DeregisterDBProxyTargets	데이터베이스 프록시 대상 그룹에서 대상을 제거할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1458)		
			db* (p. 1459)		
			proxy* (p. 1460)		
			target-group* (p. 1460)		
DescribeAccountAttributes	고객 계정에 대한 모든 속성을 나열합니다.	List			
DescribeCertificates	이 AWS 계정에 대해 Amazon RDS에서 제공하는 CA 인증서 세트를 나열합니다.	List			
DescribeDBClusterBacktracks	DB 클러스터의 역추적에 대한 정보를 반환합니다.	List	cluster* (p. 1458)		
DescribeDBClusterEndpoints	Amazon Aurora DB 클러스터의 엔드포인트에 대한 정보를 반환합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeDBClusterParameterGroups	DBClusterParameterGroup 설명의 목록을 반환합니다.	List	cluster-pg* (p. 1459)		
DescribeDBClusterParameters	특정 DB 클러스터 파라미터 그룹에 대한 세부 파라미터 목록을 반환합니다.	List	cluster-pg* (p. 1459)		
DescribeDBClusterSnapshotAttributes	수동 DB 클러스터 스냅샷에 대한 DB 클러스터 스냅샷 속성 이름 및 값의 목록을 반환합니다.	List	cluster-snapshot* (p. 1459)		
DescribeDBClusterSnapshots	DB 클러스터 스냅샷에 대한 정보를 반환합니다.	Read			
DescribeDBClusters	프로비저닝된 Aurora DB 클러스터에 대한 정보를 반환합니다.	List	cluster* (p. 1458)		
DescribeDBEngineVersions	사용 가능한 DB 엔진의 목록을 반환합니다.	List	pg* (p. 1460)		
DescribeDBInstanceAutomatedBackups	현재 및 삭제된 인스턴스 모두에 대한 자동 백업의 목록을 반환합니다.	List			
DescribeDBInstances	프로비저닝된 RDS 인스턴스에 대한 정보를 반환합니다.	List			
DescribeDBLogFiles	DB 인스턴스에 대한 DB 로그 파일의 목록을 반환합니다.	List	db* (p. 1459)		
DescribeDBParameterGroups	DBParameterGroup 설명 목록을 반환합니다.	List	pg* (p. 1460)		
DescribeDBParameters	특정 DB 파라미터 그룹에 대한 세부 파라미터 목록을 반환합니다.	List	pg* (p. 1460)		
DescribeDBProxies	프록시를 볼 수 있는 권한을 부여합니다.	List	proxy* (p. 1460)		
DescribeDBProxyTargetGroups	데이터베이스 프록시 대상 그룹 세부 정보를 볼 수 있는 권한을 부여합니다.	List	proxy* (p. 1460)		
DescribeDBProxyTargets	데이터베이스 프록시 대상 세부 정보를 볼 수 있는 권한을 부여합니다.	List	cluster* (p. 1458)		
			db* (p. 1459)		
			proxy* (p. 1460)		
			target-group* (p. 1460)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeDBSecurityGroups	DBSecurityGroup 설명 목록을 반환합니다.	List	secgrp* (p. 1460)		
DescribeDBSnapshotAttributes	수동 DB 스냅샷에 대한 DB 스냅샷 속성 이름 및 값의 목록을 반환합니다.	List	snapshot* (p. 1460)		
DescribeDBSnapshots	DB 스냅샷에 대한 정보를 반환합니다.	List	db* (p. 1459)		
			snapshot* (p. 1460)		
DescribeDBSubnetGroups	DBSubnetGroup 설명 목록을 반환합니다.	List	subgrp* (p. 1460)		
DescribeEngineDefaultClusterParameters	클러스터 데이터베이스 엔진에 대한 기본 엔진 및 시스템 파라미터 정보를 반환합니다.	List			
DescribeEngineDefaultParameters	지정된 데이터베이스 엔진에 대한 기본 엔진 및 시스템 파라미터 정보를 반환합니다.	List			
DescribeEventCategories	모든 이벤트 소스 유형 또는 지정된 경우 지정된 소스 유형에 대한 범주 목록을 표시합니다.	List			
DescribeEventSubscriptions	고객 계정의 모든 구독 설명을 나열합니다.	List	es* (p. 1459)		
DescribeEvents	지난 14일 동안의 DB 인스턴스, DB 보안 그룹, DB 스냅샷 및 DB 파라미터 그룹과 관련된 이벤트를 반환합니다.	List	es* (p. 1459)		
DescribeExportTasks	내보내기 작업에 대한 정보를 반환합니다.	List			
DescribeGlobalClusters	Aurora 글로벌 데이터베이스 클러스터에 대한 정보를 반환합니다.	List			
DescribeOptionGroupOptions	사용 가능한 모든 옵션을 설명합니다.	List	og* (p. 1460)		
DescribeOptionGroups	사용 가능한 옵션 그룹을 설명합니다.	List	og* (p. 1460)		
DescribeOrderableDBInstanceOptions	지정된 엔진에 대해 명령 가능한 DB 인스턴스 옵션의 목록을 반환합니다.	List			
DescribePendingMaintenanceActions	대기 중인 유지 관리 작업이 하나 이상 있는 리소스(예: DB 인스턴스)의 목록을 반환합니다.	List	db* (p. 1459)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeReservedDBInstances	이 계정에 대한 예약 DB 인스턴스 또는 지정된 예약 DB 인스턴스에 대한 정보를 반환합니다.	List	ri* (p. 1460)		
DescribeReservedDBInstancesOfferings	사용 가능한 예약 DB 인스턴스 제품을 나열합니다.	List			
DescribeSourceRegions	현재 AWS 리전이 읽기 전용 복제본을 생성하거나 DB 스냅샷을 복사할 수 있는 소스 AWS 리전의 목록을 반환합니다.	List			
DescribeValidDBInstanceModifications	DB 인스턴스에서 가능한 수정 사항을 나열합니다.	List	db* (p. 1459)		
DownloadCompleteDBLogFile	지정된 데이터베이스 로그 파일의 내용을 다운로드합니다.	Read			
DownloadDBLogFilePortion	지정된 로그 파일의 전체 또는 일부를 다운로드합니다(최대 1MB).	Read	db* (p. 1459)		
FailoverDBCluster	DB 클러스터에 대한 장애 조치를 강제로 실행합니다.	쓰기	cluster* (p. 1458)		
ListTagsForResource	Amazon RDS 리소스의 모든 태그를 나열합니다.	Read	db (p. 1459)		
			es (p. 1459)		
			og (p. 1460)		
			pg (p. 1460)		
			ri (p. 1460)		
			secgrp (p. 1460)		
			snapshot (p. 1460)		
			subgrp (p. 1460)		
ModifyCurrentDBClusterCapacity	Amazon Aurora Severless DB 클러스터의 현재 클러스터 용량을 수정합니다.	쓰기	cluster* (p. 1458)		
ModifyDBCluster	Amazon Aurora DB 클러스터에 대한 설정을 수정합니다.	쓰기	cluster* (p. 1458)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			cluster-pg* (p. 1459)		
			og* (p. 1460)		
ModifyDBClusterEndpoint	Amazon Aurora DB 클러스터에서 엔드포인트의 속성을 수정합니다.	쓰기	cluster-endpoint* (p. 1459)		
ModifyDBClusterParameterGroup	DB 클러스터 파라미터 그룹의 파라미터를 수정합니다.	쓰기	cluster-pg* (p. 1459)		
ModifyDBClusterSnapshotAttribute	속성 및 값을 수동 DB 클러스터 스냅샷에 추가하거나, 수동 DB 클러스터 스냅샷에서 속성 및 값을 제거합니다.	쓰기	cluster-snapshot* (p. 1459)		
ModifyDBInstance	DB 인스턴스에 대한 설정을 수정합니다.	쓰기	db* (p. 1459)		iam:PassRole
			og* (p. 1460)		
			pg* (p. 1460)		
			secgrp* (p. 1460)		
ModifyDBParameterGroup	DB 파라미터 그룹의 파라미터를 수정합니다.	쓰기	pg* (p. 1460)		
ModifyDBProxy	데이터베이스 프록시를 수정할 수 있는 권한을 부여합니다.	쓰기	proxy* (p. 1460)		iam:PassRole
ModifyDBProxyTargetGroup	데이터베이스 프록시에 대한 대상 그룹을 수정할 수 있는 권한을 부여합니다.	쓰기	target-group* (p. 1460)		
ModifyDBSnapshot	수동 DB 스냅샷(암호화 가능 또는 불가능)을 새 엔진 버전으로 업데이트합니다.	쓰기	snapshot* (p. 1460)		
ModifyDBSnapshotAttribute	속성 및 값을 수동 DB 스냅샷에 추가하거나 수동 DB 스냅샷에서 제거합니다.	쓰기	snapshot* (p. 1460)		
ModifyDBSubnetGroup	기존 DB 서브넷 그룹을 수정합니다.	쓰기	subgrp* (p. 1460)		
ModifyEventSubscription	기존 RDS 이벤트 알림 구독을 수정합니다.	쓰기	es* (p. 1459)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifyGlobalCluster	Amazon Aurora 글로벌 클러스터에 대한 설정을 수정합니다.	쓰기	global-cluster* (p. 1459)		
ModifyOptionGroup	기존 옵션 그룹을 수정합니다.	쓰기	og* (p. 1460)		iam:PassRole
PromoteReadReplica	읽기 전용 복제본 DB 인스턴스를 독립 실행형 DB 인스턴스로 승격합니다.	쓰기	db* (p. 1459)		
PromoteReadReplicaDBCluster	읽기 전용 복제본 DB 클러스터를 독립 실행형 DB 클러스터로 승격합니다.	쓰기	cluster* (p. 1458)		
PurchaseReservedDBInstancesOffering	예약 DB 인스턴스 제공을 구매합니다.	쓰기	ri* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461)	
RebootDBInstance	DB 인스턴스를 재부팅하면 데이터베이스 엔진 서비스가 재시작됩니다.	쓰기	db* (p. 1459)		
RegisterDBProxyTargets	데이터베이스 프록시 대상 그룹에 대상을 추가할 수 있는 권한을 부여합니다.	쓰기	target-group* (p. 1460)		
RemoveFromGlobalCluster	Aurora 글로벌 데이터베이스 클러스터에서 Aurora 보조 클러스터를 분리합니다.	쓰기	cluster* (p. 1458)		
			global-cluster* (p. 1459)		
RemoveRoleFromDBCluster	Aurora DB 클러스터에서 AWS Identity and Access Management(IAM) 역할을 연결 해제합니다.	쓰기	cluster* (p. 1458)		iam:PassRole
RemoveRoleFromDBInstance	DB 인스턴스에서 AWS Identity and Access Management(IAM) 역할을 연결 해제합니다.	쓰기	db* (p. 1459)		iam:PassRole
RemoveSourceIdentifierFromSubscription	기존 RDS 이벤트 알림 구독에서 소스 식별자를 제거합니다.	쓰기	es* (p. 1459)		
RemoveTagsFromResource	Amazon RDS 리소스에서 메타데이터 태그를 제거합니다.	태그 지정	db (p. 1459)		
			es (p. 1459)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			og (p. 1460)		
			pg (p. 1460)		
			ri (p. 1460)		
			secgrp (p. 1460)		
			snapshot (p. 1460)		
			subgrp (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
ResetDBClusterParameterGroup	DB 클러스터 파라미터 그룹의 파라미터를 기본값으로 수정합니다.	쓰기	cluster-pg* (p. 1459)		
ResetDBParameterGroup	DB 파라미터 그룹의 파라미터를 엔진/시스템 기본값으로 수정합니다.	쓰기	pg* (p. 1460)		
RestoreDBClusterFromS3	Amazon S3 버킷에 저장된 데이터에서 Amazon Aurora DB 클러스터를 생성합니다.	쓰기	cluster* (p. 1458)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462) rds:DatabaseEngine (p. 1461) rds:DatabaseName (p. 1461) rds:StorageEncrypted (p. 1461)	
RestoreDBClusterFromSnapshot	DB 클러스터 스냅샷에서 새 DB 클러스터를 생성합니다.	쓰기	cluster* (p. 1458)		iam:PassRole
			cluster-snapshot* (p. 1459)		
			og* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
RestoreDBClusterToPointInTime	DB 클러스터를 임의의 시점으로 복원합니다	쓰기	cluster* (p. 1458)		iam:PassRole
			og* (p. 1460)		
			subgrp* (p. 1460)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
RestoreDBInstanceFromDBSnapshot	DB 스냅샷에서 새 DB 인스턴스를 생성합니다.	쓰기	db* (p. 1459)		iam:PassRole
			og* (p. 1460)		
			snapshot* (p. 1460)		
			subgrp* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
RestoreDBInstanceFromS3	Amazon S3 버킷에서 새 DB를 생성합니다.	쓰기	db* (p. 1459)		iam:PassRole
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
RestoreDBInstanceToPointInTime	DB 인스턴스를 임의의 특정 시점으로 복원합니다.	쓰기	db* (p. 1459)		iam:PassRole
			og* (p. 1460)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			snapshot* (p. 1460)		
			subgrp* (p. 1460)		
				aws:RequestTag/${TagKey} (p. 1461) aws:TagKeys (p. 1461) rds:req-tag/${TagKey} (p. 1462)	
RevokeDBSecurityGroupIngress	이전에 권한이 부여된 IP 범위나 EC2 또는 VPC 보안 그룹에 대한 DBSecurityGroup의 수신을 취소합니다.	쓰기	secgrp* (p. 1460)		
StartActivityStream	사용자가 활동 스트림을 시작할 수 있습니다.	쓰기	cluster* (p. 1458)		
StartDBCluster	DB 클러스터를 시작합니다.	쓰기	cluster* (p. 1458)		
StartDBInstance	DB 인스턴스를 시작합니다.	쓰기	db* (p. 1459)		
StartExportTask	DB 스냅샷에 대한 새 내보내기 작업을 시작합니다.	쓰기			iam:PassRole
StopActivityStream	사용자가 활동 스트림을 중지할 수 있습니다.	쓰기	cluster* (p. 1458)		
StopDBCluster	DB 클러스터를 중지합니다.	쓰기	cluster* (p. 1458)		
StopDBInstance	DB 인스턴스를 중지합니다.	쓰기	db* (p. 1459)		

Amazon RDS에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1442)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
cluster	`arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}`	aws:ResourceTag/${TagKey} (p. 1461)

리소스 유형	ARN	조건 키
		rds:cluster-tag/${TagKey} (p. 1461)
cluster-endpoint	arn:${Partition}:rds:${Region}:${Account}:cluster-endpoint:${DbClusterEndpoint}	aws:ResourceTag/${TagKey} (p. 1461)
cluster-pg	arn:${Partition}:rds:${Region}:${Account}:cluster-pg:${ClusterParameterGroupName}	aws:ResourceTag/${TagKey} (p. 1461) rds:cluster-pg-tag/${TagKey} (p. 1461)
cluster-snapshot	arn:${Partition}:rds:${Region}:${Account}:cluster-snapshot:${ClusterSnapshotName}	aws:ResourceTag/${TagKey} (p. 1461) rds:cluster-snapshot-tag/${TagKey} (p. 1461)
db	arn:${Partition}:rds:${Region}:${Account}:db:${DbInstanceName}	aws:ResourceTag/${TagKey} (p. 1461) rds:DatabaseClass (p. 1461) rds:DatabaseEngine (p. 1461) rds:DatabaseName (p. 1461) rds:MultiAz (p. 1461) rds:Piops (p. 1461) rds:StorageEncrypted (p. 1461) rds:StorageSize (p. 1461) rds:Vpc (p. 1461) rds:db-tag/${TagKey} (p. 1461)
es	arn:${Partition}:rds:${Region}:${Account}:es:${SubscriptionName}	aws:ResourceTag/${TagKey} (p. 1461) rds:es-tag/${TagKey} (p. 1461)
global-cluster	arn:${Partition}:rds:${Account}:global-cluster:${GlobalCluster}	

리소스 유형	ARN	조건 키
og	`arn:${Partition}:rds:${Region}:${Account}:og:${OptionGroupName}`	aws:ResourceTag/${TagKey} (p. 1461) rds:og-tag/${TagKey} (p. 1461)
pg	`arn:${Partition}:rds:${Region}:${Account}:pg:${ParameterGroupName}`	aws:ResourceTag/${TagKey} (p. 1461) rds:pg-tag/${TagKey} (p. 1462)
proxy	`arn:${Partition}:rds:${Region}:${Account}:db-proxy:${DbProxyId}`	
ri	`arn:${Partition}:rds:${Region}:${Account}:ri:${ReservedDbInstanceName}`	aws:ResourceTag/${TagKey} (p. 1461) rds:ri-tag/${TagKey} (p. 1462)
secgrp	`arn:${Partition}:rds:${Region}:${Account}:secgrp:${SecurityGroupName}`	aws:ResourceTag/${TagKey} (p. 1461) rds:secgrp-tag/${TagKey} (p. 1462)
snapshot	`arn:${Partition}:rds:${Region}:${Account}:snapshot:${SnapshotName}`	aws:ResourceTag/${TagKey} (p. 1461) rds:snapshot-tag/${TagKey} (p. 1462)
subgrp	`arn:${Partition}:rds:${Region}:${Account}:subgrp:${SubnetGroupName}`	aws:ResourceTag/${TagKey} (p. 1461) rds:subgrp-tag/${TagKey} (p. 1462)
target	`arn:${Partition}:rds:${Region}:${Account}:target:${TargetId}`	
target-group	`arn:${Partition}:rds:${Region}:${Account}:target-group:${TargetGroupId}`	

Amazon RDS의 조건 키

Amazon RDS는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
rds:DatabaseClass	DB 인스턴스 클래스의 유형입니다.	문자열
rds:DatabaseEngine	MySQL과 같은 데이터베이스 엔진입니다.	문자열
rds:DatabaseName	DB 인스턴스에 있는 데이터베이스의 사용자 정의 이름입니다.	문자열
rds:EndpointType	엔드포인트의 유형으로 READER, WRITER, CUSTOM 중 하나입니다.	문자열
rds:MultiAz	DB 인스턴스를 여러 가용 영역에서 실행할지 여부를 지정하는 값입니다. DB 인스턴스가 다중 AZ를 사용하고 있음을 나타내려면 true를 지정합니다.	부울
rds:Piops	인스턴스가 지원하는 프로비저닝된 IOPS(PIOPS)의 개수가 포함된 값입니다. PIOPS가 활성화되어 있지 않은 DB 인스턴스를 나타내려면 0을 지정합니다.	숫자
rds:StorageEncrypted	DB 인스턴스 스토리지를 암호화해야 하는지 지정하는 값입니다. 스토리지 암호화를 적용하려면 true를 지정하십시오.	부울
rds:StorageSize	스토리지 볼륨 크기(GB)입니다.	숫자
rds:Vpc	DB 인스턴스를 Amazon Virtual Private Cloud(Amazon VPC)에서 실행할지 여부를 지정하는 값입니다. DB 인스턴스가 Amazon VPC에서 실행됨을 나타내려면 true를 지정합니다.	부울
rds:cluster-pg-tag/${TagKey}	DB 클러스터 파라미터 그룹에 연결된 태그입니다.	문자열
rds:cluster-snapshot-tag/${TagKey}	DB 클러스터 스냅샷에 연결된 태그입니다.	문자열
rds:cluster-tag/${TagKey}	DB 클러스터에 연결된 태그입니다.	문자열
rds:db-tag/${TagKey}	DB 인스턴스에 연결된 태그입니다.	문자열
rds:es-tag/${TagKey}	이벤트 구독에 연결된 태그입니다.	문자열
rds:og-tag/${TagKey}	DB 옵션 그룹에 연결된 태그입니다.	문자열

조건 키	설명	유형
rds:pg-tag/${TagKey}	DB 파라미터 그룹에 연결된 태그입니다.	문자열
rds:req-tag/${TagKey}	리소스에 태그 지정하는 데 사용할 수 있는 태그 키와 값 집합을 제한합니다.	문자열
rds:ri-tag/${TagKey}	예약 DB 인스턴스에 연결된 태그입니다.	문자열
rds:secgrp-tag/${TagKey}	DB 보안 그룹에 연결된 태그입니다.	문자열
rds:snapshot-tag/${TagKey}	DB 스냅샷에 연결된 태그입니다.	문자열
rds:subgrp-tag/${TagKey}	DB 서브넷 그룹에 연결된 태그입니다.	문자열

Amazon RDS Data API에 사용되는 작업, 리소스 및 조건 키

Amazon RDS Data API(서비스 접두사: `rds-data`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon RDS Data API에서 정의한 작업 (p. 1462)
- Amazon RDS Data API에서 정의한 리소스 유형 (p. 1463)
- Amazon RDS Data API에 사용되는 조건 키 (p. 1463)

Amazon RDS Data API에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchExecuteStatement	데이터 배열에서 일괄 SQL 문을 실행합니다.	쓰기			
BeginTransaction	SQL 트랜잭션을 시작합니다.	쓰기			
CommitTransaction	BeginTransaction 작업으로 시작된 SQL 트랜잭션을 종료하고 변경 사항을 커밋합니다.	쓰기			rds-data:BeginTransaction
ExecuteSql	하나 이상의 SQL 문을 실행합니다. 이 작업은 더 이상 사용되지 않습니다. BatchExecuteStatement 또는 ExecuteStatement 작업을 사용합니다.	쓰기			
ExecuteStatement	데이터베이스에 대해 SQL 문을 실행합니다.	쓰기			
RollbackTransaction	트랜잭션의 롤백을 수행합니다. 트랜잭션을 롤백하면 변경 내용이 취소됩니다.	쓰기			rds-data:BeginTransaction

Amazon RDS Data API에서 정의한 리소스 유형

Amazon RDS Data API는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon RDS Data API에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon RDS Data API에 사용되는 조건 키

RDS Data API에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon RDS IAM 인증에 사용되는 작업, 리소스 및 조건 키

Amazon RDS IAM 인증(서비스 접두사: `rds-db`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon RDS IAM 인증에 의해 정의된 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
connect	IAM 역할 또는 사용자가 RDS 데이터베이스에 연결할 수 있도록 허용합니다.	권한 관리	db-user* (p. 1464)		

Amazon RDS IAM 인증에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1464)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
db-user	`arn:${Partition}:rds-db:${Region}:${Account}:dbuser:${DbiResourceId}/${DbUserName}`	

Amazon RDS IAM 인증에 사용되는 조건 키

RDS IAM 인증에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Redshift에 사용되는 작업, 리소스 및 조건 키

Amazon Redshift(서비스 접두사: `redshift`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Redshift에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptReservedNodeExchange	구성을 변경하지 않고 DC1 예약 노드를 DC2 예약 노드로 교환할 수 있는 권한을 부여합니다.	쓰기			
AuthorizeClusterSecurityGroupIngress	Amazon Redshift 보안 그룹에 인바운드(수신) 규칙을 추가할 수 있는 권한을 부여합니다.	권한 관리	securitygroup* (p. 1473)		
			securitygroupingress-ec2securitygroup* (p. 1474)		
AuthorizeSnapshotAccess	지정된 AWS 계정에 스냅샷을 복원할 수 있는 권한을 부여합니다.	권한 관리	snapshot* (p. 1474)		
BatchDeleteClusterSnapshots	최대 크기 100의 배치로 스냅샷을 삭제할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1474)		
BatchModifyClusterSnapshots	스냅샷 목록에 대한 설정을 수정할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1474)		
CancelQuery [권한만 해당]	Amazon Redshift 콘솔을 통해 쿼리를 취소할 수 있는 권한을 부여합니다.	쓰기			
CancelQuerySession [권한만 해당]	Amazon Redshift 콘솔에서 쿼리를 볼 수 있는 권한을 부여합니다.	쓰기			
CancelResize	크기 조정 작업을 취소할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
CopyClusterSnapshot	클러스터 스냅샷을 복사할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1474)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateCluster	클러스터를 생성할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
CreateClusterParameterGroup	Amazon Redshift 파라미터 그룹을 생성할 수 있는 권한을 부여합니다.	쓰기	parametergroup* (p. 1473)		
CreateClusterSecurityGroup	Amazon Redshift 보안 그룹을 생성할 수 있는 권한을 부여합니다.	쓰기	securitygroup* (p. 1473)		
CreateClusterSnapshot	지정된 클러스터의 수동 스냅샷을 생성할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1474)		
CreateClusterSubnetGroup	Amazon Redshift 서브넷 그룹을 생성할 수 있는 권한을 부여합니다.	쓰기	subnetgroup* (p. 1474)		
CreateClusterUser	지정된 Amazon Redshift 사용자가 없는 경우 자동으로 생성할 수 있는 권한을 부여합니다.	권한 관리	dbuser* (p. 1473)		
				redshift:DbUser (p. 1474)	
CreateEventSubscription	Amazon Redshift 이벤트 알림 구독을 생성할 수 있는 권한을 부여합니다.	쓰기	eventsubscription* (p. 1473)		
CreateHsmClientCertificate	클러스터가 HSM에 연결하는 데 사용하는 HSM 클라이언트 인증서를 생성할 수 있는 권한을 부여합니다.	쓰기	hsmclientcertificate* (p. 1473)		
CreateHsmConfiguration	하드웨어 보안 모듈(HSM)에서 데이터베이스 암호화 키를 저장하고 사용하기 위해 클러스터에 필요한 정보를 담고 있는 HSM 구성을 생성할 수 있는 권한을 부여합니다.	쓰기	hsmconfiguration* (p. 1473)		
CreateSavedQuery [권한만 해당]	Amazon Redshift 콘솔을 통해 저장된 SQL 쿼리를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateScheduledAction	Amazon Redshift 예약 작업을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateSnapshotCopyGrant	대상 AWS 리전에서 스냅샷 복사 권한을 생성하고 복사된 스냅샷을 암호화할 수 있는 권한을 부여합니다.	권한 관리	snapshotcopygrant* (p. 1474)		
CreateSnapshotSchedule	스냅샷 일정을 생성할 수 있는 권한을 부여합니다.	쓰기	snapshotschedule* (p. 1474)		
CreateTags	지정된 리소스에 하나 이상의 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteCluster	이전에 프로비저닝된 클러스터를 삭제할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
DeleteClusterParameterGroup	Amazon Redshift 파라미터 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	parametergroup* (p. 1473)		
DeleteClusterSecurityGroup	Amazon Redshift 보안 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	securitygroup* (p. 1473)		
DeleteClusterSnapshot	수동 스냅샷을 삭제할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1474)		
DeleteClusterSubnetGroup	클러스터 서브넷 그룹을 삭제할 수 있는 권한을 부여합니다.	쓰기	subnetgroup* (p. 1474)		
DeleteEventSubscription	Amazon Redshift 이벤트 알림 구독을 삭제할 수 있는 권한을 부여합니다.	쓰기	eventsubscription* (p. 1473)		
DeleteHsmClientCertificate	HSM 클라이언트 인증서를 삭제할 수 있는 권한을 부여합니다.	쓰기	hsmclientcertificate* (p. 1473)		
DeleteHsmConfiguration	Amazon Redshift HSM 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기	hsmconfiguration* (p. 1473)		
DeleteSavedQueries [권한만 해당]	Amazon Redshift 콘솔을 통해 저장된 SQL 쿼리를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteScheduledAction	Amazon Redshift 예약 작업을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteSnapshotCopyGrant	스냅샷 복사 권한을 삭제할 수 있는 권한을 부여합니다.	쓰기	snapshotcopygrant* (p. 1474)		
DeleteSnapshotSchedule	스냅샷 일정을 삭제할 수 있는 권한을 부여합니다.	쓰기	snapshotschedule* (p. 1474)		
DeleteTags	리소스에서 하나 이상의 태그를 삭제할 수 있는 권한을 부여합니다.	태그 지정			
DescribeAccountAttributes	지정된 AWS 계정에 연결된 속성을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeClusterDbRevisions	클러스터에 대한 데이터베이스 개정을 설명할 수 있는 권한을 부여합니다.	List			
DescribeClusterParameterGroups	생성한 파라미터 그룹과 기본 파라미터 그룹을 포함한 Amazon Redshift 파라미터 그룹을 설명할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeClusterParameters	Amazon Redshift 파라미터 그룹에 포함된 파라미터를 설명할 수 있는 권한을 부여합니다.	Read	parametergroup* (p. 1473)		
DescribeClusterSecurityGroups	Amazon Redshift 보안 그룹을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeClusterSnapshots	클러스터 스냅샷에 대한 메타데이터가 포함된 하나 이상의 스냅샷 객체를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeClusterSubnetGroups	클러스터 스냅샷 그룹에 대한 메타데이터가 포함된 하나 이상의 클러스터 서브넷 그룹 객체를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeClusterTracks	사용 가능한 유지 관리 트랙을 설명할 수 있는 권한을 부여합니다.	List			
DescribeClusterVersions	사용 가능한 Amazon Redshift 클러스터 버전을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeClusters	프로비저닝된 클러스터의 속성을 설명할 수 있는 권한을 부여합니다.	List			
DescribeDefaultClusterParameters	파라미터 그룹 패밀리에 대한 파라미터 설정을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeEventCategories	모든 이벤트 소스 유형 또는 지정된 소스 유형에 대한 이벤트 범주를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeEventSubscriptions	지정된 AWS 계정에 대한 Amazon Redshift 이벤트 알림 구독을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeEvents	지난 14일간 클러스터, 보안 그룹, 스냅샷 및 파라미터 그룹과 관련된 이벤트를 설명할 수 있는 권한을 부여합니다.	List			
DescribeHsmClientCertificates	HSM 클라이언트 인증서를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeHsmConfigurations	Amazon Redshift HSM 구성을 설명할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeLoggingStatus	쿼리 및 연결 시도와 같은 정보가 클러스터에 대해 기록되는지 여부를 설명할 수 있는 권한을 부여합니다.	Read	cluster* (p. 1473)		
DescribeNodeConfigurationOptions	지정된 작업 유형에 대한 노드 유형, 노드 수 및 디스크 사용과 같은 가능한 노드 구성의 속성을 설명할 수 있는 권한을 부여합니다.	List			
DescribeOrderableClusterOptions	주문 가능한 클러스터 옵션을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeQuery [권한만 해당]	Amazon Redshift 콘솔을 통해 쿼리를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeReservedNodeOfferings	Amazon Redshift에서 사용 가능한 예약 노드 오퍼링을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeReservedNodes	예약 노드를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeResize	클러스터의 마지막 크기 조정 작업을 설명할 수 있는 권한을 부여합니다.	Read	cluster* (p. 1473)		
DescribeSavedQueries [권한만 해당]	Amazon Redshift 콘솔을 통해 저장된 쿼리를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeScheduledActions	생성된 Amazon Redshift 예약 작업을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeSnapshotCopyGrants	대상 AWS 리전에서 지정된 AWS 계정이 소유한 스냅샷 복사 권한을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeSnapshotSchedules	스냅샷 일정을 설명할 수 있는 권한을 부여합니다.	Read	snapshotschedule* (p. 1474)		
DescribeStorage	계정 수준 백업 스토리지 크기 및 잠정 스토리지를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeTable [권한만 해당]	Amazon Redshift 콘솔을 통해 테이블을 설명할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeTableRestoreStatus	RestoreTableFromClusterSnapshot API 작업을 사용하여 이루어진 하나 이상의 테이블 복원 요청의 상태를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeTags	태그를 설명할 수 있는 권한을 부여합니다.	Read			
DisableLogging	클러스터에 대한 쿼리 및 연결 시도와 같은 로깅 정보를 비활성화할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
DisableSnapshotCopy	클러스터에 대한 스냅샷 자동 복사를 비활성화할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
EnableLogging	클러스터에 대해 쿼리 및 연결 시도와 같은 로깅 정보를 활성화할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
EnableSnapshotCopy	클러스터에 대한 스냅샷 자동 복사를 활성화할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
ExecuteQuery [권한만 해당]	Amazon Redshift 콘솔을 통해 쿼리를 실행할 수 있는 권한을 부여합니다.	쓰기			
FetchResults [권한만 해당]	Amazon Redshift 콘솔을 통해 쿼리 결과를 가져올 수 있는 권한을 부여합니다.	Read			
GetClusterCredentials	지정된 AWS 계정으로 Amazon Redshift 데이터베이스에 액세스할 수 있는 임시 자격 증명을 가져올 수 있는 권한을 부여합니다.	쓰기	dbuser* (p. 1473)		
			dbgroup (p. 1473)		
			dbname (p. 1473)		
				redshift:DbName (p. 1474) redshift:DbUser (p. 1474) redshift:DurationSeconds (p. 1474)	
GetReservedNodeExchangeOfferings	지정된 DC1 예약 노드의 결제 유형, 기간 및 시간 요금과 일치하는 DC2 ReservedNodeOfferings의 배열을 가져올 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
JoinGroup	지정된 Amazon Redshift 그룹에 가입할 수 있는 권한을 부여합니다.	권한 관리	dbgroup* (p. 1473)		
ListDatabases [권한만 해당]	Amazon Redshift 콘솔을 통해 데이터베이스를 나열할 수 있는 권한을 부여합니다.	List			
ListSavedQueries [권한만 해당]	Amazon Redshift 콘솔을 통해 저장된 쿼리를 나열할 수 있는 권한을 부여합니다.	List			
ListSchemas [권한만 해당]	Amazon Redshift 콘솔을 통해 스키마를 나열할 수 있는 권한을 부여합니다.	List			
ListTables [권한만 해당]	Amazon Redshift 콘솔을 통해 테이블을 나열할 수 있는 권한을 부여합니다.	List			
ModifyCluster	클러스터의 설정을 수정할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
ModifyClusterDbRevision	클러스터의 데이터베이스 개정을 수정할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
ModifyClusterIamRoles	클러스터가 다른 AWS 서비스에 액세스하기 위해 사용할 수 있는 AWS Identity and Access Management(IAM) 역할의 목록을 수정할 수 있는 권한을 부여합니다.	권한 관리	cluster* (p. 1473)		
ModifyClusterMaintenance	클러스터의 유지 관리 설정을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyClusterParameterGroup	파라미터 그룹의 파라미터를 수정할 수 있는 권한을 부여합니다.	쓰기	parametergroup* (p. 1473)		
ModifyClusterSnapshot	스냅샷의 설정을 수정할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1474)		
ModifyClusterSnapshotSchedule	클러스터에 대한 스냅샷 일정을 수정할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
ModifyClusterSubnetGroup	지정된 VPC 서브넷 목록을 포함하도록 클러스터 서브넷 그룹을 수정할 수 있는 권한을 부여합니다.	쓰기	subnetgroup* (p. 1474)		
ModifyEventSubscription	기존 Amazon Redshift 이벤트 알림 구독을 수정할 수 있는 권한을 부여합니다.	쓰기	eventsubscription* (p. 1473)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ModifySavedQuery [권한만 해당]	Amazon Redshift 콘솔을 통해 기존의 저장된 쿼리를 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifyScheduledAction	기존 Amazon Redshift 예약 작업을 수정할 수 있는 권한을 부여합니다.	쓰기			
ModifySnapshotCopyRetentionPeriod	소스 AWS 리전에서 스냅샷을 복사한 후 대상 AWS 리전에 스냅샷을 보관할 일수를 수정할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
ModifySnapshotSchedule	스냅샷 일정을 수정할 수 있는 권한을 부여합니다.	쓰기	snapshotschedule* (p. 1474)		
PauseCluster	클러스터를 일시 중지할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
PurchaseReservedNodeOffering	예약 노드를 구매할 수 있는 권한을 부여합니다.	쓰기			
RebootCluster	클러스터를 재부팅할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
ResetClusterParameterGroup	파라미터 그룹의 파라미터를 하나 이상 기본값으로 설정하고 파라미터의 소스 값을 "engine-default"로 설정할 수 있는 권한을 부여합니다.	쓰기	parametergroup* (p. 1473)		
ResizeCluster	클러스터의 크기를 변경할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
RestoreFromClusterSnapshot	스냅샷에서 클러스터를 생성할 수 있는 권한을 부여합니다.	쓰기	snapshot* (p. 1474)		
RestoreTableFromClusterSnapshot	Amazon Redshift 클러스터 스냅샷의 테이블에서 테이블을 생성할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
			snapshot* (p. 1474)		
ResumeCluster	클러스터를 다시 시작할 수 있는 권한을 부여합니다.	쓰기	cluster* (p. 1473)		
RevokeClusterSecurityGroupIngress	이전에 권한이 부여된 IP 범위 또는 Amazon EC2 보안 그룹에 대한 Amazon Redshift 보안 그룹의 수신 규칙을 취소할 수 있는 권한을 부여합니다.	권한 관리	securitygroup* (p. 1473)		
			securitygroupingress-ec2securitygroup* (p. 1474)		
RevokeSnapshotAccess	스냅샷을 복원하기 위해 지정된 AWS 계정에서 액세스 권한을 취소할 수 있는 권한을 부여합니다.	권한 관리	snapshot* (p. 1474)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RotateEncryptionKey	클러스터의 암호화 키를 교체할 수 있는 권한을 부여합니다.	권한 관리	cluster* (p. 1473)		
ViewQueriesFromConsole [권한만 해당]	Amazon Redshift 콘솔을 통해 쿼리 결과를 볼 수 있는 권한을 부여합니다.	List			
ViewQueriesInConsole [권한만 해당]	Amazon Redshift 콘솔을 통해 실행 중인 쿼리 및 로드를 종료할 수 있는 권한을 부여합니다.	List			

Amazon Redshift에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1465)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
cluster	`arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	
dbgroup	`arn:${Partition}:redshift:${Region}:${Account}:dbgroup:${ClusterName}/${DbGroup}`	
dbname	`arn:${Partition}:redshift:${Region}:${Account}:dbname:${ClusterName}/${DbName}`	
dbuser	`arn:${Partition}:redshift:${Region}:${Account}:dbuser:${ClusterName}/${DbUser}`	
eventsubscription	`arn:${Partition}:redshift:${Region}:${Account}:eventsubscription:${EventSubscriptionName}`	
hsmclientcertificate	`arn:${Partition}:redshift:${Region}:${Account}:hsmclientcertificate:${HSMClientCertificateId}`	
hsmconfiguration	`arn:${Partition}:redshift:${Region}:${Account}:hsmconfiguration:${HSMConfigurationId}`	
parametergroup	`arn:${Partition}:redshift:${Region}:${Account}:parametergroup:${ParameterGroupName}`	
securitygroup	`arn:${Partition}:redshift:${Region}:${Account}:securitygroup:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ec2SecurityGroupId}`	

리소스 유형	ARN	조건 키
securitygroupingress cidr	`arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/cidrip/${IpRange}`	
securitygroupingress ec2securitygroup	`arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ece2SecuritygroupId}`	
snapshot	`arn:${Partition}:redshift:${Region}:${Account}:snapshot:${ClusterName}/${SnapshotName}`	
snapshotcopygrant	`arn:${Partition}:redshift:${Region}:${Account}:snapshotcopygrant:${SnapshotCopyGrantName}`	
snapshotschedule	`arn:${Partition}:redshift:${Region}:${Account}:snapshotschedule:${ParameterGroupName}`	
subnetgroup	`arn:${Partition}:redshift:${Region}:${Account}:subnetgroup:${SubnetGroupName}`	

Amazon Redshift에 사용되는 조건 키

Amazon Redshift는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
redshift:DbName	데이터베이스 이름을 기준으로 액세스를 필터링합니다.	문자열
redshift:DbUser	데이터베이스 사용자 이름을 기준으로 액세스를 필터링합니다.	문자열
redshift:DurationSeconds	임시 자격 증명 설정이 만료되기 전까지의 초 수를 기준으로 액세스를 필터링합니다.	문자열

Amazon Rekognition에 사용되는 작업, 리소스 및 조건 키

Amazon Rekognition(서비스 접두사: `rekognition`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Rekognition에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CompareFaces	소스 입력 이미지에 있는 얼굴을 대상 입력 이미지에서 감지된 각 얼굴과 비교합니다.	Read			
CreateCollection	AWS 리전에 모음을 생성합니다. 그런 다음 IndexFaces API를 사용하여 얼굴을 모음에 추가할 수 있습니다.	쓰기	collection* (p. 1478)		
CreateProject	새 Amazon Rekognition Custom Labels 프로젝트를 생성합니다.	쓰기	project* (p. 1478)		
CreateProjectVersion	모델의 새 버전을 생성하고 훈련을 시작합니다.	쓰기	project* (p. 1478)		
			projectversion* (p. 1478)		
CreateStreamProcessor	스트리밍 비디오에서 얼굴을 감지하고 인식하는 데 사용할 수 있는 Amazon Rekognition 스트림 프로세서를 생성합니다.	쓰기	collection* (p. 1478)		
			streamprocessor* (p. 1478)		
DeleteCollection	지정된 모음을 삭제합니다. 이 작업으로 인해 모음의 모든 얼굴이 제거됩니다.	쓰기	collection* (p. 1478)		
DeleteFaces	모음에서 얼굴을 삭제합니다.	쓰기	collection* (p. 1478)		
DeleteProject	프로젝트를 삭제합니다.	쓰기	project* (p. 1478)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteProjectVersion	모델을 삭제합니다.	쓰기	projectversion* (p. 1478)		
DeleteStreamProcessor	이름으로 식별된 스트림 프로세서를 삭제합니다.	쓰기	streamprocessor* (p. 1478)		
DescribeCollection	지정된 모음을 설명합니다.	Read	collection* (p. 1478)		
DescribeProjectVersions	Amazon Rekognition Custom Labels 프로젝트의 모델 버전을 나열하고 설명합니다.	Read	project* (p. 1478)		
DescribeProjects	Amazon Rekognition Custom Labels 프로젝트에 대한 정보를 나열하고 가져옵니다.	Read			
DescribeStreamProcessor	CreateStreamProcessor로 생성된 스트림 프로세서에 대한 정보를 제공합니다.	Read	streamprocessor* (p. 1478)		
DetectCustomLabels	Amazon Rekognition Custom Labels 모델 버전을 사용하여 제공된 이미지에서 사용자 지정 레이블을 감지합니다.	Read	projectversion* (p. 1478)		
DetectFaces	입력으로 제공된 이미지(JPEG 또는 PNG) 내의 사람 얼굴을 감지합니다.	Read			
DetectLabels	입력으로 제공된 이미지(JPEG 또는 PNG) 내의 실제 레이블에 대한 인스턴스를 감지합니다.	Read			
DetectModerationLabels	입력 이미지 내의 조정 레이블을 감지합니다.	Read			
DetectText	입력 이미지의 텍스트를 감지하고 이를 머신 판독 가능한 텍스트로 변환합니다.	Read			
GetCelebrityInfo	자신의 Rekognition ID를 기반으로 유명 인사에 대한 이름과 추가 정보를 가져옵니다.	Read			
GetCelebrityRecognition	StartCelebrityRecognition으로 시작된 Rekognition 비디오 분석에 대한 유명 인사 인식 결과를 가져옵니다.	Read			
GetContentModeration	StartContentModeration으로 시작된 Rekognition 비디오 분석에 대한 콘텐츠 조정 분석 결과를 가져옵니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetFaceDetection	StartFaceDetection으로 시작된 Rekognition 비디오 분석에 대한 얼굴 감지 결과를 가져옵니다.	Read			
GetFaceSearch	StartFaceSearch로 시작된 Rekognition 비디오 얼굴 검색에 대한 얼굴 검색 결과를 가져옵니다.	Read			
GetLabelDetection	StartLabelDetection으로 시작된 Rekognition 비디오 분석의 레이블 감지 결과를 가져옵니다.	Read			
GetPersonTracking	비디오 내에서 감지된 사람에 관한 정보를 가져옵니다.	Read			
GetTextDetection	StartTextDetection으로 시작된 Rekognition 비디오 분석에 대한 텍스트 감지 결과를 가져옵니다.	Read			
IndexFaces	입력 이미지에서 얼굴을 감지하고 이를 지정된 모음에 추가합니다.	쓰기	collection* (p. 1478)		
ListCollections	계정의 모음 ID 목록을 반환합니다.	Read	collection* (p. 1478)		
ListFaces	지정된 모음의 얼굴에 대한 메타데이터를 반환합니다.	Read	collection* (p. 1478)		
ListStreamProcessors	CreateStreamProcessor로 생성한 스트림 프로세서의 목록을 가져옵니다.	List	streamprocessor* (p. 1478)		
RecognizeCelebrities	입력 이미지에서 인식된 유명 인사의 배열을 반환합니다.	Read			
SearchFaces	지정된 입력 얼굴 ID의 경우 지정된 모음에서 일치하는 얼굴을 검색합니다.	Read	collection* (p. 1478)		
SearchFacesByImage	지정된 입력 이미지의 경우 먼저 이미지에서 가장 큰 얼굴을 감지한 다음 지정된 모음에서 일치하는 얼굴을 검색합니다.	Read	collection* (p. 1478)		
StartCelebrityRecognition	비디오에서 유명 인사의 비동기 인식을 시작합니다.	쓰기			
StartContentModeration	비디오에서 노골적이거나 선정적인 성인 콘텐츠의 비동기 감지를 시작합니다.	쓰기			
StartFaceDetection	비디오에서 얼굴의 비동기 감지를 시작합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartFaceSearch	비디오에서 감지된 사람의 얼굴과 일치하는 모음의 얼굴에 대한 비동기 검색을 시작합니다.	쓰기	collection* (p. 1478)		
StartLabelDetection	비디오에서 레이블의 비동기 감지를 시작합니다.	쓰기			
StartPersonTracking	비디오에서 사람의 비동기 추적을 시작합니다.	쓰기			
StartProjectVersion	모델 버전의 배포를 시작합니다.	쓰기	projectversion* (p. 1478)		
StartStreamProcessor	스트림 프로세서의 처리를 시작합니다.	쓰기	streamprocessor* (p. 1478)		
StartTextDetection	비디오에서 텍스트의 비동기 감지를 시작합니다.	쓰기			
StopProjectVersion	배치된 모델 버전을 중지합니다.	쓰기	projectversion* (p. 1478)		
StopStreamProcessor	CreateStreamProcessor로 생성된 실행 중인 스트림 프로세서를 중지합니다.	쓰기	streamprocessor* (p. 1478)		

Amazon Rekognition에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1475)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
collection	`arn:${Partition}:rekognition:${Region}:${Account}:collection/${CollectionId}`	
streamprocessor	`arn:${Partition}:rekognition:${Region}:${Account}:streamprocessor/${StreamprocessorId}`	
project	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/${CreationTimestamp}`	
projectversion	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/version/${VersionName}/${CreationTimestamp}`	

Amazon Rekognition의 조건 키

Rekognition에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Resource Access Manager에 사용되는 작업, 리소스 및 조건 키

AWS Resource Access Manager(서비스 접두사: `ram`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Resource Access Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptResourceShareInvitation	지정된 리소스 공유 초대를 수락합니다.	쓰기	resource-share-invitation* (p. 1484)		
				ram:ShareOwnerAccountId (p. 1485)	
AssociateResourceShare	리소스 및/또는 보안 주체를 리소스 공유와 연결합니다.	쓰기	resource-share* (p. 1484)		
				aws:ResourceTag/${TagKey} (p. 1484) ram:ResourceShareName (p. 1485)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				ram:AllowsExternalPrincipals (p. 1484) ram:Principal (p. 1484) ram:RequestedResourceType (p. 1485) ram:ResourceArn (p. 1485)	
AssociateResourceSharePermission	권한을 리소스 공유에 연결합니다.	쓰기	permission* (p. 1484)		
			resource-share* (p. 1484)		
				aws:ResourceTag/${TagKey} (p. 1484) ram:AllowsExternalPrincipals (p. 1484) ram:ResourceShareName (p. 1485) ram:PermissionArn (p. 1484)	
CreateResourceShare	제공된 리소스 및/또는 보안 주체로 리소스 공유를 생성합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1484) aws:TagKeys (p. 1484) ram:RequestedResourceType (p. 1485) ram:ResourceArn (p. 1485) ram:RequestedAllowsExternalPrincipals (p. 1484) ram:Principal (p. 1484)	
DeleteResourceShare	리소스 공유를 삭제합니다.	쓰기	resource-share* (p. 1484)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:ResourceTag/${TagKey} (p. 1484) ram:ResourceShareName (p. 1485) ram:AllowsExternalPrincipals (p. 1484)	
DisassociateResourceShare	리소스 공유에서 리소스 및/또는 보안 주체를 연결 해제합니다.	쓰기	resource-share* (p. 1484)		
				aws:ResourceTag/${TagKey} (p. 1484) ram:ResourceShareName (p. 1485) ram:AllowsExternalPrincipals (p. 1484) ram:Principal (p. 1484) ram:RequestedResourceType (p. 1485) ram:ResourceArn (p. 1485)	
DisassociateResourceSharePermission	리소스 공유에서 권한을 연결 해제합니다.	쓰기	permission* (p. 1484)		
			resource-share* (p. 1484)		
				aws:ResourceTag/${TagKey} (p. 1484) ram:AllowsExternalPrincipals (p. 1484) ram:ResourceShareName (p. 1485) ram:PermissionArn (p. 1484)	
EnableSharingWithAwsOrganization	고객의 조직에 액세스하고 고객의 계정에서 SLR을 생성할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetPermission	AWS RAM 권한의 내용을 가져옵니다.	Read	permission* (p. 1484)		
				ram:PermissionArn (p. 1484)	
GetResourcePolicies	사용자가 소유하고 공유한 지정된 리소스에 대한 정책을 가져옵니다.	Read			
GetResourceShareAssociations	제공된 목록으로부터 또는 지정된 유형의 지정된 상태를 기준으로 리소스 공유 연결 세트를 가져옵니다.	Read			
GetResourceShareInvitations	지정된 초대 ARN 또는 리소스 공유 ARN을 기준으로 리소스 공유 초대를 가져옵니다.	Read			
GetResourceShares	제공된 목록으로부터 또는 지정된 상태를 기준으로 리소스 공유 세트를 가져옵니다.	Read			
ListPendingInvitationResources	사용자와 공유되지만 초대가 아직 보류 중인 리소스 공유의 리소스를 나열합니다.	Read	resource-share-invitation* (p. 1484)		
ListPermissions	AWS RAM 권한을 나열합니다.	List			
ListPrincipals	사용자가 리소스를 공유한 보안 주체 또는 사용자와 리소스를 공유한 보안 주체를 나열합니다.	List			
ListResourceSharePermissions	리소스 공유와 연결된 권한을 나열합니다.	List	resource-share* (p. 1484)		
				aws:ResourceTag/${TagKey} (p. 1484) ram:ResourceShareName (p. 1485) ram:AllowsExternalPrincipals (p. 1484)	
ListResources	리소스 공유에 추가한 리소스 또는 사용자와 공유되는 리소스를 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RejectResourceShareInvitation	지정된 리소스 공유 초대를 거부합니다.	쓰기	resource-share-invitation* (p. 1484)		
				ram:ShareOwnerAccountId (p. 1485)	
TagResource	지정된 리소스 공유에 태그를 지정합니다.	쓰기	resource-share* (p. 1484)		
				aws:RequestTag/${TagKey} (p. 1484) aws:TagKeys (p. 1484)	
UntagResource	지정된 리소스 공유에서 태그를 제거합니다.	쓰기	resource-share* (p. 1484)		
				aws:RequestTag/${TagKey} (p. 1484) aws:TagKeys (p. 1484)	
UpdateResourceShare	리소스 공유의 속성을 업데이트합니다.	쓰기	resource-share* (p. 1484)		
				aws:ResourceTag/${TagKey} (p. 1484) ram:ResourceShareName (p. 1485) ram:AllowsExternalPrincipals (p. 1484) ram:RequestedAllowsExternalPrincipals (p. 1484)	

AWS Resource Access Manager에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1479)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
resource-share	`arn:${Partition}:ram:${Region}:${Account}:resource-share/${ResourcePath}`	aws:ResourceTag/${TagKey} (p. 1484) ram:AllowsExternalPrincipals (p. 1484) ram:ResourceShareName (p. 1485)
resource-share-invitation	`arn:${Partition}:ram:${Region}:${Account}:resource-share-invitation/${ResourcePath}`	
permission	`arn:${Partition}:ram::${Account}:permission/${ResourcePath}`	ram:PermissionArn (p. 1484)

AWS Resource Access Manager에 사용되는 조건 키

AWS Resource Access Manager는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	리소스 공유를 생성 또는 태그 지정할 때 반드시 사용해야 하는 태그 키-값 페어를 지정합니다. 사용자가 이 특정 키들을 전달하지 않거나 태그를 전혀 지정하지 않으면 요청은 실패합니다.	문자열
aws:ResourceTag/${TagKey}	지정된 태그 키-값 페어를 갖는 리소스에서만 작업을 수헹할 수 있음을 표시합니다.	문자열
aws:TagKeys	리소스 공유를 생성 또는 태그 지정할 때 사용할 수 있는 태그 키를 지정합니다.	문자열
ram:AllowsExternalPrincipals	외부 보안 주체와의 공유를 허용 또는 거부하는 리소스 공유에서만 이 작업을 수행할 수 있음을 표시합니다. 예를 들어 외부 보안 주체와의 공유를 허용하는 리소스 공유에서만 작업을 수행할 수 있을 경우 true를 지정합니다. 외부 보안 주체는 사용자의 AWS 조직에 속하지 않는 AWS 계정입니다.	Bool
ram:PermissionArn	지정된 권한 ARN을 사용하는 리소스에서만 이 작업을 수행할 수 있음을 나타냅니다.	Arn
ram:Principal	지정된 형식의 보안 주체가 리소스 공유와 연결 또는 연결 해제될 수 있습니다.	문자열
ram:RequestedAllowsExternalPrincipals	요청에는 'allowExternalPrincipals'에 대해 지정된 값이 있어야 합니다. 외부 보안 주체는 사용자의 AWS Organization에 속하지 않는 AWS 계정입니다.	Bool

조건 키	설명	유형
ram:RequestedResourceType	지정된 리소스 유형에서만 이 작업을 수행할 수 있음을 표시합니다.	문자열
ram:ResourceArn	지정된 ARN을 갖는 리소스에서만 이 작업을 수행할 수 있음을 표시합니다.	Arn
ram:ResourceShareName	지정된 이름을 갖는 리소스 공유에서만 이 작업을 수행할 수 있음을 표시합니다.	문자열
ram:ShareOwnerAccountId	특정 계정이 소유하는 리소스 공유에서만 이 작업을 수행할 수 있음을 표시합니다. 예를 들어 이 조건 키를 사용하여 리소스 공유 소유자의 계정 ID를 기준으로 수락 또는 거부할 수 있는 리소스 공유 초대를 지정할 수 있습니다.	문자열

Amazon Resource Group Tagging API에 사용되는 작업, 리소스 및 조건 키

Amazon Resource Group Tagging API(서비스 접두사: `tag`)는 IAM 정책에 사용할 수 있는 다음과 같은 서비스별 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Resource Group Tagging API에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeReportCreation	StartReportCreation 작업의 상태를 설명합니다.	Read			
GetComplianceSummary	유효 태그 정책을 준수하지 않는 리소스 수를 보여 주는 테이블을 가져옵니다.	Read			
GetResources	주어진 태그 필터와 일치하는 태그 지정된 AWS 리소스를 가져옵니다.	Read			
GetTagKeys	특정 리전의 계정을 위한 모든 tagKeys를 가져옵니다.	Read			
GetTagValues	특정 리전의 계정을 위한 모든 tagValues를 가져옵니다.	Read			
StartReportCreation	조직의 계정에 있는 태그가 지정된 모든 리소스를 나열하고 각 리소스가 유효한 태그 정책을 준수하는지 여부를 나열하는 보고서를 생성합니다.	쓰기			
TagResources	AWS 리소스에 태그를 추가합니다.	태그 지정			
UntagResources	AWS 리소스에서 태그를 제거합니다.	태그 지정			

Amazon Resource Group Tagging API에서 정의한 리소스 유형

Amazon Resource Group Tagging API는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Resource Group Tagging API에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Resource Group Tagging API에 사용되는 조건 키

Resource Group Tagging에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Resource Groups에 사용되는 작업, 리소스 및 조건 키

AWS Resource Groups(서비스 접두사: `resource-groups`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Resource Groups에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateGroup	지정된 이름, 설명 및 리소스 쿼리로 그룹을 생성합니다.	태그 지정	group* (p. 1488)		
				aws:RequestTag/${TagKey} (p. 1488) aws:TagKeys (p. 1488)	
DeleteGroup	지정된 리소스 그룹을 삭제합니다.	쓰기	group* (p. 1488)		
GetGroup	지정된 리소스 그룹의 정보를 가져옵니다.	Read	group* (p. 1488)		
GetGroupQuery	지정된 리소스 그룹과 연결된 쿼리를 가져옵니다.	Read	group* (p. 1488)		
GetTags	지정된 리소스 그룹과 연결된 태그를 가져옵니다.	Read	group* (p. 1488)		
ListGroupResources	지정된 리소스 그룹의 멤버인 리소스를 나열합니다.	List	group* (p. 1488)		
ListGroups	모든 리소스 그룹을 나열합니다.	List	group* (p. 1488)		
SearchResources	지정된 쿼리와 일치하는 AWS 리소스 식별자의 목록을 반환합니다.	List			
Tag	지정된 리소스 그룹에 태그를 지정합니다.	태그 지정	group* (p. 1488)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1488) aws:TagKeys (p. 1488)	
Untag	지정된 리소스 그룹과 연결된 태그를 제거합니다.	태그 지정	group* (p. 1488)		
				aws:TagKeys (p. 1488)	
UpdateGroup	지정된 리소스 그룹을 업데이트합니다.	쓰기	group* (p. 1488)		
UpdateGroupQuery	지정된 리소스 그룹과 연결된 쿼리를 업데이트합니다.	쓰기	group* (p. 1488)		

AWS Resource Groups에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1487)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
group	`arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}`	aws:ResourceTag/${TagKey} (p. 1488)

AWS Resource Groups의 조건 키

AWS Resource Groups는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS RoboMaker에 사용되는 작업, 리소스 및 조건 키

AWS RoboMaker(서비스 접두사: `robomaker`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS RoboMaker에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchDescribeSimulationJob	여러 시뮬레이션 작업을 설명합니다.	Read			
CancelDeploymentJob	배포 작업을 취소합니다.	쓰기	deploymentJob* (p. 1493)		
CancelSimulationJob	시뮬레이션 작업을 취소합니다.	쓰기	simulationJob* (p. 1493)		
CancelSimulationJobBatch	시뮬레이션 작업 배치 취소	쓰기	simulationJobBatch* (p. 1493)		
CreateDeploymentJob	배포 작업 생성	쓰기		aws:TagKeys (p. 1494) aws:RequestTag/${TagKey} (p. 1494)	iam:CreateServiceLinkedI

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateFleet	동일한 로봇 애플리케이션에서 실행되는 로봇의 논리적 그룹을 나타내는 배포 플릿을 생성합니다.	쓰기		aws:TagKeys (p. 1494) aws:RequestTag/${TagKey} (p. 1494)	
CreateRobot	플릿에 등록할 수 있는 로봇을 생성합니다.	쓰기		aws:TagKeys (p. 1494) aws:RequestTag/${TagKey} (p. 1494)	iam:CreateServiceLinkedI
CreateRobotApplication	로봇 애플리케이션을 생성합니다.	쓰기		aws:TagKeys (p. 1494) aws:RequestTag/${TagKey} (p. 1494)	
CreateRobotApplicationVersion	로봇 애플리케이션의 스냅샷을 생성합니다.	쓰기	robotApplication* (p. 1493)		s3:GetObject
CreateSimulationApplication	시뮬레이션 애플리케이션을 생성합니다.	쓰기		aws:TagKeys (p. 1494) aws:RequestTag/${TagKey} (p. 1494)	
CreateSimulationApplicationVersion	시뮬레이션 애플리케이션의 스냅샷을 생성합니다.	쓰기	simulationApplication* (p. 1493)		s3:GetObject
CreateSimulationJob	시뮬레이션 작업을 생성합니다.	쓰기		aws:TagKeys (p. 1494) aws:RequestTag/${TagKey} (p. 1494)	iam:CreateServiceLinkedI
DeleteFleet	배포 플릿을 삭제합니다.	쓰기	deploymentFleet* (p. 1494)		
DeleteRobot	로봇을 삭제합니다.	쓰기	robot* (p. 1494)		
DeleteRobotApplication	로봇 애플리케이션을 삭제합니다.	쓰기	robotApplication* (p. 1493)		
DeleteSimulationApplication	시뮬레이션 애플리케이션을 삭제합니다.	쓰기	simulationApplication* (p. 1493)		
DeregisterRobot	플릿에서 로봇을 등록 취소합니다.	쓰기	deploymentFleet* (p. 1494)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			robot* (p. 1494)		
DescribeDeploymentJob	배포 작업을 설명합니다.	Read	deploymentJob* (p. 1493)		
DescribeFleet	배포 플릿을 설명합니다.	Read	deploymentFleet* (p. 1494)		
DescribeRobot	로봇을 설명합니다.	Read	robot* (p. 1494)		
DescribeRobotApplication	로봇 애플리케이션을 설명합니다.	Read	robotApplication* (p. 1493)		
DescribeSimulationApplication	시뮬레이션 애플리케이션을 설명합니다.	Read	simulationApplication* (p. 1493)		
DescribeSimulationJob	시뮬레이션 작업을 설명합니다.	Read	simulationJob* (p. 1493)		
DescribeSimulationJobBatch	시뮬레이션 작업 배치 설명	Read	simulationJobBatch* (p. 1493)		
ListDeploymentJobs	배포 작업을 나열합니다.	List			
ListFleets	플릿을 나열합니다.	List			
ListRobotApplications	로봇 애플리케이션을 나열합니다.	List			
ListRobots	로봇을 나열합니다.	List			
ListSimulationApplications	시뮬레이션 애플리케이션을 나열합니다.	List			
ListSimulationJobBatches	시뮬레이션 작업 배치 나열	List			
ListSimulationJobs	시뮬레이션 작업을 나열합니다.	List			
ListTagsForResource	RoboMaker 리소스에 대한 태그를 나열합니다.	List	deploymentFleet (p. 1494)		
			deploymentJob (p. 1493)		
			robot (p. 1494)		
			robotApplication (p. 1493)		
			simulationApplication (p. 1493)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			simulationJob (p. 1493)		
			simulationJobBatch (p. 1493)		
RegisterRobot	로봇을 플릿에 등록합니다.	쓰기	deploymentFleet* (p. 1494)		
			robot* (p. 1494)		
RestartSimulationJob	실행 중인 시뮬레이션 작업을 다시 시작합니다.	쓰기	simulationJob* (p. 1493)		
StartSimulationJobBatch	시뮬레이션 작업 배치 생성	쓰기		aws:TagKeys (p. 1494) aws:RequestTag/${TagKey} (p. 1494)	iam:CreateServiceLinkedI
SyncDeploymentJob	가장 최근에 배포된 로봇 애플리케이션이 플릿의 모든 로봇에 배포되어 있는지 확인합니다.	쓰기	deploymentFleet* (p. 1494)		iam:CreateServiceLinkedI
TagResource	RoboMaker 리소스에 태그를 추가합니다.	쓰기	deploymentFleet (p. 1494)		
			deploymentJob (p. 1493)		
			robot (p. 1494)		
			robotApplication (p. 1493)		
			simulationApplication (p. 1493)		
			simulationJob (p. 1493)		
			simulationJobBatch (p. 1493)		
				aws:TagKeys (p. 1494) aws:RequestTag/${TagKey} (p. 1494)	
UntagResource	RoboMaker 리소스에서 태그를 제거합니다.	쓰기	deploymentFleet (p. 1494)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			deploymentJob (p. 1493)		
			robot (p. 1494)		
			robotApplication (p. 1493)		
			simulationApplication (p. 1493)		
			simulationJob (p. 1493)		
			simulationJobBatch (p. 1493)		
				aws:TagKeys (p. 1494)	
UpdateRobotApplication	로봇 애플리케이션을 업데이트합니다.	쓰기	robotApplication* (p. 1493)		
UpdateSimulationApplication	시뮬레이션 애플리케이션을 업데이트합니다.	쓰기	simulationApplication* (p. 1493)		

AWS RoboMaker에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1489)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
robotApplication	`arn:${Partition}:robomaker:${Region}:${Account}:robot-application/${ApplicationName}/${CreatedOnEpoch}`	aws:ResourceTag/${TagKey} (p. 1494)
simulationApplication	`arn:${Partition}:robomaker:${Region}:${Account}:simulation-application/${ApplicationName}/${CreatedOnEpoch}`	aws:ResourceTag/${TagKey} (p. 1494)
simulationJob	`arn:${Partition}:robomaker:${Region}:${Account}:simulation-job/${SimulationJobId}`	aws:ResourceTag/${TagKey} (p. 1494)
simulationJobBatch	`arn:${Partition}:robomaker:${Region}:${Account}:simulation-job-batch/${SimulationJobBatchId}`	aws:ResourceTag/${TagKey} (p. 1494)
deploymentJob	`arn:${Partition}:robomaker:${Region}:${Account}:deployment-job/${DeploymentJobId}`	aws:ResourceTag/${TagKey} (p. 1494)

리소스 유형	ARN	조건 키
robot	`arn:${Partition}:robomaker:${Region}:${Account}:robot/${RobotName}/${CreatedOnEpoch}`	aws:ResourceTag/${TagKey} (p. 1494)
deploymentFleet	`arn:${Partition}:robomaker:${Region}:${Account}:deployment-fleet/${FleetName}/${CreatedOnEpoch}`	aws:ResourceTag/${TagKey} (p. 1494)

AWS RoboMaker에 사용되는 조건 키

AWS RoboMaker는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}		문자열
aws:ResourceTag/${TagKey}		문자열
aws:TagKeys		문자열

Amazon Route 53에 사용되는 작업, 리소스 및 조건 키

Amazon Route 53(서비스 접두사: `route53`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Route 53에서 정의한 작업 (p. 1494)
- Amazon Route 53에서 정의한 리소스 유형 (p. 1500)
- Amazon Route 53의 조건 키 (p. 1500)

Amazon Route 53에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateVPCWithHostedZone	추가 Amazon VPC를 프라이빗 호스팅 영역과 연결할 수 있는 권한을 부여합니다.	쓰기	hostedzone* (p. 1500)		
ChangeResourceRecordSets	지정된 도메인 또는 하위 도메인 이름에 대한 신뢰할 수 있는 DNS 정보를 포함하는 레코드를 생성, 업데이트 또는 삭제할 수 있는 권한을 부여합니다.	쓰기	hostedzone* (p. 1500)		
ChangeTagsForResource	상태 확인 또는 호스팅 영역에 대한 태그를 추가, 편집 또는 삭제할 수 있는 권한을 부여합니다.	태그 지정	healthcheck* (p. 1500)		
			hostedzone* (p. 1500)		
CreateHealthCheck	웹 애플리케이션, 웹 서버 및 기타 리소스의 상태와 성능을 모니터링하는 새 상태 확인을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateHostedZone	Domain Name System(DNS)이 도메인(예: example.com) 및 하위 도메인의 트래픽을 인터넷에서 라우팅하는 방식을 지정하는 데 사용하는 퍼블릭 호스팅 영역을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateQueryLoggingConfig	DNS 쿼리 로깅에 대한 구성을 생성할 수 있는 권한을 부여합니다.	쓰기	hostedzone* (p. 1500)		
CreateReusableDelegationSet	다중 호스팅 영역에서 재사용할 수 있는 위임 세트(4개의 이름 서버 그룹)를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateTrafficPolicy	하나의 도메인 이름(예: example.com) 또는 하나의 하위 도메인 이름(예: www.example.com)에 대한 다중 DNS 레코드를 생성하는 데 사용하는 트래픽 정책을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateTrafficPolicyInstance	지정된 트래픽 정책 버전의 설정에 따라 지정된 호스팅 영역에 레	쓰기	hostedzone* (p. 1500)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
	코드를 생성할 수 있는 권한을 부여합니다.		trafficpolicy* (p. 1500)		
CreateTrafficPolicyVersion	기존 트래픽 정책의 새 버전을 생성할 수 있는 권한을 부여합니다.	쓰기	trafficpolicy* (p. 1500)		
CreateVPCAssociationAuthorization	지정된 VPC를 생성한 AWS 계정을 승인하여 다른 계정에서 생성된 지정된 호스팅 영역과 VPC를 연결하는 AssociateVPCWithHostedZone 요청을 제출할 수 있는 권한을 부여합니다.	쓰기	hostedzone* (p. 1500)		
DeleteHealthCheck	상태 확인을 삭제할 수 있는 권한을 부여합니다.	쓰기	healthcheck* (p. 1500)		
DeleteHostedZone	호스팅 영역을 삭제할 수 있는 권한을 부여합니다.	쓰기	hostedzone* (p. 1500)		
DeleteQueryLoggingConfig	DNS 쿼리 로깅에 대한 구성을 삭제할 수 있는 권한을 부여합니다.	쓰기	queryloggingconfig* (p. 1500)		
DeleteReusableDelegationSet	재사용 가능한 위임 세트를 삭제할 수 있는 권한을 부여합니다.	쓰기	delegationset* (p. 1500)		
DeleteTrafficPolicy	트래픽 정책을 삭제할 수 있는 권한을 부여합니다.	쓰기	trafficpolicy* (p. 1500)		
DeleteTrafficPolicyInstance	트래픽 정책 인스턴스와 인스턴스 생성 시 Route 53에서 생성한 모든 레코드를 삭제할 수 있는 권한을 부여합니다.	쓰기	trafficpolicyinstance* (p. 1500)		
DeleteVPCAssociationAuthorization	Amazon Virtual Private Cloud를 Route 53 프라이빗 호스팅 영역과 연결하기 위한 승인을 제거할 수 있는 권한을 부여합니다.	쓰기	hostedzone* (p. 1500)		
DisassociateVPCFromHostedZone	Route 53 프라이빗 호스팅 영역에서 Amazon Virtual Private Cloud를 연결 해제할 수 있는 권한을 부여합니다.	쓰기			
	시나리오: Disassociate by the VPC owner		hostedzone* (p. 1500) hostedzone (p. 1500)		
	시나리오: Disassociate by the hosted zone owner		hostedzone* (p. 1500) hostedzone (p. 1500)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetAccountLimit	현재 계정에 대해 지정된 한도를 가져올 수 있는 권한을 부여합니다(예: 계정을 사용하여 생성할 수 있는 최대 상태 확인 수).	Read			
GetChange	하나 이상의 레코드를 생성, 업데이트 또는 삭제하기 위한 요청의 현재 상태를 가져올 수 있는 권한을 부여합니다.	List	change* (p. 1500)		
GetCheckerIpRanges	Route 53 상태 확인 프로그램에서 리소스 상태를 확인하는 데 사용되는 IP 범위의 목록을 가져올 수 있는 권한을 부여합니다.	List			
GetGeoLocation	지정된 지리적 위치가 Route 53 지리적 위치 레코드에 지원되는지 여부에 대한 정보를 가져올 수 있는 권한을 부여합니다.	List			
GetHealthCheck	지정된 상태 확인에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	healthcheck* (p. 1500)		
GetHealthCheckCount	현재 AWS 계정과 연결된 상태 확인의 수를 가져올 수 있는 권한을 부여합니다.	List			
GetHealthCheckLastFailureReason	지정된 상태 확인이 최근에 실패한 이유를 가져올 수 있는 권한을 부여합니다.	List	healthcheck* (p. 1500)		
GetHealthCheckStatus	지정된 상태 확인의 상태를 가져올 수 있는 권한을 부여합니다.	List	healthcheck* (p. 1500)		
GetHostedZone	Route 53에서 호스팅 영역에 할당한 4개의 이름 서버를 포함하여 지정된 호스팅 영역에 대한 정보를 가져올 수 있는 권한을 부여합니다.	List	hostedzone* (p. 1500)		
GetHostedZoneCount	현재 AWS 계정과 연결된 호스팅 영역의 수를 가져올 수 있는 권한을 부여합니다.	List			
GetHostedZoneLimit	지정된 호스팅 영역에 대해 지정된 한도를 가져올 수 있는 권한을 부여합니다.	Read	hostedzone* (p. 1500)		
GetQueryLoggingConfig	DNS 쿼리 로깅에 대해 지정된 구성에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	queryloggingconfig* (p. 1500)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetReusableDelegationSet	위임 세트에 할당된 4개의 이름 서버를 포함하여 지정된 재사용 가능한 위임 세트에 대한 정보를 가져올 수 있는 권한을 부여합니다.	List	delegationset* (p. 1500)		
GetReusableDelegationSetLimit	지정된 재사용 가능한 위임 세트와 연결할 수 있는 최대 호스팅 영역 수를 가져올 수 있는 권한을 부여합니다.	Read	delegationset* (p. 1500)		
GetTrafficPolicy	지정된 트래픽 정책 버전에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	trafficpolicy* (p. 1500)		
GetTrafficPolicyInstance	지정된 트래픽 정책 인스턴스에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	trafficpolicyinstance* (p. 1500)		
GetTrafficPolicyInstanceCount	현재 AWS 계정과 연결된 트래픽 정책 인스턴스의 수를 가져올 수 있는 권한을 부여합니다.	Read			
ListGeoLocations	지리적 위치에 대해 Route 53에서 지원하는 지리적 위치의 목록을 가져올 수 있는 권한을 부여합니다.	List			
ListHealthChecks	현재 AWS 계정과 연결된 상태 확인의 목록을 가져올 수 있는 권한을 부여합니다.	List			
ListHostedZones	현재 AWS 계정과 연결된 퍼블릭 및 프라이빗 호스팅 영역의 목록을 가져올 수 있는 권한을 부여합니다.	List			
ListHostedZonesByName	사전 순서로 호스팅 영역의 목록을 가져올 수 있는 권한을 부여합니다. 호스팅 영역은 레이블을 반대로 하여 이름을 기준으로 정렬됩니다(예: com.example.www).	List			
ListQueryLoggingConfigs	현재 AWS 계정과 연결된 DNS 쿼리 로깅에 대한 구성 또는 지정된 호스팅 영역과 연결된 구성을 나열할 수 있는 권한을 부여합니다.	List	queryloggingconfig* (p. 1500)		
ListResourceRecordSets	지정된 호스팅 영역의 레코드를 나열할 수 있는 권한을 부여합니다.	List	hostedzone* (p. 1500)		
ListReusableDelegationSets	현재 AWS 계정과 연결된 재사용 가능한 위임 세트를 나열할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTagsForResource	하나의 상태 확인 또는 호스팅 영역에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	healthcheck (p. 1500)		
			hostedzone (p. 1500)		
ListTagsForResources	최대 10개의 상태 확인 또는 호스팅 영역에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	healthcheck (p. 1500)		
			hostedzone (p. 1500)		
ListTrafficPolicies	현재 AWS 계정과 연결된 모든 트래픽 정책의 최신 버전에 대한 정보를 가져올 수 있는 권한을 부여합니다. 정책은 생성된 순서로 나열됩니다.	Read			
ListTrafficPolicyInstances	현재 AWS 계정을 사용하여 생성한 트래픽 정책 인스턴스에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read			
ListTrafficPolicyInstancesByHostedZone	지정된 호스팅 영역에서 생성한 트래픽 정책 인스턴스에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	hostedzone* (p. 1500)		
ListTrafficPolicyInstancesByPolicy	지정된 트래픽 정책 버전을 사용하여 생성한 트래픽 정책 인스턴스에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	trafficpolicy* (p. 1500)		
ListTrafficPolicyVersions	지정된 트래픽 정책의 모든 버전에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	trafficpolicy* (p. 1500)		
ListVPCAssociationAuthorizations	다른 계정에서 생성되었으며 지정된 호스팅 영역과 연결할 수 있는 VPC의 목록을 가져올 수 있는 권한을 부여합니다.	Read	hostedzone* (p. 1500)		
TestDNSAnswer	지정된 레코드 이름 및 유형의 DNS 쿼리에 대한 응답으로 Route 53에서 반환하는 값을 가져올 수 있는 권한을 부여합니다.	Read			
UpdateHealthCheck	기존 상태 확인을 업데이트할 수 있는 권한을 부여합니다.	쓰기	healthcheck* (p. 1500)		
UpdateHostedZoneComment	지정된 호스팅 영역에 대한 설명을 업데이트할 수 있는 권한을 부여합니다.	쓰기	hostedzone* (p. 1500)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateTrafficPolicyComment	지정된 트래픽 정책 버전에 대한 설명을 업데이트할 수 있는 권한을 부여합니다.	쓰기	trafficpolicy* (p. 1500)		
UpdateTrafficPolicyInstance	지정된 트래픽 정책 버전의 설정에 따라 생성된 지정된 호스팅 영역의 레코드를 업데이트할 수 있는 권한을 부여합니다.	쓰기	trafficpolicyinstance* (p. 1500)		

Amazon Route 53에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1494)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
change	`arn:${Partition}:route53:::change/${Id}`	
delegationset	`arn:${Partition}:route53:::delegationset/${Id}`	
healthcheck	`arn:${Partition}:route53:::healthcheck/${Id}`	
hostedzone	`arn:${Partition}:route53:::hostedzone/${Id}`	
trafficpolicy	`arn:${Partition}:route53:::trafficpolicy/${Id}`	
trafficpolicyinstance	`arn:${Partition}:route53:::trafficpolicyinstance/${Id}`	
queryloggingconfig	`arn:${Partition}:route53:::queryloggingconfig/${Id}`	

Amazon Route 53의 조건 키

Route 53에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Route 53 Resolver에 사용되는 작업, 리소스 및 조건 키

Amazon Route 53 Resolver(서비스 접두사: `route53resolver`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Route 53 Resolver에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateResolverEndpointIpAddress	지정된 IP 주소를 해석기 엔드포인트와 연결할 수 있는 권한을 부여합니다. 이것은 DNS 쿼리가 네트워크(아웃바운드) 또는 VPC(인바운드)까지 전달되는 IP 주소입니다.	쓰기	resolver-endpoint* (p. 1503)		
AssociateResolverRule	지정된 해석기 규칙을 지정된 VPC와 연결할 수 있는 권한을 부여합니다.	쓰기	resolver-rule* (p. 1503)		
CreateResolverEndpoint	해석기 엔드포인트를 생성할 수 있는 권한을 부여합니다. 해석기 엔드포인트에는 인바운드 및 아웃바운드의 두 유형이 있습니다.	쓰기	resolver-endpoint* (p. 1503)		
CreateResolverRule	DNS 쿼리가 VPC 시작되는 경우, VPC에서 쿼리를 보내는 방법을 정의할 수 있는 권한을 부여합니다.	쓰기	resolver-rule* (p. 1503)		
DeleteResolverEndpoint	해석기 엔드포인트를 삭제할 수 있는 권한을 부여합니다. 해석기 엔드포인트를 삭제하는 효과는 인바운드 또는 아웃바운드 해석기 엔드포인트에 따라 달라집니다.	쓰기	resolver-endpoint* (p. 1503)		
DeleteResolverRule	해석기 규칙을 삭제할 수 있는 권한을 부여합니다.	쓰기	resolver-rule* (p. 1503)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DisassociateResolverEndpointIpAddress	해석기 엔드포인트에서 지정된 IP 주소를 제거할 수 있는 권한을 부여합니다. 이것은 DNS 쿼리가 네트워크(아웃바운드) 또는 VPC(인바운드)까지 전달되는 IP 주소입니다.	쓰기	resolver-endpoint* (p. 1503)		
DisassociateResolverRule	지정된 해석기 규칙과 지정된 VPC 사이의 연결을 제거할 수 있는 권한을 부여합니다.	쓰기	resolver-rule* (p. 1503)		
GetResolverEndpoint	지정된 해석기 엔드포인트에 대한 정보를 가져올 수 있는 권한을 부여합니다(해석기 엔드포인트 유형(인바운드 또는 아웃바운드), DNS 쿼리가 VPC와 사이에서 전달되는 IP 주소 등).	Read	resolver-endpoint* (p. 1503)		
GetResolverRule	지정된 해석기 규칙에 대한 정보를 가져올 수 있는 권한을 부여합니다(규칙이 DNS 쿼리를 전달하는 도메인 이름, 쿼리가 전달되는 IP 주소 등).	Read	resolver-rule* (p. 1503)		
GetResolverRuleAssociation	지정된 해석기 규칙과 VPC 사이의 연결에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	resolver-rule* (p. 1503)		
GetResolverRulePolicy	해석기 규칙 정책에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read	resolver-rule* (p. 1503)		
ListResolverEndpointIpAddresses	지정된 해석기 엔드포인트에 대해, DNS 쿼리가 네트워크(아웃바운드) 또는 VPC(인바운드)까지 전달되는 IP 주소를 나열할 수 있는 권한을 부여합니다.	List	resolver-endpoint* (p. 1503)		
ListResolverEndpoints	현재 AWS 계정을 사용하여 생성된 모든 해석기 엔드포인트를 나열할 수 있는 권한을 부여합니다.	List	resolver-endpoint* (p. 1503)		
ListResolverRuleAssociations	현재 AWS 계정을 사용하여 해석기 규칙과 VPC 사이에 생성된 연결을 나열할 수 있는 권한을 부여합니다.	List	resolver-rule* (p. 1503)		
ListResolverRules	현재 AWS 계정을 사용하여 생성된 해석기 규칙을 나열할 수 있는 권한을 부여합니다.	List	resolver-rule* (p. 1503)		
ListTagsForResource	지정된 리소스와 연결한 태그를 나열할 수 있는 권한을 부여합니다.	Read	resolver-endpoint (p. 1503)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			resolver-rule (p. 1503)		
PutResolverRulePolicy	다른 AWS 계정이 사용할 Resolver 작업 및 리소스를 지정할 수 있는 권한을 부여합니다.	쓰기	resolver-rule* (p. 1503)		
TagResource	지정된 리소스에 하나 이상의 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	resolver-endpoint (p. 1503)		
			resolver-rule (p. 1503)		
UntagResource	지정된 리소스에서 하나 이상의 태그를 제거할 수 있는 권한을 부여합니다.	태그 지정	resolver-endpoint (p. 1503)		
			resolver-rule (p. 1503)		
UpdateResolverEndpoint	인바운드 또는 아웃바운드 해석기 엔드포인트에 대해 선택된 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기	resolver-endpoint* (p. 1503)		
UpdateResolverRule	지정된 해석기 규칙에 대한 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기	resolver-rule* (p. 1503)		

Amazon Route 53 Resolver에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1501)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
resolver-rule	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-rule/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1504)
resolver-endpoint	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-endpoint/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1504)

Amazon Route 53 Resolver에 사용되는 조건 키

Amazon Route 53 Resolver는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon Route53 Domains에 사용되는 작업, 리소스 및 조건 키

Amazon Route53 Domains(서비스 접두사: `route53domains`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Route53 Domains에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CheckDomainAvailability	한 도메인 이름의 가용성을 확인할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteTagsForDomain	도메인에 대해 지정된 태그를 삭제할 수 있는 권한을 부여합니다.	태그 지정			
DisableDomainAutoRenew	도메인 등록이 만료되기 전에 지정된 도메인을 자동으로 갱신하도록 Amazon Route 53을 구성할 수 있는 권한을 부여합니다.	쓰기			
DisableDomainTransferLock	도메인에 대한 이전 잠금(특히 clientTransferProhibited 상태)을 제거하여 도메인 이전을 허용할 수 있는 권한을 부여합니다.	쓰기			
EnableDomainAutoRenew	도메인 등록이 만료되기 전에 지정된 도메인을 자동으로 갱신하도록 Amazon Route 53을 구성할 수 있는 권한을 부여합니다.	쓰기			
EnableDomainTransferLock	도메인에 대한 이전 잠금(특히 clientTransferProhibited 상태)을 설정하여 도메인 이전을 방지할 수 있는 권한을 부여합니다.	쓰기			
GetContactReachabilityStatus	새 도메인 등록과 같이 등록자 연락처의 이메일 주소가 유효한지 확인해야 하는 작업의 경우, 등록자 연락처의 응답 여부에 대한 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetDomainDetail	도메인에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	Read			
GetDomainSuggestions	도메인 이름이나 단순히 단어 또는 구(공백 제외)일 수 있는 문자열이 제공된 경우, 제안된 도메인 이름의 목록을 가져올 수 있는 권한을 부여합니다.	Read			
GetOperationDetail	완료되지 않은 작업의 현재 상태를 가져올 수 있는 권한을 부여합니다.	Read			
ListDomains	현재 AWS 계정에 대해 Amazon Route 53에 등록된 모든 도메인 이름을 나열할 수 있는 권한을 부여합니다.	List			
ListOperations	아직 완료되지 않은 작업의 ID를 나열할 수 있는 권한을 부여합니다.	List			
ListTagsForDomain	지정된 도메인과 연결된 모든 태그를 나열할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RegisterDomain	도메인을 등록할 수 있는 권한을 부여합니다.	쓰기			
RenewDomain	지정된 연수에 따라 도메인을 갱신할 수 있는 권한을 부여합니다.	쓰기			
ResendContactReachabilityEmail	새 도메인 등록과 같이 등록자 연락처의 이메일 주소가 유효한지 확인해야 하는 작업의 경우, 확인 이메일을 등록자 연락처의 현재 이메일 주소로 재전송할 수 있는 권한을 부여합니다.	쓰기			
RetrieveDomainAuthCode	도메인의 AuthCode를 가져올 수 있는 권한을 부여합니다.	쓰기			
TransferDomain	다른 등록 기관의 도메인을 Amazon Route 53로 이전할 수 있는 권한을 부여합니다.	쓰기			
UpdateDomainContact	도메인의 연락처 정보를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateDomainContactPrivacy	도메인 연락처 개인 정보 보호 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateDomainNameservers	도메인에 대한 현재 이름 서버 세트를 지정된 이름 서버 세트로 바꿀 수 있는 권한을 부여합니다.	쓰기			
UpdateTagsForDomain	지정된 도메인에 대한 태그를 추가 또는 업데이트할 수 있는 권한을 부여합니다.	태그 지정			
ViewBilling	지정된 기간 동안 현재 AWS 계정에 대한 모든 도메인 관련 결제 레코드를 반환할 수 있는 권한을 부여합니다.	Read			

Amazon Route53 Domains에서 정의한 리소스 유형

Amazon Route53 Domains는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Route53 Domains에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Route53 Domains의 조건 키

Route53 Domains에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon S3에 사용되는 작업, 리소스 및 조건 키

Amazon S3(서비스 접두사: `s3`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon S3에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AbortMultipartUpload	멀티파트 업로드를 중단합니다.	쓰기	object* (p. 1556)		
				s3:DataAccessPointArn (p. 1557) s3:DataAccessPointAccount (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:x-amz-content-sha256 (p. 1558)	
BypassGovernanceRetention	거버넌스 모드 객체 보존 설정의 우회를 허용합니다.	권한 관리	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:RequestObjectTag/<key> (p. 1557) s3:RequestObjectTagKeys (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-acl (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:x-amz-copy-source (p. 1558) s3:x-amz-grant-full-control (p. 1558) s3:x-amz-grant-read (p. 1558) s3:x-amz-grant-read-acp (p. 1558) s3:x-amz-grant-write (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:x-amz-grant-write-acp (p. 1558) s3:x-amz-metadata-directive (p. 1558) s3:x-amz-server-side-encryption (p. 1558) s3:x-amz-server-side-encryption-aws-kms-key-id (p. 1558) s3:x-amz-storage-class (p. 1558) s3:x-amz-website-redirect-location (p. 1558) s3:object-lock-mode (p. 1557) s3:object-lock-retain-until-date (p. 1558) s3:object-lock-remaining-retention-days (p. 1558) s3:object-lock-legal-hold (p. 1557)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateAccessPoint	새 액세스 포인트를 생성합니다.	쓰기	accesspoint* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:locationconstraint (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-acl (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
CreateBucket	새 버킷을 만듭니다.	쓰기	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:locationconstraint (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-acl (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:x-amz-grant-full-control (p. 1558) s3:x-amz-grant-read (p. 1558) s3:x-amz-grant-read-acp (p. 1558) s3:x-amz-grant-write (p. 1558) s3:x-amz-grant-write-acp (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateJob	새 Amazon S3 Batch Operations 작업을 생성합니다.	쓰기		s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:RequestJobPriority (p. 1557) s3:RequestJobOperation (p. 1557)	
DeleteAccessPoint	URI에 명명된 액세스 포인트를 삭제합니다.	쓰기	accesspoint* (p. 1556)		
				s3:DataAccessPointArn (p. 1557) s3:DataAccessPointAccount (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
DeleteAccessPointPolicy	지정된 액세스 포인트에서 정책을 삭제합니다.	권한 관리	accesspoint* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointArn (p. 1557) s3:DataAccessPointAccount (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
DeleteBucket	URI에 이름을 올린 버킷을 삭제합니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
DeleteBucketPolicy	지정된 버킷에서 정책을 삭제합니다.	권한 관리	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteBucketWebsite	버킷에 대한 웹 사이트 구성을 제거합니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
DeleteObject	객체의 널(null) 버전(있는 경우)을 제거하고 삭제 마커를 삽입합니다(그러면 삭제 마커가 객체의 현재 버전이 됩니다).	쓰기	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
DeleteObjectTagging	DELETE 작업의 이 구현은 태깅 하위 자원을 사용하여 지정된 객체에서 전체 태그 집합을 제거합니다.	태그 지정	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
DeleteObjectVersion	객체의 지정된 버전을 제거하려면 버킷 소유자여야 하고 versionId 하위 자원을 사용해야 합니다.	쓰기	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:versionid (p. 1558) s3:x-amz-content-sha256 (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteObjectVersionTagging	DELETE Object 태그 지정(특정 버전의 객체용)	태그 지정	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:versionid (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
DescribeJob	Amazon S3 Batch Operations 작업에 대한 구성 파라미터 및 상태를 검색합니다.	Read	job* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetAccelerateConfiguration	GET 작업의 이 구현은 가속화 하위 자원을 사용하여 버킷의 Transfer Acceleration 상태(활성 또는 일시 중지됨)를 반환합니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetAccessPoint	액세스 포인트 메타데이터를 검색합니다.	Read		s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetAccessPointPolicy	지정된 액세스 포인트의 정책을 반환합니다.	Read	accesspoint* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetAccessPointPolicyStatus	특정 액세스 포인트의 정책에 대한 정책 상태를 검색합니다.	Read	accesspoint* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetAccountPublicAccessBlock	AWS 계정에 대한 PublicAccessBlock 구성을 검색합니다.	Read		s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetAnalyticsConfiguration	GET 작업의 이 구현은 버킷에서 분석 구성(분석 구성 ID로 식별됨)을 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketAcl	버킷의 ACL(액세스 제어 목록)을 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketCORS	버킷에 대한 CORS 정보 집합을 반환합니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketLocation	버킷의 리전을 반환합니다.	Read	bucket* (p. 1556)		
GetBucketLogging	사용자가 해당 상태를 보고 수정해야 하는 버킷 및 권한의 로깅 상태를 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketNotification	버킷의 알림 구성을 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketObjectLockConfiguration	특정 버킷에 대한 객체 잠금 구성을 가져옵니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558)	
GetBucketPolicy	지정된 버킷의 정책을 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketPolicyStatus	특정 S3 버킷에 대해 해당 버킷이 퍼블릭임을 나타내는 정책 상태를 검색합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketPublicAccessBlock	특정 S3 버킷에 대한 PublicAccessBlock 구성을 검색합니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketRequestPayment	버킷의 결제 요청 구성을 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketTagging	버킷과 연결된 태그 집합을 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketVersioning	버킷의 버전 관리 상태를 반환합니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetBucketWebsite	버킷과 연결된 웹 사이트 구성을 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetEncryptionConfiguration	버킷에 설정된 암호화 구성 정보를 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetInventoryConfiguration	GET 작업의 이 구현은 버킷에서 인벤토리 구성(인벤토리 구성 ID로 식별됨)을 반환합니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetLifecycleConfiguration	버킷에 설정된 수명 주기 구성 정보를 반환합니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetMetricsConfiguration	버킷의 CloudWatch 요청 지표(지표 구성 ID로 지정)에 대한 지표 구성을 가져옵니다. 단, 여기에 일간 스토리지 지표는 포함되지 않습니다.	Read	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObject	Amazon S3에서 객체를 검색합니다.	Read	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObjectAcl	객체의 ACL(액세스 제어 목록)을 반환합니다.	Read	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetObjectLegalHold	특정 객체에 대한 객체 법적 보존을 가져옵니다.	Read	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObjectRetention	특정 객체에 대한 객체 법적 보존을 가져옵니다.	Read	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetObjectTagging	GET 작업의 이 구현은 객체와 연결된 태그를 반환합니다. 그러면 객체와 연결된 태깅 하위 리소스에 대한 GET 요청을 보낼 수 있습니다.	Read	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObjectTorrent	버킷에서 토렌트 파일을 반환합니다.	Read	object* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObjectVersion	여러 다른 버전을 반환하려면 versionId 하위 리소스를 사용합니다.	Read	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:versionid (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObjectVersionAcl	여러 다른 버전에 대한 ACL 정보를 반환하려면 versionId 하위 리소스를 사용합니다.	Read	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:versionid (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObjectVersionForReplication	S3 복제에서 수행된 권한	Read	object* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObjectVersionTagging	GET Object 태그 지정(특정 버전의 객체에 적용)	Read	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:versionid (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetObjectVersionTorrent	여러 다른 버전에 대한 Torrent 파일을 반환하려면 versionId 하위 리소스를 사용합니다.	Read	object* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:versionid (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
GetReplicationConfiguration	버킷에 설정된 복제 구성 정보를 반환합니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ListAccessPoints	액세스 포인트를 나열합니다.	Read		s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ListAllMyBuckets	요청의 인증된 발신자가 소유한 모든 버킷의 목록을 반환합니다.	List		s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ListBucket	버킷의 객체를 일부 또는 전부(최대 1,000개) 반환합니다.	List	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:delimiter (p. 1557) s3:max-keys (p. 1557) s3:prefix (p. 1558) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ListBucketMultipartUploads	진행 중인 멀티파트 업로드를 나열합니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ListBucketVersions	버전 하위 리소스를 사용하여 버킷에 있는 객체의 모든 버전에 대한 메타데이터를 나열합니다.	Read	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:delimiter (p. 1557) s3:max-keys (p. 1557) s3:prefix (p. 1558) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ListJobs	현재 작업 및 최근 종료된 작업을 나열합니다.	Read		s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ListMultipartUploadParts	특정 멀티파트 업로드에 대해 업로드된 파트를 나열합니다.	Read	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ObjectOwnerOverrideToBucketOwner	S3 복제에서 수행된 권한	권한 관리	object* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutAccelerateConfiguration	PUT 작업의 이 구현은 가속화 하위 자원을 사용하여 기존 버킷의 Transfer Acceleration 상태를 설정합니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutAccessPointPolicy	액세스 포인트에 대한 데이터 정책을 추가하거나 바꿉니다.	권한 관리	accesspoint* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutAccountPublicAccessBlock	AWS 계정에 대한 PublicAccessBlock 구성을 생성 또는 수정합니다.	권한 관리		s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutAnalyticsConfiguration	PUT 작업의 이 구현은 버킷에 분석 구성(분석 ID로 식별됨)을 추가합니다. 버킷당 최대 1,000개의 분석 구성을 설정할 수 있습니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutBucketAcl	ACL(액세스 제어 목록)을 사용하여 기존 버킷에 대한 권한을 설정합니다.	권한 관리	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-acl (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:x-amz-grant-full-control (p. 1558) s3:x-amz-grant-read (p. 1558) s3:x-amz-grant-read-acp (p. 1558) s3:x-amz-grant-write (p. 1558) s3:x-amz-grant-write-acp (p. 1558)	
PutBucketCORS	버킷에 대한 CORS 구성을 설정합니다.	쓰기	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutBucketLogging	버킷에 대한 로깅 파라미터를 설정합니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutBucketNotification	버킷에서 특정 이벤트가 발생할 때 알림을 받을 수 있습니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutBucketObjectLockConfiguration	특정 버킷에 대한 객체 잠금 구성을 배포합니다.	쓰기	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558)	
PutBucketPolicy	버킷에 대한 정책을 추가하거나 대체합니다.	권한 관리	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutBucketPublicAccessBlock	특정 S3 버킷에 대한 PublicAccessBlock 구성을 생성 또는 수정합니다.	권한 관리	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutBucketRequestPayment	버킷의 결제 요청 구성을 설정합니다.	쓰기	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutBucketTagging	기존 버킷에 태그 집합을 추가합니다.	태그 지정	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutBucketVersioning	기존 버킷의 버전 관리 상태를 설정합니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutBucketWebsite	웹 사이트 하위 리소스에 지정된 웹사이트의 구성을 설정합니다.	쓰기	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutEncryptionConfiguration	버킷에 대한 암호화 구성을 설정합니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutInventoryConfiguration	PUT 작업의 이 구현은 버킷에 인벤토리 구성(인벤토리 ID로 식별됨)을 추가합니다. 버킷당 최대 1,000개의 인벤토리 구성을 설정할 수 있습니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutLifecycleConfiguration	버킷에 새로운 수명 주기 구성을 생성하거나 기존 수명 주기 구성을 대체합니다.	쓰기	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutMetricsConfiguration	버킷의 CloudWatch 요청 지표(지표 구성 ID로 지정)에 대한 지표 구성을 설정하거나 업데이트합니다.	쓰기	bucket* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutObject	버킷에 객체를 추가합니다.	쓰기	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:RequestObjectTag/<key> (p. 1557) s3:RequestObjectTagKeys (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-acl (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:x-amz-copy-source (p. 1558) s3:x-amz-grant-full-control (p. 1558) s3:x-amz-grant-read (p. 1558) s3:x-amz-grant-read-acp (p. 1558) s3:x-amz-grant-write (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:x-amz-grant-write-acp (p. 1558) s3:x-amz-metadata-directive (p. 1558) s3:x-amz-server-side-encryption (p. 1558) s3:x-amz-server-side-encryption-aws-kms-key-id (p. 1558) s3:x-amz-storage-class (p. 1558) s3:x-amz-website-redirect-location (p. 1558) s3:object-lock-mode (p. 1557) s3:object-lock-retain-until-date (p. 1558) s3:object-lock-remaining-retention-days (p. 1558) s3:object-lock-legal-hold (p. 1557)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutObjectAcl	버킷에 이미 존재하는 객체에 대한 ACL(액세스 제어 목록) 권한을 설정합니다.	권한 관리	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-acl (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:x-amz-grant-full-control (p. 1558) s3:x-amz-grant-read (p. 1558) s3:x-amz-grant-read-acp (p. 1558) s3:x-amz-grant-write (p. 1558) s3:x-amz-grant-write-acp (p. 1558) s3:x-amz-storage-	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				class (p. 1558)	
PutObjectLegalHold	특정 객체에 대한 객체 법적 보존을 내보냅니다.	쓰기	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:object-lock-legal-hold (p. 1557)	
PutObjectRetention	특정 객체에 대한 객체 보존을 내보냅니다.	쓰기	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:object-lock-mode (p. 1557) s3:object-lock-retain-until-date (p. 1558) s3:object-lock-remaining-retention-days (p. 1558)	
PutObjectTagging	PUT 작업의 이 구현은 태깅 하위 자원을 사용하여 기존 객체에 태그 집합을 추가합니다.	태그 지정	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:RequestObjectTag/<key> (p. 1557) s3:RequestObjectTagKeys (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutObjectVersionAcl	객체의 ACL은 객체 버전 수준에서 설정됩니다.	권한 관리	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:versionid (p. 1558) s3:x-amz-acl (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:x-amz-grant-full-control (p. 1558) s3:x-amz-grant-read (p. 1558) s3:x-amz-grant-read-acp (p. 1558) s3:x-amz-grant-write (p. 1558) s3:x-amz-grant-write-acp (p. 1558)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:x-amz-storage-class (p. 1558)	
PutObjectVersionTagging	PUT Object 태그 지정(특정 버전의 객체에 적용)	태그 지정	object* (p. 1556)		
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:ExistingObjectTag/<key> (p. 1557) s3:RequestObjectTag/<key> (p. 1557) s3:RequestObjectTagKeys (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:versionid (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
PutReplicationConfiguration	버전 관리를 사용하는 버킷에서 이 작업을 새로운 복제 구성을 생성합니다(또는 기존 구성(있는 경우)을 대체합니다).	쓰기	bucket* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ReplicateDelete	S3 복제에서 수행된 권한	쓰기	object* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
ReplicateObject	S3 복제에서 수행된 권한	쓰기	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:x-amz-server-side-encryption (p. 1558) s3:x-amz-server-side-encryption-aws-kms-key-id (p. 1558)	
ReplicateTags	S3 복제에서 수행된 권한	태그 지정	object* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
RestoreObject	아카이브된 객체의 임시 사본을 복원합니다.	쓰기	object* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:DataAccessPointAccount (p. 1557) s3:DataAccessPointArn (p. 1557) s3:AccessPointNetworkOrigin (p. 1557) s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558)	
UpdateJobPriority	기존 작업의 우선 순위를 업데이트합니다.	쓰기	job* (p. 1556)		
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:RequestJobPriority (p. 1557) s3:ExistingJobPriority (p. 1557) s3:ExistingJobOperation (p. 1557)	
UpdateJobStatus	지정된 작업의 상태를 업데이트합니다.	쓰기	job* (p. 1556)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				s3:authtype (p. 1557) s3:signatureage (p. 1558) s3:signatureversion (p. 1558) s3:x-amz-content-sha256 (p. 1558) s3:ExistingJobPriority (p. 1557) s3:ExistingJobOperation (p. 1557) s3:JobSuspendedCause (p. 1557)	

Amazon S3에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1507)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
accesspoint	`arn:${Partition}:s3:${Region}:${Account}:accesspoint/${AccessPointName}`	
bucket	`arn:${Partition}:s3:::${BucketName}`	
object	`arn:${Partition}:s3:::${BucketName}/${ObjectName}`	
job	`arn:${Partition}:s3:${Region}:${Account}:job/${JobId}`	

Amazon S3에 사용되는 조건 키

Amazon S3는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
s3:AccessPointNetworkOrigin	요청과 관련된 액세스 포인트에서 수신할 수 있는 트래픽의 네트워크 유형	문자열
s3:DataAccessPointAccount	요청과 관련된 데이터 작업 액세스 포인트를 소유하는 계정의 AWS 계정 ID	문자열
s3:DataAccessPointArn	요청과 관련된 데이터 작업 액세스 포인트의 ARN	문자열
s3:ExistingJobOperation		문자열
s3:ExistingJobPriority		숫자
s3:ExistingObjectTag/<key>	기존 객체 태그에 특정 태그 키 및 값이 있다는 것을 확인할 수 있습니다.	문자열
s3:JobSuspendedCause		문자열
s3:LocationConstraint	사용자가 특정 리전에서만 버킷을 만들도록 제한할 수 있습니다.	문자열
s3:RequestJobOperation		문자열
s3:RequestJobPriority		숫자
s3:RequestObjectTag/<key>	객체에 대해 허용하고자 하는 태그 키 및 값을 제한합니다.	문자열
s3:RequestObjectTagKeys	객체에 대해 허용하고자 하는 태그 키를 제한합니다.	문자열
s3:VersionId	s3:PutObjectVersionTagging 작업에 대한 권한을 특정 객체 버전으로 제한할 수 있습니다.	문자열
s3:authtype		문자열
s3:delimiter	사용자에게 GET Bucket Object versions 요청에 구분 기호 파라미터를 지정하도록 요구할 수 있습니다.	문자열
s3:locationconstraint	사용자가 특정 리전에서만 버킷을 만들도록 제한할 수 있습니다.	문자열
s3:max-keys	사용자에게 max-keys(최대 키 개수) 파라미터를 지정하도록 요구함으로써 ListBucket 요청에 대한 응답으로 Amazon S3가 반환하는 키의 개수를 제한할 수 있습니다.	숫자
s3:object-lock-legal-hold	지정된 객체 법적 보존 상태를 강제 적용합니다.	문자열
s3:object-lock-mode	지정된 객체 보존 모드를 강제 적용합니다.	문자열

조건 키	설명	유형
s3:object-lock-remaining-retention-days	남은 보존 일수를 기준으로 객체를 강제 적용합니다.	문자열
s3:object-lock-retain-until-date	특정 retain-until-date를 강제 적용합니다.	문자열
s3:prefix	ListBucket API의 응답을 키 이름에 특정 접두사가 있는 경우로 제한할 수 있습니다.	문자열
s3:signatureage		숫자
s3:signatureversion		문자열
s3:versionid		문자열
s3:x-amz-acl	객체를 업로딩할 때 특정 액세스 권한을 요구할 수 있습니다.	문자열
s3:x-amz-content-sha256		문자열
s3:x-amz-copy-source	복사 원본을 특정 버킷, 버킷의 특정 폴더 또는 버킷의 특정 객체로 제한할 수 있습니다.	문자열
s3:x-amz-grant-full-control		문자열
s3:x-amz-grant-read		문자열
s3:x-amz-grant-read-acp		문자열
s3:x-amz-grant-write		문자열
s3:x-amz-grant-write-acp		문자열
s3:x-amz-metadata-directive	객체가 업로드될 때 특정 동작(COPY 또는 REPLACE)을 강제로 실행할 수 있습니다.	문자열
s3:x-amz-server-side-encryption	사용자가 업로드한 객체를 저장할 때 암호화하도록 요청에 이 헤더를 지정하도록 사용자에게 요구할 수 있습니다.	문자열
s3:x-amz-server-side-encryption-aws-kms-key-id		문자열
s3:x-amz-storage-class		문자열
s3:x-amz-website-redirect-location		문자열

Amazon SageMaker에 사용되는 작업, 리소스 및 조건 키

Amazon SageMaker(서비스 접두사: `sagemaker`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon SageMaker에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTags	지정된 Amazon SageMaker 리소스에 대한 하나 이상의 태그를 추가하거나 덮어씁니다.	태그 지정	app (p. 1585)		
			automl-job (p. 1586)		
			domain (p. 1585)		
			endpoint (p. 1586)		
			endpoint-config (p. 1586)		
			experiment (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			experiment-trial (p. 1587)		
			experiment-trial-component (p. 1587)		
			flow-definition (p. 1584)		
			human-task-ui (p. 1584)		
			hyper-parameter-tuning-job (p. 1586)		
			labeling-job (p. 1584)		
			model (p. 1586)		
			monitoring-schedule (p. 1586)		
			notebook-instance (p. 1585)		
			processing-job (p. 1585)		
			training-job (p. 1585)		
			transform-job (p. 1586)		
			user-profile (p. 1585)		
			workteam (p. 1584)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	
AssociateTrialComponent	시도 구성 요소를 시도와 연결합니다.	쓰기	experiment-trial* (p. 1587)		
			experiment-trial-component* (p. 1587)		
BatchGetMetrics [권한만 해당]	훈련 작업과 같은 SageMaker 리소스와 연결된 지표를 검색합니다. 이 API는 현재 공개적으로 노출되어 있지 않지만, 관리자는 이 작업을 제어 할 수 있습니다.	Read	training-job* (p. 1585)		
BatchPutMetrics [권한만 해당]	훈련 작업과 같은 SageMaker 리소스와 연결된 지표를 게시합니다. 이 API는 현재 공개적으로 노출되어 있지 않지만, 관리자는 이 작업을 제어 할 수 있습니다.	쓰기	training-job* (p. 1585)		
CreateAlgorithm	알고리즘을 생성합니다.	쓰기	algorithm* (p. 1585)		
CreateApp	SageMaker Studio UserProfile에 대한 애플리케이션을 생성할 수 있는 권한을 부여합니다.	쓰기	app* (p. 1585)		
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:InstanceTypes (p. 1588)	
CreateAutoMLJob	AutoML 작업을 생성합니다.	쓰기	automl-job* (p. 1586)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:InterContainerTrafficEncryp (p. 1588) sagemaker:OutputKmsKey (p. 1588) sagemaker:VolumeKmsKey (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588)	
CreateCodeRepository	코드 리포지토리를 생성합니다.	쓰기	code-repository* (p. 1585)		
CreateCompilationJob	컴파일 작업 생성	쓰기	compilation-job* (p. 1586)		iam:PassRole
CreateDomain	SageMaker Studio에 대한 도메인을 생성할 수 있는 권한을 부여합니다.	쓰기	domain* (p. 1585)		iam:CreateServiceLinkedI iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:AppNetworkAccess (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588) sagemaker:DomainSharingOutputKmsK (p. 1587) sagemaker:HomeEfsFileSystemKmsKe (p. 1588)	
CreateEndpoint	요청에 지정된 엔드포인트 구성을 사용하여 엔드포인트를 생성합니다.	쓰기	endpoint* (p. 1586)		
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	
CreateEndpointConfig	Amazon SageMaker 호스팅 서비스를 사용하여 배포할 수 있는 엔드포인트 구성을 생성합니다.	쓰기	endpoint-config* (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:AcceleratorTypes (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:ModelArn (p. 1588) sagemaker:VolumeKmsKey (p. 1588)	
CreateExperiment	실험을 생성합니다.	쓰기	experiment* (p. 1586)		
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	
CreateFlowDefinition	인적 워크플로우에 대한 설정을 정의하는 흐름 정의를 생성합니다.	쓰기	flow-definition* (p. 1584)		iam:PassRole
				sagemaker:WorkteamArn (p. 1588) sagemaker:WorkteamType (p. 1588) aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	
CreateHumanTaskUi	인적 검토 워크플로우 사용자 인터페이스에 사용할 설정을 정의합니다.	쓰기	human-task-ui* (p. 1584)		
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateHyperParameterTuningJob	Amazon SageMaker를 사용하여 배포할 수 있는 하이퍼 파라미터 튜닝 작업을 생성합니다.	쓰기	hyper-parameter-tuning-job* (p. 1586)		iam:PassRole
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:FileSystemAccessMode (p. 1587) sagemaker:FileSystemDirectoryPath (p. 1587) sagemaker:FileSystemId (p. 1587) sagemaker:FileSystemType (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:InterContainerTrafficEncryp (p. 1588) sagemaker:MaxRuntimeInSeconds (p. 1588) sagemaker:NetworkIsolation (p. 1588) sagemaker:OutputKmsKey (p. 1588) sagemaker:VolumeKmsKey (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateLabelingJob	레이블 지정 작업을 시작합니다. 레이블 지정 작업은 레이블이 지정되지 않은 데이터를 가져와 SageMaker 모델을 훈련하는 데 사용할 수 있는 레이블이 지정된 데이터를 출력으로 생성합니다.	쓰기	labeling-job* (p. 1584)		iam:PassRole
				sagemaker:WorkteamArn (p. 1588) sagemaker:WorkteamType (p. 1588) sagemaker:VolumeKmsKey (p. 1588) sagemaker:OutputKmsKey (p. 1588) aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	
CreateModel	Amazon SageMaker에서 모델을 생성합니다. 요청에서, 모델의 이름을 지정하고 하나 이상의 컨테이너를 설명합니다.	쓰기	model* (p. 1586)		iam:PassRole
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:NetworkIsolation (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588)	
CreateModelPackage	모델 패키지를 생성합니다.	쓰기	model-package* (p. 1586)		
CreateMonitoringSchedule	모니터링 일정을 생성합니다.	쓰기	monitoring-schedule* (p. 1586)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:MaxRuntimeInSeconds (p. 1588) sagemaker:NetworkIsolation (p. 1588) sagemaker:OutputKmsKey (p. 1588) sagemaker:VolumeKmsKey (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588)	
CreateNotebookInstance	Amazon SageMaker 노트북 인스턴스를 생성합니다. 노트북 인스턴스는 Jupyter 노트북에서 실행하는 Amazon EC2 인스턴스입니다.	쓰기	notebook-instance* (p. 1585)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:AcceleratorTypes (p. 1587) sagemaker:DirectInternetAccess (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:RootAccess (p. 1588) sagemaker:VolumeKmsKey (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588)	
CreateNotebookInstanceLifecycleConfig	Amazon SageMaker를 사용하여 배포할 수 있는 노트북 인스턴스 수명 주기 구성을 생성합니다.	쓰기	notebook-instance-lifecycle-config* (p. 1585)		
CreatePresignedDomainUrl	AuthMode가 'IAM'일 때 브라우저에서 지정된 UserProfile로 도메인을 연결하는 데 사용할 수 있는 URL을 반환할 수 있는 권한을 부여합니다.	쓰기	user-profile* (p. 1585)		
CreatePresignedNotebookInstanceUrl	노트북 인스턴스에 연결하기 위해 브라우저에서 사용할 수 있는 URL을 반환합니다.	쓰기	notebook-instance* (p. 1585)		
CreateProcessingJob	처리 작업을 시작합니다. 훈련이 완료된 후, Amazon SageMaker는 결과로 생성된 아티팩트 및 기타 선택적 출력을 지정된 Amazon S3 위치에 저장합니다.	쓰기	processing-job* (p. 1585)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:MaxRuntimeInSeconds (p. 1588) sagemaker:NetworkIsolation (p. 1588) sagemaker:OutputKmsKey (p. 1588) sagemaker:VolumeKmsKey (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588)	
CreateTrainingJob	모델 훈련 작업을 시작합니다. 훈련이 완료된 후, Amazon SageMaker는 결과로 생성된 모델 아티팩트 및 기타 선택적 출력을 지정하는 Amazon S3 위치에 저장합니다.	쓰기	training-job* (p. 1585)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:FileSystemAccessMode (p. 1587) sagemaker:FileSystemDirectoryPath (p. 1587) sagemaker:FileSystemId (p. 1587) sagemaker:FileSystemType (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:InterContainerTrafficEncryp (p. 1588) sagemaker:MaxRuntimeInSeconds (p. 1588) sagemaker:NetworkIsolation (p. 1588) sagemaker:OutputKmsKey (p. 1588) sagemaker:VolumeKmsKey (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588)	
CreateTransformJob	변환 작업을 시작합니다. 결과를 확득한 후 Amazon SageMaker는 사용자가 지정한 Amazon S3 위치에 결과를 저장합니다.	쓰기	transform-job* (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:ModelArn (p. 1588) sagemaker:OutputKmsKey (p. 1588) sagemaker:VolumeKmsKey (p. 1588)	
CreateTrial	시도를 생성합니다.	쓰기	experiment-trial* (p. 1587)		
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	
CreateTrialComponent	시도 구성 요소를 생성합니다.	쓰기	experiment-trial-component* (p. 1587)		
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	
CreateUserProfile	SageMaker Studio 도메인에 대한 UserProfile을 생성할 수 있는 권한을 부여합니다.	쓰기	user-profile* (p. 1585)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:InstanceTypes (p. 1588) sagemaker:DomainSharingOutputKmsK (p. 1587)	
CreateWorkteam	작업 팀을 생성합니다.	쓰기	workteam* (p. 1584)		
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587)	
DeleteAlgorithm	알고리즘을 삭제합니다.	쓰기	algorithm* (p. 1585)		
DeleteApp	앱을 삭제할 수 있는 권한을 부여합니다.	쓰기	app* (p. 1585)		
DeleteCodeRepository	코드 리포지토리를 삭제합니다.	쓰기	code-repository* (p. 1585)		
DeleteDomain	도메인을 삭제할 수 있는 권한을 부여합니다.	쓰기	domain* (p. 1585)		
DeleteEndpoint	엔드포인트를 삭제합니다. Amazon SageMaker는 엔드포인트가 생성될 때 배포된 모든 리소스를 확보합니다.	쓰기	endpoint* (p. 1586)		
DeleteEndpointConfig	CreateEndpointConfig API를 사용하여 생성된 엔드포인트 구성을 삭제합니다. DeleteEndpointConfig API는 지정된 구성만 삭제합니다. 구성을 사용하여 생성된 엔드포인트는 삭제하지 않습니다.	쓰기	endpoint-config* (p. 1586)		
DeleteExperiment	실험을 삭제합니다.	쓰기	experiment* (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteFlowDefinition	지정된 흐름 정의를 삭제합니다.	쓰기	flow-definition* (p. 1584)		
DeleteHumanLoop	지정된 인적 루프를 삭제합니다.	쓰기	human-loop* (p. 1584)		
DeleteModel	CreateModel API를 사용하여 생성된 모델을 삭제합니다. DeleteModel API는 CreateModel API를 호출하여 생성한 Amazon SageMaker 내 모델 항목만 삭제합니다. 모델 아티팩트, 추론 코드 또는 모델을 생성할 때 지정한 IAM 역할은 삭제하지 않습니다.	쓰기	model* (p. 1586)		
DeleteModelPackage	모델 패키지를 삭제합니다.	쓰기	model-package* (p. 1586)		
DeleteMonitoringSchedule	모니터링 일정을 삭제합니다. Amazon SageMaker는 더 이상 예약된 모니터링을 실행하지 않습니다.	쓰기	monitoring-schedule* (p. 1586)		
DeleteNotebookInstance	Amazon SageMaker 노트북 인스턴스를 삭제합니다. 노트북 인스턴스를 삭제하려면 먼저 StopNotebookInstance API를 호출해야 합니다.	쓰기	notebook-instance* (p. 1585)		
DeleteNotebookInstanceLifecycleConfig	Amazon SageMaker를 사용하여 배포할 수 있는 노트북 인스턴스 수명 주기 구성을 삭제합니다.	쓰기	notebook-instance-lifecycle-config* (p. 1585)		
DeleteTags	Amazon SageMaker 리소스에서 지정된 태그 세트를 삭제합니다.	태그 지정	app (p. 1585)		
			automl-job (p. 1586)		
			compilation-job (p. 1586)		
			domain (p. 1585)		
			endpoint (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			endpoint-config (p. 1586)		
			experiment (p. 1586)		
			experiment-trial (p. 1587)		
			experiment-trial-component (p. 1587)		
			flow-definition (p. 1584)		
			human-task-ui (p. 1584)		
			hyper-parameter-tuning-job (p. 1586)		
			labeling-job (p. 1584)		
			model (p. 1586)		
			monitoring-schedule (p. 1586)		
			notebook-instance (p. 1585)		
			processing-job (p. 1585)		
			training-job (p. 1585)		
			transform-job (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			user-profile (p. 1585)		
			workteam (p. 1584)		
				aws:TagKeys (p. 1587)	
DeleteTrial	시도를 삭제합니다.	쓰기	experiment-trial* (p. 1587)		
DeleteTrialComponent	시도 구성 요소를 삭제합니다.	쓰기	experiment-trial-component* (p. 1587)		
DeleteUserProfile	UserProfile을 삭제할 수 있는 권한을 부여합니다.	쓰기	user-profile* (p. 1585)		
DeleteWorkteam	작업 팀을 삭제합니다.	쓰기	workteam* (p. 1584)		
DescribeAlgorithm	알고리즘에 대한 정보를 반환합니다.	Read	algorithm* (p. 1585)		
DescribeApp	앱을 설명할 수 있는 권한을 부여합니다.	Read	app* (p. 1585)		
DescribeAutoMLJob	CreateAutoMLJob API를 통해 생성된 AutoML 작업에 대해 설명합니다.	Read	automl-job* (p. 1586)		
DescribeCodeRepository	코드 리포지토리에 대한 정보를 반환합니다.	Read	code-repository* (p. 1585)		
DescribeCompilationJob	컴파일 작업에 대한 정보를 반환합니다.	Read	compilation-job* (p. 1586)		
DescribeDomain	도메인을 설명할 수 있는 권한을 부여합니다.	Read	domain* (p. 1585)		
DescribeEndpoint	엔드포인트의 설명을 반환합니다.	Read	endpoint* (p. 1586)		
DescribeEndpointConfig	CreateEndpointConfig API를 사용하여 생성된 엔드포인트 구성의 설명을 반환합니다.	Read	endpoint-config* (p. 1586)		
DescribeExperiment	실험에 대한 정보를 반환합니다.	Read	experiment* (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeFlowDefinition	지정된 흐름 정의에 대한 자세한 정보를 반환합니다.	Read	flow-definition* (p. 1584)		
DescribeHumanLoop	지정된 인적 루프에 대한 자세한 정보를 반환합니다.	Read	human-loop* (p. 1584)		
DescribeHumanTaskUi	지정된 인적 검토 워크플로우 사용자 인터페이스에 대한 자세한 정보를 반환합니다.	Read	human-task-ui* (p. 1584)		
DescribeHyperParameterTuningJob	CreateHyperParameterTuningJob API를 통해 생성된 하이퍼 파라미터 튜닝 작업을 설명합니다.	Read	hyper-parameter-tuning-job* (p. 1586)		
DescribeLabelingJob	레이블 지정 작업에 대한 정보를 반환합니다.	Read	labeling-job* (p. 1584)		
DescribeModel	CreateModel API를 사용하여 생성한 모델을 설명합니다.	Read	model* (p. 1586)		
DescribeModelPackage	모델 패키지에 대한 정보를 반환합니다.	Read	model-package* (p. 1586)		
DescribeMonitoringSchedule	모니터링 일정에 대한 정보를 반환합니다.	Read	monitoring-schedule* (p. 1586)		
DescribeNotebookInstance	노트북 인스턴스에 대한 정보를 반환합니다.	Read	notebook-instance* (p. 1585)		
DescribeNotebookInstanceLifecycleConfig	CreateNotebookInstanceLifecycleConfig API를 통해 생성된 노트북 인스턴스 수명 주기 구성을 설명합니다.	Read	notebook-instance-lifecycle-config* (p. 1585)		
DescribeProcessingJob	처리 작업에 대한 정보를 반환합니다.	Read	processing-job* (p. 1585)		
DescribeSubscribedWorkteam	가입된 작업 팀에 대한 정보를 반환합니다.	Read	workteam* (p. 1584)		
DescribeTrainingJob	훈련 작업에 대한 정보를 반환합니다.	Read	training-job* (p. 1585)		
DescribeTransformJob	변환 작업에 대한 정보를 반환합니다.	Read	transform-job* (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeTrial	시도에 대한 정보를 반환합니다.	Read	experiment-trial* (p. 1587)		
DescribeTrialComponent	시도 구성 요소에 대한 정보를 반환합니다.	Read	experiment-trial-component* (p. 1587)		
DescribeUserProfile	UserProfile을 설명할 수 있는 권한을 부여합니다.	Read	user-profile* (p. 1585)		
DescribeWorkforce	작업 인력에 대한 정보를 반환합니다.	Read	workforce* (p. 1585)		
DescribeWorkteam	작업 팀에 대한 정보를 반환합니다.	Read	workteam* (p. 1584)		
DisassociateTrialComponent	시도 구성 요소를 시도와 연결 해제합니다.	쓰기	experiment-trial* (p. 1587)		
			experiment-trial-component* (p. 1587)		
			processing-job* (p. 1585)		
GetSearchSuggestions	키워드가 제공된 경우 검색 제안 사항을 가져옵니다.	Read	training-job* (p. 1585)		
InvokeEndpoint	Amazon SageMaker 호스팅 서비스를 사용하여 모델을 제품에 배포하고 나면, 클라이언트 애플리케이션이 이 API를 사용하여 지정된 엔드포인트에 호스팅된 모델에서 추론을 가져옵니다.	Read	endpoint* (p. 1586)		
ListAlgorithms	알고리즘을 나열합니다.	List			
ListApps	계정에 앱을 나열할 수 있는 권한을 부여합니다.	List			
ListAutoMLJobs	CreateAutoMLJob을 통해 생성된 AutoML 작업을 나열합니다.	List			
ListCandidatesForAutoMLJob	CreateAutoMLJob을 통해 생성된 AutoML 작업의 후보를 나열합니다.	List			
ListCodeRepositories	코드 리포지토리를 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListCompilationJobs	컴파일 작업을 나열합니다.	List			
ListDomains	계정의 도메인을 나열할 수 있는 권한을 부여합니다.	List			
ListEndpointConfigs	엔드포인트 구성을 나열합니다.	List			
ListEndpoints	엔드포인트를 나열합니다.	List			
ListExperiments	실험을 나열합니다.	List			
ListFlowDefinitions	파라미터가 지정되어 있을 때 흐름 정의에 대한 요약 정보를 반환합니다.	List			
ListHumanLoops	파라미터가 지정되어 있을 때 인적 루프에 대한 요약 정보를 반환합니다.	List			
ListHumanTaskUis	파라미터가 지정되어 있을 때 인적 검토 워크플로우 사용자 인터페이스에 대한 요약 정보를 반환합니다.	List			
ListHyperParameterTuningJobs	Amazon SageMaker를 사용하여 생성된 하이퍼 파라미터 튜닝 작업을 나열합니다.	List			
ListLabelingJobs	레이블 지정 작업을 나열합니다.	List			
ListLabelingJobsForWorkteam	작업 팀의 레이블 지정 작업을 나열합니다.	List	workteam* (p. 1584)		
ListModelPackages	모델 패키지를 나열합니다.	List			
ListModels	CreateModel API를 사용하여 생성된 모델을 나열합니다.	List			
ListMonitoringExecutions	모니터링 실행을 나열합니다.	List			
ListMonitoringSchedules	모니터링 일정을 나열합니다.	List			
ListNotebookInstanceLifecycleConfigs	Amazon SageMaker를 사용하여 배포할 수 있는 노트북 인스턴스 수명 주기 구성을 나열합니다.	List			
ListNotebookInstances	AWS 리전에서 요청자의 계정에 있는 Amazon SageMaker 노트북 인스턴스의 목록을 반환합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListProcessingJobs	처리 작업을 나열합니다.	List			
ListSubscribedWorkteams	가입된 작업 팀을 나열합니다.	List			
ListTags	지정된 리소스와 연결된 태그 세트를 반환합니다.	List	app (p. 1585)		
			automl-job (p. 1586)		
			domain (p. 1585)		
			endpoint (p. 1586)		
			endpoint-config (p. 1586)		
			experiment (p. 1586)		
			experiment-trial (p. 1587)		
			experiment-trial-component (p. 1587)		
			flow-definition (p. 1584)		
			human-task-ui (p. 1584)		
			hyper-parameter-tuning-job (p. 1586)		
			labeling-job (p. 1584)		
			model (p. 1586)		
			monitoring-schedule (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			notebook-instance (p. 1585)		
			training-job (p. 1585)		
			transform-job (p. 1586)		
			user-profile (p. 1585)		
			workteam (p. 1584)		
ListTrainingJobs	교육 작업을 나열합니다.	List			
ListTrainingJobsForHyperParameterTuningJob	Amazon SageMaker를 사용하여 생성된 하이퍼 파라미터 튜닝 작업에 대한 훈련 작업을 나열합니다.	List	hyper-parameter-tuning-job* (p. 1586)		
ListTransformJobs	변환 작업을 나열합니다.	List			
ListTrialComponents	시도 구성 요소를 나열합니다.	List			
ListTrials	시도를 나열합니다.	List			
ListUserProfiles	계정의 UserProfile을 나열할 수 있는 권한을 부여합니다.	List			
ListWorkteams	작업 팀을 나열합니다.	List			
RenderUiTemplate	인간 주석 작업에 사용되는 UI 템플릿을 렌더링합니다.	Read			iam:PassRole
Search	훈련 작업을 검색합니다.	Read	training-job* (p. 1585)		
StartHumanLoop	인적 루프를 시작합니다.	쓰기	flow-definition* (p. 1584)		
StartMonitoringSchedule	모니터링 일정을 시작합니다.	쓰기	monitoring-schedule* (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartNotebookInstance	라이브러리의 최신 버전으로 EC2 인스턴스를 시작하고 EBS 볼륨을 연결합니다.	쓰기	notebook-instance* (p. 1585)		
StopAutoMLJob	CreateAutoMLJob을 통해 생성된 실행 중인 AutoML 작업을 중지합니다.	쓰기	automl-job* (p. 1586)		
StopCompilationJob	컴파일 작업을 중지합니다.	쓰기	compilation-job* (p. 1586)		
StopHumanLoop	지정된 인적 루프를 중지합니다.	쓰기	human-loop* (p. 1584)		
StopHyperParameterTuningJob	CreateHyperParameterTuningJob을 통해 생성된 실행 중인 하이퍼파라미터 튜닝 작업을 중지합니다.	쓰기	hyper-parameter-tuning-job* (p. 1586)		
StopLabelingJob	레이블 지정 작업을 중지합니다. 이미 생성된 모든 레이블은 중지 전에 내보내집니다	쓰기	labeling-job* (p. 1584)		
StopMonitoringSchedule	모니터링 일정을 중지합니다.	쓰기	monitoring-schedule* (p. 1586)		
StopNotebookInstance	EC2 인스턴스를 종료합니다. 인스턴스를 종료하기 전에 Amazon SageMaker가 인스턴스에서 EBS 볼륨을 연결 해제합니다. Amazon SageMaker는 EBS 볼륨을 유지합니다.	쓰기	notebook-instance* (p. 1585)		
StopProcessingJob	처리 작업을 중지합니다. 작업을 중지하기 위해, Amazon SageMaker는 작업 종료를 120초간 지연시키는 SIGTERM 신호를 알고리즘에 보냅니다.	쓰기	processing-job* (p. 1585)		
StopTrainingJob	훈련 작업을 중지합니다. 작업을 중지하기 위해, Amazon SageMaker는 작업 종료를 120초간 지연시키는 SIGTERM 신호를 알고리즘에 보냅니다.	쓰기	training-job* (p. 1585)		
StopTransformJob	변환 작업을 중지합니다. Amazon SageMaker가 StopTransformJob 요청을 수신하면 작업 상태가 중지 중으로 변경됩니다. Amazon SageMaker가 작업을 중지하면 상태가 중지됨으로 설정됩니다.	쓰기	transform-job* (p. 1586)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateCodeRepository	코드 리포지토리를 업데이트합니다.	쓰기	code-repository* (p. 1585)		
UpdateDomain	도메인을 업데이트할 수 있는 권한을 부여합니다.	쓰기	domain* (p. 1585)		
				sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:InstanceTypes (p. 1588) sagemaker:DomainSharingOutputKmsK (p. 1587)	
UpdateEndpoint	요청에 지정된 엔드포인트 구성을 사용하도록 엔드포인트를 업데이트합니다.	쓰기	endpoint* (p. 1586)		
UpdateEndpointWeightsAndCapacities	변환 가중치, 용량, 또는 엔드포인트와 연결된 하나 이상의 변수를 업데이트합니다.	쓰기	endpoint* (p. 1586)		
UpdateExperiment	실험을 업데이트합니다.	쓰기	experiment* (p. 1586)		
UpdateMonitoringSchedule	모니터링 일정을 업데이트합니다.	쓰기	monitoring-schedule* (p. 1586)		iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1587) aws:TagKeys (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:MaxRuntimeInSeconds (p. 1588) sagemaker:NetworkIsolation (p. 1588) sagemaker:OutputKmsKey (p. 1588) sagemaker:VolumeKmsKey (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:VpcSubnets (p. 1588)	
UpdateNotebookInstance 노트북 인스턴스 업데이트는 워크로드 요구 사항의 변경을 수용하기 위해 노트북 인스턴스에 사용되는 EC2 인스턴스 업그레이드 또는 다운그레이드를 포함합니다. 또한 VPC 보안 그룹도 업데이트할 수 있습니다.	노트북 인스턴스를 업데이트합니다.	쓰기	notebook-instance* (p. 1585)		
				sagemaker:AcceleratorTypes (p. 1587) sagemaker:InstanceTypes (p. 1588) sagemaker:RootAccess (p. 1588)	
UpdateNotebookInstanceLifecycleConfig	CreateNotebookInstanceLifecycleConfig API로 생성된 노트북 인스턴스 수명 주기 구성을 업데이트합니다.	쓰기	notebook-instance-lifecycle-config* (p. 1585)		
UpdateTrial	시도를 업데이트합니다.	쓰기	experiment-trial* (p. 1587)		
UpdateTrialComponent	시도 구성 요소를 업데이트합니다.	쓰기	experiment-trial-component* (p. 1587)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateUserProfile	UserProfile을 업데이트할 수 있는 권한을 부여합니다.	쓰기	user-profile* (p. 1585)		
				sagemaker:InstanceTypes (p. 1588) sagemaker:VpcSecurityGroupIds (p. 1588) sagemaker:InstanceTypes (p. 1588) sagemaker:DomainSharingOutputKmsK (p. 1587)	
UpdateWorkforce	작업 인력을 업데이트합니다.	쓰기	workforce* (p. 1585)		
UpdateWorkteam	작업 팀을 업데이트합니다.	쓰기	workteam* (p. 1584)		

Amazon SageMaker에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1559)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
human-loop	`arn:${Partition}:sagemaker:${Region}:${Account}:human-loop/${HumanLoopName}`	
flow-definition	`arn:${Partition}:sagemaker:${Region}:${Account}:flow-definition/${FlowDefinitionName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
human-task-ui	`arn:${Partition}:sagemaker:${Region}:${Account}:human-task-ui/${HumanTaskUiName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
labeling-job	`arn:${Partition}:sagemaker:${Region}:${Account}:labeling-job/${LabelingJobName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
workteam	`arn:${Partition}:sagemaker:${Region}:${Account}:workteam/${WorkteamName}`	aws:ResourceTag/${TagKey} (p. 1587)

리소스 유형	ARN	조건 키
		sagemaker:ResourceTag/${TagKey} (p. 1588)
workforce	arn:${Partition}:sagemaker:${Region}:${Account}:workforce/${WorkforceName}	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
domain	arn:${Partition}:sagemaker:${Region}:${Account}:domain/${DomainId}	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
user-profile	arn:${Partition}:sagemaker:${Region}:${Account}:user-profile/${DomainId}/${UserProfileName}	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
app	arn:${Partition}:sagemaker:${Region}:${Account}:app/${DomainId}/${UserProfileName}/${AppType}/${AppName}	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
notebook-instance	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance/${NotebookInstanceName}	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
notebook-instance-lifecycle-config	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance-lifecycle-config/${NotebookInstanceLifecycleConfigName}	
code-repository	arn:${Partition}:sagemaker:${Region}:${Account}:code-repository/${CodeRepositoryName}	
algorithm	arn:${Partition}:sagemaker:${Region}:${Account}:algorithm/${AlgorithmName}	
training-job	arn:${Partition}:sagemaker:${Region}:${Account}:training-job/${TrainingJobName}	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
processing-job	arn:${Partition}:sagemaker:${Region}:${Account}:processing-job/${ProcessingJobName}	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)

리소스 유형	ARN	조건 키
hyper-parameter-tuning-job	`arn:${Partition}:sagemaker:${Region}:${Account}:hyper-parameter-tuning-job/${HyperParameterTuningJobName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
model-package	`arn:${Partition}:sagemaker:${Region}:${Account}:model-package/${ModelPackageName}`	
model	`arn:${Partition}:sagemaker:${Region}:${Account}:model/${ModelName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
endpoint-config	`arn:${Partition}:sagemaker:${Region}:${Account}:endpoint-config/${EndpointConfigName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
endpoint	`arn:${Partition}:sagemaker:${Region}:${Account}:endpoint/${EndpointName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
transform-job	`arn:${Partition}:sagemaker:${Region}:${Account}:transform-job/${TransformJobName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
compilation-job	`arn:${Partition}:sagemaker:${Region}:${Account}:compilation-job/${CompilationJobName}`	
automl-job	`arn:${Partition}:sagemaker:${Region}:${Account}:automl-job/${AutoMLJobJobName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
monitoring-schedule	`arn:${Partition}:sagemaker:${Region}:${Account}:monitoring-schedule/${MonitoringScheduleName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
experiment	`arn:${Partition}:sagemaker:${Region}:${Account}:experiment/${ExperimentName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)

리소스 유형	ARN	조건 키
experiment-trial	`arn:${Partition}:sagemaker:${Region}:${Account}:experiment-trial/${TrialName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)
experiment-trial-component	`arn:${Partition}:sagemaker:${Region}:${Account}:experiment-trial-component/${TrialComponentName}`	aws:ResourceTag/${TagKey} (p. 1587) sagemaker:ResourceTag/${TagKey} (p. 1588)

Amazon SageMaker에 사용되는 조건 키

Amazon SageMaker는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	SageMaker 서비스에 대한 사용자의 요청에 있는 키입니다.	문자열
aws:ResourceTag/${TagKey}	태그 키 및 값 페어입니다.	문자열
aws:TagKeys	요청의 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열
sagemaker:AcceleratorTypes	요청의 리소스와 연결된 모든 액셀러레이터 유형의 목록입니다.	ArrayOfString
sagemaker:AppNetworkAccess	요청의 리소스와 연결된 앱 네트워크 액세스입니다.	문자열
sagemaker:DirectInternetAccess	요청의 리소스와 연결된 직접 인터넷 액세스입니다.	문자열
sagemaker:DomainSharingOutputKmsKey	요청의 리소스와 연결된 도메인 공유 출력 KMS 키입니다.	ARN
sagemaker:FileSystemAccessMode	요청의 리소스와 연결된 파일 시스템 액세스 모드입니다.	문자열
sagemaker:FileSystemDirectoryPath	요청의 리소스와 연결된 파일 시스템 디렉터리 경로입니다.	문자열
sagemaker:FileSystemId	요청의 리소스와 연결된 파일 시스템 ID입니다.	문자열
sagemaker:FileSystemType	요청의 리소스와 연결된 파일 시스템 유형입니다.	문자열

조건 키	설명	유형
sagemaker:HomeEfsFileSystemKmsKey	요청의 리소스와 연결된 UserProfil 홈 디렉터리에 사용되는 EFS 파일 시스템의 KMS 키 ID입니다.	ARN
sagemaker:InstanceTypes	요청의 리소스와 연결된 모든 인스턴스 유형 목록입니다.	ArrayOfString
sagemaker:InterContainerTrafficEncryption	요청의 리소스와 연결된 컨테이너 간 트래픽 암호화입니다.	Bool
sagemaker:MaxRuntimeInSeconds	요청의 리소스와 연결된 최대 실행 시간(초)입니다.	숫자
sagemaker:ModelArn	요청의 리소스와 연결된 모델 ARN입니다.	ARN
sagemaker:NetworkIsolation	요청의 리소스와 연결된 네트워크 격리입니다.	Bool
sagemaker:OutputKmsKey	요청의 리소스와 연결된 출력 KMS 키입니다.	ARN
sagemaker:ResourceTag/	리소스에 연결된 태그 키 및 값 페어의 서문 문자열입니다.	문자열
sagemaker:ResourceTag/${TagKey}	태그 키 및 값 페어입니다.	문자열
sagemaker:RootAccess	요청의 리소스와 연결된 루트 액세스입니다.	문자열
sagemaker:VolumeKmsKey	요청의 리소스와 연결된 볼륨 KMS 키입니다.	ARN
sagemaker:VpcSecurityGroupIds	요청의 리소스와 연결된 모든 VPC 보안 그룹 ID 목록입니다.	ArrayOfString
sagemaker:VpcSubnets	요청의 리소스와 연결된 모든 VPC 서브넷 목록입니다.	ArrayOfString
sagemaker:WorkteamArn	요청과 연결된 작업 팀 ARN입니다.	ARN
sagemaker:WorkteamType	요청과 연결된 작업 팀 유형입니다. public-crowd, private-crowd 또는 vendor-crowd가 될 수 있습니다.	문자열

AWS Savings Plans에 사용되는 작업, 리소스 및 조건 키

AWS Savings Plans(서비스 접두사: `savingsplans`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Savings Plans에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateSavingsPlan	Savings Plan을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1590) aws:TagKeys (p. 1590)	
DescribeSavingsPlanRates	고객 Savings Plan과 관련된 요금을 설명할 수 있는 권한을 부여합니다.	Read	savingsplan* (p. 1590)		
				aws:ResourceTag/${TagKey} (p. 1590)	
DescribeSavingsPlans	고객 계정과 관련된 Savings Plan을 설명할 수 있는 권한을 부여합니다.	Read	savingsplan* (p. 1590)		
				aws:ResourceTag/${TagKey} (p. 1590)	
DescribeSavingsPlansOfferingRates	Savings Plan 제품과 관련된 요금을 설명할 수 있는 권한을 부여합니다.	Read			
DescribeSavingsPlansOfferings	고객이 구매할 수 있는 Savings Plan 제품을 설명할 수 있는 권한을 부여합니다.	Read			
ListTagsForResource	Savings Plan에 대한 태그를 나열할 수 있는 권한을 부여합니다.	List	savingsplan* (p. 1590)		
TagResource	Savings Plan에 대한 태그를 지정할 수 있는 권한을 부여합니다.	태그 지정	savingsplan* (p. 1590)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1590) aws:RequestTag/${TagKey} (p. 1590)	
UntagResource	Savings Plan의 태그를 해제할 수 있는 권한을 부여합니다.	태그 지정	savingsplan* (p. 1590)		
				aws:TagKeys (p. 1590)	

AWS Savings Plans에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1589)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
savingsplan	`arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1590)

AWS Savings Plans에 사용되는 조건 키

AWS Savings Plans는 `Condition` 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Secrets Manager에 사용되는 작업, 리소스 및 조건 키

AWS Secrets Manager(서비스 접두사: `secretsmanager`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Secrets Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelRotateSecret	사용자가 진행 중인 보안 암호 교체를 취소할 수 있습니다.	쓰기	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
CreateSecret	사용자가 쿼리 및 교체 가능한 암호화된 데이터를 저장하는 보안 암호를 생성할 수 있습니다.	태그 지정		secretsmanager:Name (p. 1597) secretsmanager:Description (p. 1597) secretsmanager:KmsKeyId (p. 1597) aws:RequestTag/tag-key (p. 1597)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
DeleteResourcePolicy	사용자가 암호에 연결된 리소스 정책을 삭제할 수 있습니다.	권한 관리	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
DeleteSecret	사용자가 보안 암호를 삭제할 수 있습니다.	쓰기	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:RecoveryWindowInDa (p. 1597) secretsmanager:ForceDeleteWithoutRe (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
DescribeSecret	사용자가 보안 암호에 대한 메타데이터를 검색할 수 있지만 암호화된 데이터는 검색할 수 없습니다.	Read	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
GetRandomPassword	사용자가 암호 생성에 사용할 임의 문자열을 생성할 수 있습니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetResourcePolicy	사용자가 암호에 연결된 리소스 정책을 가져올 수 있습니다.	Read	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
GetSecretValue	사용자가 암호화된 데이터를 검색 및 암호화 해제할 수 있습니다.	Read	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:VersionId (p. 1597) secretsmanager:VersionStage (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
ListSecretVersionIds	사용자가 보안 암호의 사용 가능한 버전을 나열할 수 있습니다.	Read	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
ListSecrets	사용자가 사용 가능한 보안 암호를 나열할 수 있습니다.	List			
PutResourcePolicy	사용자가 리소스 정책을 암호에 연결할 수 있습니다.	권한 관리	Secret* (p. 1596)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
PutSecretValue	사용자가 새 암호화된 데이터로 보안 암호의 새 버전을 생성할 수 있습니다.	쓰기	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
RestoreSecret	사용자가 보안 암호의 삭제를 취소할 수 있습니다.	쓰기	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
RotateSecret	사용자가 보안 암호의 교체를 시작할 수 있습니다.	쓰기	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:RotationLambdaARN (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
TagResource	사용자가 태그를 보안 암호에 추가할 수 있습니다.	태그 지정	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) aws:RequestTag/tag-key (p. 1597) aws:TagKeys (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
UntagResource	사용자가 보안 암호에서 태그를 제거할 수 있습니다.	태그 지정	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) aws:TagKeys (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
UpdateSecret	사용자가 새 메타데이터 또는 암호화된 데이터의 새 버전으로 보안 암호를 업데이트할 수 있습니다.	쓰기	Secret* (p. 1596)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				secretsmanager:SecretId (p. 1597) secretsmanager:Description (p. 1597) secretsmanager:KmsKeyId (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	
UpdateSecretVersionStage	사용자가 보안 암호 간에 단계를 이동할 수 있습니다.	쓰기	Secret* (p. 1596)		
				secretsmanager:SecretId (p. 1597) secretsmanager:VersionStage (p. 1597) secretsmanager:resource/AllowRotationLambdaArn (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)	

AWS Secrets Manager에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1591)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Secret	`arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}`	aws:RequestTag/tag-key (p. 1597) aws:TagKeys (p. 1597) secretsmanager:ResourceTag/tag-key (p. 1597)

리소스 유형	ARN	조건 키
		secretsmanager:resource/AllowRotationLambdaArn (p. 1597)

AWS Secrets Manager의 조건 키

AWS Secrets Manager는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/tag-key	Secrets Manager 서비스에 대한 사용자의 요청에 있는 키를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	Secrets Manager 서비스에 대한 사용자의 요청에 있는 모든 태그 키 이름의 목록을 기준으로 액세스를 필터링합니다.	문자열
secretsmanager:Description	요청에 있는 설명 텍스트를 기준으로 액세스를 필터링합니다.	문자열
secretsmanager:ForceDeleteWithoutRecovery	암호를 복구 기간 없이 즉시 삭제해야 하는지 여부에 따라 액세스를 필터링합니다.	부울
secretsmanager:KmsKeyId	요청에 있는 KMS 키의 ARN을 기준으로 액세스를 필터링합니다.	문자열
secretsmanager:Name	요청에 있는 보안 암호의 표시 이름을 기준으로 액세스를 필터링합니다.	문자열
secretsmanager:RecoveryWindowInDays	Secrets Manager가 암호를 삭제하기 전에 대기해야 하는 기간(일)을 기준으로 액세스를 필터링합니다.	Long
secretsmanager:ResourceTag/tag-key	태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열
secretsmanager:RotationLambdaARN	요청에 있는 교체 Lambda 함수의 ARN을 기준으로 액세스를 필터링합니다.	ARN
secretsmanager:SecretId	요청에 있는 SecretID 값을 기준으로 액세스를 필터링합니다.	ARN
secretsmanager:VersionId	요청에 있는 보안 암호 버전의 고유 식별자를 기준으로 액세스를 필터링합니다.	문자열
secretsmanager:VersionStage	요청에 있는 버전 단계의 목록을 기준으로 액세스를 필터링합니다.	문자열
secretsmanager:resource/AllowRotationLambdaArn	보안 암호와 연결된 교체 Lambda 함수의 ARN을 기준으로 액세스를 필터링합니다.	ARN

AWS Security Hub에 사용되는 작업, 리소스 및 조건 키

AWS Security Hub(서비스 접두사: `securityhub`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Security Hub에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptInvitation	멤버 계정으로의 Security Hub 초대를 수락할 수 있는 권한을 부여합니다.	쓰기			
BatchDisableStandards	Security Hub에서 표준을 비활성화할 수 있는 권한을 부여합니다.	쓰기	standards-subscription* (p. 1601)		
BatchEnableStandards	Security Hub에서 표준을 활성화할 수 있는 권한을 부여합니다.	쓰기	standard* (p. 1601)		
BatchImportFindings	통합 제품에서 결과를 Security Hub로 가져올 수 있는 권한을 부여합니다.	쓰기		securityhub:TargetAccount (p. 1602)	
CreateActionTarget	Security Hub에서 사용자 지정 작업을 생성할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateInsight	Security Hub에서 통찰력을 생성할 수 있는 권한을 부여합니다. 통찰력은 관련 결과의 모음입니다.	쓰기			
CreateMembers	Security Hub에서 멤버 계정을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeclineInvitations	멤버 계정으로의 Security Hub 초대를 거부할 수 있는 권한을 부여합니다.	쓰기			
DeleteActionTarget	Security Hub에서 사용자 지정 작업을 삭제할 수 있는 권한을 부여합니다.	쓰기	action-target* (p. 1602)		
DeleteInsight	Security Hub에서 통찰력을 삭제할 수 있는 권한을 부여합니다.	쓰기	insight* (p. 1601)		
DeleteInvitations	멤버 계정으로의 Security Hub 초대를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteMembers	Security Hub 멤버 계정을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DescribeActionTargets	API를 사용하여 사용자 지정 작업 목록을 검색할 수 있는 권한을 부여합니다.	Read			
DescribeHub	계정에서 허브 리소스에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read			
DescribeProducts	사용 가능한 Security Hub 제품 통합에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read			
DescribeStandards	Security Hub 표준에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	hub* (p. 1601)		
DescribeStandardsControls	Security Hub 표준 제어에 대한 정보를 검색할 수 있는 권한을 부여합니다.	Read	hub* (p. 1601)		
DisableImportFindingsForProduct	Security Hub 통합 제품에 대해 결과 가져오기를 비활성화할 수 있는 권한을 부여합니다.	쓰기	product* (p. 1601)		
DisableSecurityHub	Security Hub를 비활성화할 수 있는 권한을 부여합니다.	쓰기			
DisassociateFromMasterAccount	Security Hub 멤버 계정에 마스터 계정과의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DisassociateMembers	연결된 마스터 계정에서 Security Hub 멤버 계정을 연결 해제할 수 있는 권한을 부여합니다.	쓰기			
EnableImportFindingsForProduct	Security Hub 통합 제품에 대한 결과를 가져올 수 있는 권한을 부여합니다.	쓰기	product* (p. 1601)		
EnableSecurityHub	Security Hub를 활성화할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1602) aws:TagKeys (p. 1602)	
GetEnabledStandards	Security Hub에서 활성화된 표준 목록을 검색할 수 있는 권한을 부여합니다.	List			
GetFindings	Security Hub에서 결과 목록을 검색할 수 있는 권한을 부여합니다.	Read			
GetInsightResults	Security Hub에서 통찰력 결과를 검색할 수 있는 권한을 부여합니다.	Read	insight* (p. 1601)		
GetInsights	Security Hub 통찰력을 검색할 수 있는 권한을 부여합니다.	List	insight* (p. 1601)		
GetInvitationsCount	계정으로 전송된 Security Hub 멤버십 초대 수를 검색할 수 있는 권한을 부여합니다.	Read			
GetMasterAccount	Security Hub 마스터 계정에 대한 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read			
GetMembers	Security Hub 멤버 계정의 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read			
InviteMembers	다른 AWS 계정을 Security Hub 멤버 계정으로 초대할 수 있는 권한을 부여합니다.	쓰기			
ListEnabledProductsForImport	현재 활성화된 Security Hub 통합 제품을 검색할 수 있는 권한을 부여합니다.	List			
ListInvitations	계정으로 전송된 Security Hub 초대를 검색할 수 있는 권한을 부여합니다.	List			
ListMembers	마스터 계정과 연결된 Security Hub 멤버 계정에 대한 세부 정보를 검색할 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTagsForResource	리소스와 연결된 태그를 나열할 수 있는 권한을 부여합니다.	List	hub* (p. 1601)		
TagResource	Security Hub 리소스에 태그를 추가할 수 있는 권한을 부여합니다.	쓰기	hub* (p. 1601)		
UntagResource	Security Hub 리소스에서 태그를 제거할 수 있는 권한을 부여합니다.	쓰기	hub* (p. 1601)		
UpdateActionTarget	Security Hub에서 사용자 지정 작업을 업데이트할 수 있는 권한을 부여합니다.	쓰기	action-target* (p. 1602)		
UpdateFindings	Security Hub 결과를 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateInsight	Security Hub에서 통찰력을 업데이트할 수 있는 권한을 부여합니다.	쓰기	insight* (p. 1601)		
UpdateStandardsControl	Security Hub 표준 제어를 업데이트할 수 있는 권한을 부여합니다.	쓰기	hub* (p. 1601)		

AWS Security Hub에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1598)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
insight	`arn:${Partition}:securityhub:${Region}:${Account}:insight/${CompanyId}/${ProductId}/${UniqueId}`	
standard	`arn:${Partition}:securityhub:::ruleset/${StandardsName}/v/${StandardsVersion}`	
standards-subscription	`arn:${Partition}:securityhub:${Region}:${Account}:subscription/${StandardsName}/v/${StandardsVersion}`	
product-subscription	`arn:${Partition}:securityhub:${Region}:${Account}:product-subscription/${Company}/${ProductId}`	
product	`arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}`	
hub	`arn:${Partition}:securityhub:${Region}:${Account}:hub/default`	aws:ResourceTag/${TagKey} (p. 1602)

리소스 유형	ARN	조건 키
action-target	`arn:${Partition}:securityhub:${Region}:${Account}:action/custom/${Id}`	

AWS Security Hub에 사용되는 조건 키

AWS Security Hub는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
securityhub:TargetAccount	결과를 가져오려는 AWS 계정의 ID입니다. AWS Security Finding 형식에서 이 필드는 AwsAccountId라고 합니다.	문자열

AWS Security Token Service에 사용되는 작업, 리소스 및 조건 키

AWS Security Token Service(서비스 접두사: `sts`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS Security Token Service에서 정의한 작업 (p. 1602)
- AWS Security Token Service에서 정의한 리소스 유형 (p. 1607)
- AWS Security Token Service 조건 키 (p. 1608)

AWS Security Token Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssumeRole	평소에는 액세스 권한이 없을 수 있는 AWS 리소스에 액세스하기 위해 사용할 수 있는 일련의 임시 보안 자격 증명을 반환합니다.	쓰기	role* (p. 1607)		
				aws:TagKeys (p. 1608) aws:PrincipalTag/${TagKey} (p. 1608) aws:RequestTag/${TagKey} (p. 1608) sts:TransitiveTagKeys (p. 1610)	
AssumeRoleWithSAML	SAML 인증 응답을 통해 인증된 사용자에 대한 임시 보안 자격 증명 집합을 반환합니다.	쓰기	role* (p. 1607)		
				saml:namequalifier (p. 1610) saml:sub (p. 1610) saml:sub_type (p. 1610) saml:aud (p. 1608) saml:iss (p. 1609) saml:doc (p. 1609) saml:cn (p. 1608) saml:commonName (p. 1609) saml:eduorghomepageuri (p. 1609)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				saml:eduorgidentityauthnpolicyuri (p. 1609) saml:eduorglegalname (p. 1609) saml:eduorgsuperioruri (p. 1609) saml:eduorgwhitepagesuri (p. 1609) saml:edupersonaffiliation (p. 1609) saml:edupersonassurance (p. 1609) saml:edupersonentitlement (p. 1609) saml:edupersonnickname (p. 1609) saml:edupersonorgdn (p. 1609) saml:edupersonorgunitdn (p. 1609) saml:edupersonprimaryaffiliation (p. 1609) saml:edupersonprimaryorgunitdn (p. 1609) saml:edupersonprincipalname (p. 1609) saml:edupersonscopedaffiliation (p. 1609) saml:edupersontargetedid (p. 1609) saml:givenName (p. 1609) saml:mail (p. 1609) saml:name (p. 1610) saml:organizationStatus (p. 1610)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				saml:primaryGroupSID (p. 1610) saml:surname (p. 1610) saml:uid (p. 1610) saml:x500UniqueIdentifier (p. 1610) aws:TagKeys (p. 1608) aws:PrincipalTag/${TagKey} (p. 1608) aws:RequestTag/${TagKey} (p. 1608) sts:TransitiveTagKeys (p. 1610)	
AssumeRoleWithWebIdentity	웹 자격 증명 공급자로 모바일 또는 웹 애플리케이션에서 인증된 사용자에 대한 임시 보안 자격 증명 집합을 반환합니다.	쓰기	role* (p. 1607)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				cognito-identity.amazonaws.com:amr (p. 1608) cognito-identity.amazonaws.com:aud (p. 1608) cognito-identity.amazonaws.com:sub (p. 1608) www.amazon.com:app_id (p. 1610) www.amazon.com:user_id (p. 1610) graph.facebook.com:app_id (p. 1608) graph.facebook.com:id (p. 1608) accounts.google.com:aud (p. 1608) accounts.google.com:oaud (p. 1608) accounts.google.com:sub (p. 1608) aws:TagKeys (p. 1608) aws:PrincipalTag/${TagKey} (p. 1608) aws:RequestTag/${TagKey} (p. 1608) sts:TransitiveTagKeys (p. 1610)	
DecodeAuthorizationMessage	AWS 요청에 대한 응답으로 반환되는 인코딩 메시지로부터 받은 요청의 권한 부여 상태에 대한 추가 정보를 디코딩합니다.	쓰기			
GetAccessKeyInfo	요청에 대해 파라미터로 전달되는 액세스 키 ID에 대한 세부 정보를 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetCallerIdentity	API를 호출하는 데 사용되는 IAM 자격 증명에 대한 세부 정보를 반환합니다.	Read			
GetFederationToken	연합된 사용자를 위한 일련의 임시 보안 자격 증명(액세스 키 ID, 보안 액세스 키 및 보안 토큰으로 구성)을 반환합니다.	Read	user (p. 1608)		
				aws:TagKeys (p. 1608) aws:PrincipalTag/${TagKey} (p. 1608) aws:RequestTag/${TagKey} (p. 1608)	
GetSessionToken	AWS 계정 또는 IAM 사용자에 대한 일련의 임시 보안 자격 증명(액세스 키 ID, 보안 액세스 키 및 보안 토큰으로 구성)을 반환합니다.	Read			
TagSession [권한만 해당]	STS 세션에 태그를 추가할 수 있는 권한을 부여합니다.	태그 지정	role (p. 1607)		
			user (p. 1608)		
				aws:TagKeys (p. 1608) aws:PrincipalTag/${TagKey} (p. 1608) aws:RequestTag/${TagKey} (p. 1608) sts:TransitiveTagKeys (p. 1610)	

AWS Security Token Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1602)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
role	`arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}`	aws:ResourceTag/${TagKey} (p. 1608)

리소스 유형	ARN	조건 키
user	`arn:${Partition}:iam::${Account}:user/${UserNameWithPath}`	

AWS Security Token Service 조건 키

AWS Security Token Service는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
accounts.google.com:aud	Google 애플리케이션 ID를 기준으로 작업을 필터링합니다.	문자열
accounts.google.com:oaud	Google 고객을 기준으로 작업을 필터링합니다.	문자열
accounts.google.com:sub	클레임 제목(Google 사용자 ID)을 기준으로 작업을 필터링합니다.	문자열
aws:FederatedProvider	사용자를 인증하는 데 사용된 IdP를 기준으로 작업을 필터링합니다.	문자열
aws:PrincipalTag/${TagKey}	요청을 하는 보안 주체와 연결된 태그를 기준으로 작업을 필터링합니다.	문자열
aws:RequestTag/${TagKey}	요청에서 전달되는 태그를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에서 전달되는 태그 키를 기준으로 작업을 필터링합니다.	문자열
cognito-identity.amazonaws.com:amr	Amazon Cognito의 로그인 정보를 기준으로 작업을 필터링합니다.	문자열
cognito-identity.amazonaws.com:aud	Amazon Cognito 자격 증명 풀 ID를 기준으로 작업을 필터링합니다.	문자열
cognito-identity.amazonaws.com:sub	클레임 제목(Amazon Cognito 사용자 ID)을 기준으로 작업을 필터링합니다.	문자열
graph.facebook.com:app_id	Facebook 애플리케이션 ID를 기준으로 작업을 필터링합니다.	문자열
graph.facebook.com:id	Facebook 사용자 ID를 기준으로 작업을 필터링합니다.	문자열
saml:aud	SAML 어설션이 표시되는 엔드포인트 URL을 기준으로 작업을 필터링합니다.	문자열
saml:cn	eduOrg 속성을 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
saml:commonName	commonName 속성을 기준으로 작업을 필터링합니다.	문자열
saml:doc	역할을 수임하는 데 사용된 보안 주체를 기준으로 작업을 필터링합니다.	문자열
saml:eduorghomepageuri	eduOrg 속성을 기준으로 작업을 필터링합니다.	문자열
saml:eduorgidentityauthnpolicyuri	eduOrg 속성을 기준으로 작업을 필터링합니다.	문자열
saml:eduorglegalname	eduOrg 속성을 기준으로 작업을 필터링합니다.	문자열
saml:eduorgsuperioruri	eduOrg 속성을 기준으로 작업을 필터링합니다.	문자열
saml:eduorgwhitepagesuri	eduOrg 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonaffiliation	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonassurance	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonentitlement	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonnickname	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonorgdn	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonorgunitdn	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonprimaryaffiliation	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonprimaryorgunitdn	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonprincipalname	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersonscopedaffiliation	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:edupersontargetedid	eduPerson 속성을 기준으로 작업을 필터링합니다.	문자열
saml:givenName	givenName 속성을 기준으로 작업을 필터링합니다.	문자열
saml:iss	URN으로 표시되는 발급자를 기준으로 작업을 필터링합니다.	문자열
saml:mail	mail 속성을 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
saml:name	name 속성을 기준으로 작업을 필터링합니다.	문자열
saml:namequalifier	발급자의 해시 값, 계정 ID 및 표시 이름을 기준으로 작업을 필터링합니다.	문자열
saml:organizationStatus	organizationStatus 속성을 기준으로 작업을 필터링합니다.	문자열
saml:primaryGroupSID	primaryGroupSID 속성을 기준으로 작업을 필터링합니다.	문자열
saml:sub	클레임 제목(SAML 사용자 ID)을 기준으로 작업을 필터링합니다.	문자열
saml:sub_type	영구 값, 임시 값 또는 전체 형식 URI를 기준으로 작업을 필터링합니다.	문자열
saml:surname	surname 속성을 기준으로 작업을 필터링합니다.	문자열
saml:uid	uid 속성을 기준으로 작업을 필터링합니다.	문자열
saml:x500UniqueIdentifier	uid 속성을 기준으로 작업을 필터링합니다.	문자열
sts:ExternalId	다른 계정에서 역할을 수임할 때 필요한 고유 식별자를 기준으로 작업을 필터링합니다.	문자열
sts:TransitiveTagKeys	요청에서 전달되는 전이적 태그 키를 기준으로 작업을 필터링합니다.	문자열
www.amazon.com:app_id	Login with Amazon 애플리케이션 ID를 기준으로 필터링합니다.	문자열
www.amazon.com:user_id	Login with Amazon 사용자 ID를 기준으로 작업을 필터링합니다.	문자열

AWS Server Migration Service에 사용되는 작업, 리소스 및 조건 키

AWS Server Migration Service(서비스 접두사: `sms`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Server Migration Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateApp	온프레미스 애플리케이션을 AWS로 마이그레이션하기 위한 애플리케이션 구성을 생성합니다.	쓰기			
CreateReplicationJob	온프레미스 서버를 AWS로 마이그레이션하기 위한 작업을 생성합니다.	쓰기			
DeleteApp	기존 애플리케이션 구성을 삭제합니다.	쓰기			
DeleteAppLaunchConfiguration	기존 애플리케이션에 대한 시작 구성을 삭제합니다.	쓰기			
DeleteAppReplicationConfiguration	기존 애플리케이션에 대한 복제 구성을 삭제합니다.	쓰기			
DeleteReplicationJob	온프레미스 서버를 AWS로 마이그레이션하기 위한 기존 작업을 삭제합니다.	쓰기			
DeleteServerCatalog	AWS로 수집된 온프레미스 서버의 전체 목록을 삭제합니다.	쓰기			
DisassociateConnector	연결된 커넥터를 연결 해제합니다.	쓰기			
GenerateChangeSet	애플리케이션의 CloudFormation 스택에 대한 changeSet를생성합니다.	쓰기			
GenerateTemplate	기존 애플리케이션에 대한 CloudFormation 템플릿을 생성합니다.	쓰기			
GetApp	기존 애플리케이션의 구성 및 상태를 가져옵니다.	Read			
GetAppLaunchConfiguration	기존 애플리케이션에 대한 시작 구성을 가져옵니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetAppReplicationConfiguration	기존 애플리케이션에 대한 복제 구성을 가져옵니다.	Read			
GetConnectors	연결된 모든 커넥터를 가져옵니다.	Read			
GetMessages [권한만 해당]	AWS Server Migration Service에서 서버 마이그레이션 커넥터로 메시지를 가져옵니다.	Read			
GetReplicationJobs	온프레미스 서버를 AWS로 마이그레이션하기 위한 모든 기존 작업을 가져옵니다.	Read			
GetReplicationRuns	기존 작업에 대한 모든 실행을 가져옵니다.	Read			
GetServers	가져온 모든 서버를 가져옵니다.	Read			
ImportServerCatalog	온프레미스 서버의 전체 목록을 수집합니다.	쓰기			
LaunchApp	기존 애플리케이션에 대해 CloudFormation 스택을 생성하고 시작합니다.	쓰기			
ListApps	기존 애플리케이션에 대한 요약의 목록을 가져옵니다.	List			
PutAppLaunchConfiguration	기존 애플리케이션에 대한 시작 구성을 생성하거나 업데이트합니다.	쓰기			
PutAppReplicationConfiguration	기존 애플리케이션에 대한 복제 구성을 생성하거나 업데이트합니다.	쓰기			
SendMessage [권한만 해당]	서버 마이그레이션 커넥터에서 AWS Server Migration Service로 메시지를 전송합니다.	쓰기			
StartAppReplication	기존 애플리케이션에 대한 복제 작업을 생성하고 시작합니다.	쓰기			
StartOnDemandReplicationRun	기존 복제 작업의 복제 실행을 시작합니다.	쓰기			
StopAppReplication	기존 애플리케이션에 대한 복제 작업을 중지하고 삭제합니다.	쓰기			
TerminateApp	기존 애플리케이션에 대한 CloudFormation 스택을 종료합니다.	쓰기			
UpdateApp	기존 애플리케이션 구성을 업데이트합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateReplicationJob	온프레미스 서버를 AWS로 마이그레이션하기 위한 기존 작업을 업데이트합니다.	쓰기			

AWS Server Migration Service에서 정의한 리소스 유형

AWS Server Migration Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Server Migration Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Server Migration Service에 사용되는 조건 키

ServerMigrationService에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Serverless Application Repository에 사용되는 작업, 리소스 및 조건 키

AWS Serverless Application Repository(서비스 접두사: `serverlessrepo`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

주제

AWS Serverless Application Repository에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateApplication	동일한 호출에서 첫 번째 애플리케이션 버전을 생성할 AWS SAM 파일을 비롯하여 애플리케이션을 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateApplicationVersion	애플리케이션 버전을 생성합니다.	쓰기	applications* (p. 1615)		
CreateCloudFormationChangeSet	지정된 애플리케이션에 대한 AWS CloudFormation ChangeSet을 생성합니다.	쓰기	applications* (p. 1615)		
				serverlessrepo:applicationType (p. 1615)	
CreateCloudFormationTemplate	AWS CloudFormation 템플릿을 생성합니다.	쓰기	applications* (p. 1615)		
				serverlessrepo:applicationType (p. 1615)	
DeleteApplication	지정된 애플리케이션을 삭제합니다.	쓰기	applications* (p. 1615)		
GetApplication	지정된 애플리케이션을 가져옵니다.	Read	applications* (p. 1615)		
				serverlessrepo:applicationType (p. 1615)	
GetApplicationPolicy	지정된 애플리케이션에 대한 정책을 가져옵니다.	Read	applications* (p. 1615)		
GetCloudFormationTemplate	지정된 AWS CloudFormation 템플릿을 가져옵니다.	Read	applications* (p. 1615)		
ListApplicationDependencies	컨테이닝 애플리케이션에 중첩된 애플리케이션의 목록을 검색합니다.	List	applications* (p. 1615)		
				serverlessrepo:applicationType (p. 1615)	
ListApplicationVersions	요청자가 소유한 지정된 애플리케이션의 버전을 나열합니다.	List	applications* (p. 1615)		
				serverlessrepo:applicationType (p. 1615)	
ListApplications	요청자가 소유한 애플리케이션을 나열합니다.	List			
PutApplicationPolicy	지정된 애플리케이션에 대한 정책을 적용합니다.	쓰기	applications* (p. 1615)		
SearchApplications	이 사용자에 대한 권한이 있는 애플리케이션을 모두 가져옵니다	Read		serverlessrepo:applicationType (p. 1615)	
UnshareApplication	지정된 애플리케이션의 공유를 해제합니다.	쓰기	applications* (p. 1615)		
UpdateApplication	애플리케이션의 메타데이터를 업데이트합니다	쓰기	applications* (p. 1615)		

AWS Serverless Application Repository에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1613)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
applications	`arn:${Partition}:serverlessrepo:${Region}:${Account}:applications/${ResourceId}`	

AWS Serverless Application Repository의 조건 키

AWS Serverless Application Repository는 `Condition` 정책의 IAM 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
serverlessrepo:applicationType	애플리케이션 유형	문자열

AWS Service Catalog에 사용되는 작업, 리소스 및 조건 키

AWS Service Catalog(서비스 접두사: `servicecatalog`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS Service Catalog에서 정의한 작업 (p. 1615)
- AWS Service Catalog에서 정의한 리소스 유형 (p. 1622)
- AWS Service Catalog에 사용되는 조건 키 (p. 1622)

AWS Service Catalog에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AcceptPortfolioShare	사용자와 공유된 포트폴리오를 허용합니다.	쓰기	Portfolio* (p. 1622)		
AssociateBudgetWithResource	예산을 리소스와 연결합니다.	쓰기			
AssociatePrincipalWithPortfolio	IAM 보안 주체를 포트폴리오와 연결하여, 지정된 포트폴리오와 연결된 제품에 대한 지정된 보안 주체 액세스를 제공합니다.	쓰기	Portfolio* (p. 1622)		
AssociateProductWithPortfolio	제품을 포트폴리오와 연결합니다.	쓰기			
AssociateServiceActionWithProvisioningArtifact	작업을 프로비저닝 아티팩트와 연결합니다.	쓰기	Product* (p. 1622)		
AssociateTagOptionWithResource	지정된 TagOption을 지정된 포트폴리오 또는 제품과 연결합니다.	쓰기	Portfolio (p. 1622)		
			Product (p. 1622)		
BatchAssociateServiceActionWithProvisioningArtifact	여러 셀프 서비스 작업을 프로비저닝 아티팩트와 연결합니다.	쓰기			
BatchDisassociateServiceActionFromProvisioningArtifact	지정된 프로비저닝 아티팩트에서 셀프 서비스 작업 배치를 연결 해제합니다.	쓰기			
CopyProduct	지정된 소스 제품을 지정된 대상 제품 또는 새 제품으로 복사합니다.	쓰기			
CreateConstraint	연결된 제품 및 포트폴리오에 대한 제약을 생성합니다.	쓰기	Product* (p. 1622)		
CreatePortfolio	포트폴리오를 생성합니다.	쓰기	Portfolio* (p. 1622)		
				aws:RequestTag/${TagKey} (p. 1622) aws:TagKeys (p. 1622)	
CreatePortfolioShare	소유한 포트폴리오를 다른 AWS 계정과 공유합니다.	권한 관리	Portfolio* (p. 1622)		
CreateProduct	제품 및 해당 제품의 첫 번째 프로비저닝한 결과물을 생성합니다.	쓰기	Product* (p. 1622)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1622) aws:TagKeys (p. 1622)	
CreateProvisionedProductPlan	새로운 프로비저닝된 제품 계획을 추가합니다.	쓰기			
CreateProvisioningArtifact	기존 제품에 새로운 프로비저닝한 결과물을 추가합니다.	쓰기	Product* (p. 1622)		
CreateServiceAction	셀프 서비스 작업을 생성합니다.	쓰기			
CreateTagOption	TagOption을 생성합니다.	쓰기			
DeleteConstraint	연결된 제품 및 포트폴리오에서 기존 제약을 제거 및 삭제합니다.	쓰기			
DeletePortfolio	포트폴리오에서 모든 연결 및 공유가 제거된 경우 포트폴리오를 삭제합니다.	쓰기	Portfolio* (p. 1622)		
DeletePortfolioShare	이전에 포트폴리오를 공유한 AWS 계정에서 소유한 포트폴리오의 공유를 해제합니다.	권한 관리	Portfolio* (p. 1622)		
DeleteProduct	제품에서 모든 연결이 제거된 경우 제품을 삭제합니다.	쓰기	Product* (p. 1622)		
DeleteProvisionedProductPlan	프로비저닝된 제품 계획을 삭제합니다.	쓰기			
DeleteProvisioningArtifact	제품에서 프로비저닝한 결과물을 삭제합니다.	쓰기	Product* (p. 1622)		
DeleteServiceAction	셀프 서비스 작업을 삭제합니다.	쓰기			
DeleteTagOption	지정된 TagOption을 삭제합니다.	쓰기			
DescribeConstraint	제약을 설명합니다.	Read			
DescribeCopyProductStatus	지정된 제품 복사 작업의 상태를 가져옵니다.	Read			
DescribePortfolio	포트폴리오를 설명합니다.	Read	Portfolio* (p. 1622)		
DescribePortfolioShareStatus	지정된 포트폴리오 공유 작업의 상태를 가져옵니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeProduct	최종 사용자로서 제품을 설명합니다.	Read	Product* (p. 1622)		
DescribeProductAsAdmin	관리자로서 제품을 설명합니다.	Read	Product* (p. 1622)		
DescribeProductView	최종 사용자로서 제품을 설명합니다.	Read			
DescribeProvisionedProduct	프로비저닝된 제품을 설명합니다.	Read			
DescribeProvisionedProductPlan	프로비저닝된 제품 계획을 설명합니다.	Read			
DescribeProvisioningArtifact	프로비저닝한 결과물을 설명합니다.	Read	Product* (p. 1622)		
DescribeProvisioningParameters	지정된 프로비저닝한 결과물을 성공적으로 프로비저닝하기 위해 지정해야 하는 파라미터를 설명합니다.	Read	Product* (p. 1622)		
DescribeRecord	레코드를 설명하고 출력을 나열합니다.	Read		servicecatalog:accountLevel (p. 1622) servicecatalog:roleLevel (p. 1622) servicecatalog:userLevel (p. 1623)	
DescribeServiceAction	셀프 서비스 작업을 설명합니다.	Read			
DescribeServiceActionExecutionParameters	지정된 프로비저닝된 제품에서 지정된 서비스 작업을 실행한 경우 기본 파라미터를 가져옵니다.	Read			
DescribeTagOption	지정된 TagOption에 대한 정보를 가져옵니다.	Read			
DisableAWSOrganizationsAccess	AWS Organizations 기능을 통한 포트폴리오 공유를 비활성화합니다.	쓰기			
DisassociateBudgetFromResource	리소스에서 예산을 연결 해제합니다.	쓰기			
DisassociatePrincipalFromPortfolio	포트폴리오에서 IAM 보안 주체를 연결 해제합니다.	쓰기	Portfolio* (p. 1622)		
DisassociateProductFromPortfolio	포트폴리오에서 제품을 연결 해제합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DisassociateServiceActionFromProvisioningArtifact	지정된 프로비저닝 아티팩트에서 지정된 셀프 서비스 작업 연결을 연결 해제합니다.	쓰기	Product* (p. 1622)		
DisassociateTagOptionFromResource	지정된 리소스에서 지정된 TagOption을 연결 해제합니다.	쓰기	Portfolio (p. 1622)		
			Product (p. 1622)		
EnableAWSOrganizationsAccess	AWS Organizations를 통해 포트폴리오 공유 기능을 활성화합니다.	쓰기			
ExecuteProvisionedProductPlan	프로비저닝된 제품 계획을 실행합니다.	쓰기			
ExecuteProvisionedProductServiceAction	프로비저닝된 제품 계획을 실행합니다.	쓰기			
GetAWSOrganizationsAccessStatus	AWS Organization 포트폴리오 공유 기능의 액세스 상태를 가져옵니다.	Read			
ListAcceptedPortfolioShares	사용자가 수락했고 사용자와 공유된 포트폴리오를 나열합니다.	List			
ListBudgetsForResource	리소스에 연결된 예산을 모두 나열합니다.	List			
ListConstraintsForPortfolio	제공된 포트폴리오와 연결된 제약을 나열합니다.	List			
ListLaunchPaths	최종 사용자로서 제공된 제품을 시작하는 여러 방법을 나열합니다.	List	Product* (p. 1622)		
ListOrganizationPortfolioAccess	지정된 포트폴리오에 대한 액세스 권한이 있는 조직 노드를 나열합니다.	List			
ListPortfolioAccess	제공된 포트폴리오를 공유한 AWS 계정을 나열합니다.	List	Portfolio* (p. 1622)		
ListPortfolios	계정에 속한 포트폴리오를 나열합니다.	List			
ListPortfoliosForProduct	제공된 제품과 연결된 포트폴리오를 나열합니다.	List	Product* (p. 1622)		
ListPrincipalsForPortfolio	제공된 포트폴리오와 연결된 IAM 보안 주체를 나열합니다.	List	Portfolio* (p. 1622)		
ListProvisionedProductPlans	프로비저닝된 제품 계획을 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListProvisioningArtifacts	제공된 제품과 연결된 프로비저닝한 결과물을 나열합니다.	List	Product* (p. 1622)		
ListProvisioningArtifactsForServiceAction	지정된 셀프 서비스 작업에 대한 모든 프로비저닝 아티팩트를 나열합니다.	List			
ListRecordHistory	계정에 속한 모든 레코드 또는 제공된 프로비저닝된 제품에 관련된 모든 레코드를 나열합니다.	List		servicecatalog:accountLevel (p. 1622) servicecatalog:roleLevel (p. 1622) servicecatalog:userLevel (p. 1623)	
ListResourcesForTagOption	지정된 TagOption과 연결된 리소스를 나열합니다.	List			
ListServiceActions	모든 셀프 서비스 작업을 나열합니다.	List			
ListServiceActionsForProvisioningArtifact	계정의 지정된 프로비저닝 아티팩트와 연결된 모든 서비스 작업을 나열합니다.	List	Product* (p. 1622)		
ListStackInstancesForProvisionedProduct	CFN_STACKSET 유형 프로비저닝된 제품과 연결된 각 스택 인스턴스의 계정, 리전 및 상태를 나열합니다.	List			
ListTagOptions	지정된 TagOption 또는 모든 TagOption을 나열합니다.	List			
ProvisionProduct	지정된 프로비저닝한 결과물로 제품을 프로비저닝하고 파라미터를 시작합니다.	쓰기	Product* (p. 1622)		
RejectPortfolioShare	사용자가 이전에 수락한 사용자와 공유된 포트폴리오를 거부합니다.	쓰기	Portfolio* (p. 1622)		
ScanProvisionedProducts	계정에 속한 모든 프로비저닝된 제품을 나열합니다.	List		servicecatalog:accountLevel (p. 1622) servicecatalog:roleLevel (p. 1622) servicecatalog:userLevel (p. 1623)	
SearchProducts	최종 사용자로서 사용할 수 있는 제품을 나열합니다.	List			
SearchProductsAsAdmin	계정에 속한 모든 제품 또는 제공된 포트폴리오와 연결된 모든 제품을 나열합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SearchProvisionedProducts	계정에 속한 모든 프로비저닝된 제품을 나열합니다.	List		servicecatalog:accountLevel (p. 1622) servicecatalog:roleLevel (p. 1622) servicecatalog:userLevel (p. 1623)	
TerminateProvisionedProduct	기존의 프로비저닝된 제품을 종료합니다.	쓰기		servicecatalog:accountLevel (p. 1622) servicecatalog:roleLevel (p. 1622) servicecatalog:userLevel (p. 1623)	
UpdateConstraint	기존 제약의 메타데이터 필드를 업데이트합니다.	쓰기			
UpdatePortfolio	기존 포트폴리오의 메타데이터 필드 및/또는 태그를 업데이트합니다.	쓰기	Portfolio* (p. 1622)		
				aws:RequestTag/${TagKey} (p. 1622) aws:TagKeys (p. 1622)	
UpdateProduct	기존 제품의 메타데이터 필드 및/또는 태그를 업데이트합니다.	쓰기	Product* (p. 1622)		
				aws:RequestTag/${TagKey} (p. 1622) aws:TagKeys (p. 1622)	
UpdateProvisionedProduct	기존 프로비저닝된 제품을 업데이트합니다.	쓰기		servicecatalog:accountLevel (p. 1622) servicecatalog:roleLevel (p. 1622) servicecatalog:userLevel (p. 1623)	
UpdateProvisionedProductProperties	기존 프로비저닝된 제품의 속성을 업데이트합니다.	쓰기			
UpdateProvisioningArtifact	기존 프로비저닝한 결과물의 메타데이터 필드를 업데이트합니다.	쓰기	Product* (p. 1622)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateServiceAction	셀프 서비스 작업을 업데이트합니다.	쓰기			
UpdateTagOption	지정된 TagOption을 업데이트합니다.	쓰기			

AWS Service Catalog에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1615)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
Portfolio	`arn:${Partition}:catalog:${Region}:${Account}:portfolio/${PortfolioId}`	aws:ResourceTag/${TagKey} (p. 1622)
Product	`arn:${Partition}:catalog:${Region}:${Account}:product/${ProductId}`	aws:ResourceTag/${TagKey} (p. 1622)

AWS Service Catalog에 사용되는 조건 키

AWS Service Catalog는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

> **Note**
>
> 이 조건 키가 IAM 정책에서 사용되는 방식을 보여주는 예시 정책은 AWS Service Catalog Administrator Guide의 프로비저닝된 제품 관리에 대한 예시 액세스 정책을 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
servicecatalog:accountLevel	사용자가 계정에 속한 모든 사용자가 생성한 리소스를 보고 이에 대한 작업을 수행할 수 있도록 허용합니다.	문자열
servicecatalog:roleLevel	사용자가 본인 또는 본인과 동일한 역할로 연동한 사용자에 의해 생성된 리소스를 보고 이에 대한 작업을 수행할 수 있도록 허용합니다.	문자열

조건 키	설명	유형
servicecatalog:userLevel	사용자가 본인이 생성한 리소스만 보고 이에 대한 작업을 수행할 수 있도록 허용합니다.	문자열

Service Quotas에 대한 작업, 리소스 및 조건 키

Service Quotas(서비스 접두사: `servicequotas`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Service Quotas에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateServiceQuotaTemplate	Service Quotas 템플릿과 조직을 연결하는 권한을 부여합니다.	쓰기			
DeleteServiceQuotaIncreaseRequestFromTemplate	서비스 할당량 템플릿에서 지정된 서비스 할당량을 제거하는 권한을 부여합니다.	쓰기			
DisassociateServiceQuotaTemplate	조직으로부터 Service Quotas 템플릿을 분리하는 권한을 부여합니다.	쓰기			
GetAWSDefaultServiceQuota	AWS 기본값을 포함한 지정된 서비스 할당량에 대한 세부 정보를 반환할 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetAssociationForServiceQuotaTemplate	Service Quotas 템플릿이 조직과 연결되어 있는지 여부를 알려주는 ServiceQuotaTemplateAssociationStatus 값을 검색할 권한을 부여합니다.	Read			
GetRequestedServiceQuotaChange	특정 서비스 할당량 증가 요청에 대한 세부 정보를 검색할 권한을 부여합니다.	Read			
GetServiceQuota	지정된 값을 포함한 지정된 서비스 할당량에 대한 세부 정보를 반환할 권한을 부여합니다.	Read			
GetServiceQuotaIncreaseRequestFromTemplate	서비스 할당량 템플릿에서 서비스 할당량 증가에 대한 세부 정보를 검색할 권한을 부여합니다.	Read			
ListAWSDefaultServiceQuotas	지정된 AWS 서비스에 대한 모든 기본 서비스 할당량을 나열할 권한을 부여합니다.	Read			
ListRequestedServiceQuotaChangeHistory	서비스에 대한 할당량의 변경 사항 목록을 요청할 권한을 부여합니다.	Read			
ListRequestedServiceQuotaChangeHistoryByQuota	특정 서비스 할당량에 대한 변경 사항 목록을 요청할 권한을 부여합니다.	Read			
ListServiceQuotaIncreaseRequestsInTemplate	서비스 할당량 템플릿에서 서비스 할당량 증가 요청 목록을 반환할 권한을 부여합니다.	Read			
ListServiceQuotas	지정된 AWS 서비스, 해당 계정 및 해당 리전의 모든 서비스 할당량을 나열할 권한을 부여합니다.	Read			
ListServices	Service Quotas에 제공되는 AWS 서비스를 나열할 권한을 부여합니다.	Read			
PutServiceQuotaIncreaseRequestIntoTemplate	서비스 할당량 템플릿에 할당량을 정의하고 추가할 권한을 부여합니다.	쓰기	quota (p. 1625)		
				servicequotas:service (p. 1625)	
RequestServiceQuotaIncrease	서비스 할당량 증가 요청을 제출할 권한을 부여합니다.	쓰기	quota (p. 1625)		
				servicequotas:service (p. 1625)	

Service Quotas에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1623)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
quota	`arn:${Partition}:servicequotas:${Region}:${Account}:${ServiceCode}/${QuotaCode}`	

Service Quotas에 대한 조건 키

Service Quotas는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
servicequotas:service	지정된 AWS 서비스에 대한 액세스를 필터링 또는 제한합니다.	문자열

Amazon SES에 사용되는 작업, 리소스 및 조건 키

Amazon SES(서비스 접두사: `ses`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon SES에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시

됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CloneReceiptRuleSet	기존 수신 규칙 세트를 복제하여 하나를 생성합니다.	쓰기			
CreateConfigurationSet	새로운 구성 세트를 생성합니다.	쓰기			
CreateConfigurationSetEventDestination	구성 세트 이벤트 대상을 생성합니다.	쓰기			
CreateConfigurationSetTrackingOptions	확인 및 이벤트 추적을 위한 구성 세트와 사용자 지정 도메인 간의 연결을 생성합니다.	쓰기			
CreateCustomVerificationEmailTemplate	새 사용자 지정 확인 이메일 템플릿을 생성합니다.	쓰기			
CreateReceiptFilter	새 IP 주소 필터를 생성합니다.	쓰기			
CreateReceiptRule	수신 규칙을 생성합니다.	쓰기			
CreateReceiptRuleSet	빈 수신 규칙 세트를 생성합니다.	쓰기			
CreateTemplate	이메일 템플릿을 생성합니다.	쓰기			
DeleteConfigurationSet	구성 세트를 삭제합니다.	쓰기			
DeleteConfigurationSetEventDestination	구성 세트 이벤트 대상을 삭제합니다.	쓰기			
DeleteConfigurationSetTrackingOptions	확인 및 이벤트 추적을 위한 구성 세트와 사용자 지정 도메인 간의 연결을 삭제합니다.	쓰기			
DeleteCustomVerificationEmailTemplate	기존 사용자 지정 확인 이메일 템플릿을 삭제합니다.	쓰기			
DeleteIdentity	확인된 자격 증명의 목록에서 지정된 자격 증명(이메일 주소 또는 도메인)을 삭제합니다.	쓰기			
DeleteIdentityPolicy	확인된 자격 증명의 목록에서 지정된 자격 증명(이메일 주소 또는 도메인)을 삭제합니다.	쓰기			
DeleteReceiptFilter	지정된 IP 주소 필터를 삭제합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteReceiptRule	지정된 수신 규칙을 삭제합니다.	쓰기			
DeleteReceiptRuleSet	지정된 수신 규칙 세트와 여기에 포함된 모든 수신 규칙을 삭제합니다.	쓰기			
DeleteTemplate	이메일 템플릿을 삭제합니다.	쓰기			
DeleteVerifiedEmailAddress	확인된 주소의 목록에서 지정된 이메일 주소를 삭제합니다.	쓰기			
DescribeActiveReceiptRuleSet	현재 활성화된 수신 규칙 세트에 대한 메타데이터 및 수신 규칙을 반환합니다.	Read			
DescribeConfigurationSet	지정된 구성 세트의 세부 정보를 반환합니다.	Read			
DescribeReceiptRule	지정된 수신 규칙의 세부 정보를 반환합니다.	Read			
DescribeReceiptRuleSet	지정된 수신 규칙 세트의 세부 정보를 반환합니다.	Read			
GetAccountSendingEnabled	현재 리전에 대한 Amazon SES 계정의 이메일 전송 상태를 반환합니다.	Read			
GetCustomVerificationEmailTemplate	지정된 템플릿 이름에 대한 사용자 지정 이메일 확인 템플릿을 반환합니다.	Read			
GetIdentityDkimAttributes	개체에 대한 Easy DKIM 서명의 현재 상태를 반환합니다.	Read			
GetIdentityMailFromDomainAttributes	자격 증명(이메일 주소 및/또는 도메인)의 목록에 대한 사용자 지정 MAIL FROM 속성을 반환합니다.	Read			
GetIdentityNotificationAttributes	확인 자격 증명(이메일 주소 및/또는 도메인)의 목록이 주어진 경우, 자격 증명 알림 속성을 설명하는 구조를 반환합니다.	Read			
GetIdentityPolicies	주어진 자격 증명(이메일 주소 또는 도메인)에 대한 요청된 전송 권한 부여 정책을 반환합니다.	Read			
GetIdentityVerificationAttributes	자격 증명(이메일 주소 및/또는 도메인)의 목록이 주어진 경우, 각 자격 증명에 대한 확인 상태 및 (도메인 자격 증명의 경우) 확인 토큰을 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetSendQuota	사용자의 현재 전송 한도를 반환합니다.	Read			
GetSendStatistics	사용자의 전송 통계를 반환합니다. 결과는 지난 2주 동안의 전송 활동을 나타내는 데이터 요소 목록입니다.	Read			
GetTemplate	지정된 템플릿에 대한 템플릿 객체(제목, HTML 부분 및 텍스트 부분을 포함함)를 반환합니다.	Read			
ListConfigurationSets	현재 AWS 리전에서 Amazon SES 계정과 연결된 구성 세트 목록을 반환합니다.	List			
ListCustomVerificationEmailTemplates	현재 AWS 리전에서 계정에 대한 기존 사용자 지정 확인 이메일 템플릿을 나열합니다.	List			
ListIdentities	확인 상태와 관계 없이, AWS 계정에 대한 모든 자격 증명(이메일 주소 및 도메인)이 포함된 목록을 반환합니다.	List			
ListIdentityPolicies	주어진 자격 증명(이메일 주소 또는 도메인)에 연결된 전송 권한 부여 정책의 목록을 반환합니다.	List			
ListReceiptFilters	AWS 계정과 연결된 IP 주소 필터를 나열합니다.	List			
ListReceiptRuleSets	AWS 계정에 존재하는 수신 규칙 세트를 나열합니다.	List			
ListTemplates	현재 AWS 리전에서 Amazon SES 계정에 있는 이메일 템플릿을 나열합니다.	List			
ListVerifiedEmailAddresses	확인된 모든 이메일 주소가 포함된 목록을 반환합니다.	List			
PutIdentityPolicy	지정된 자격 증명(이메일 주소 또는 도메인)에 대한 전송 권한 부여 정책을 추가하거나 업데이트합니다.	쓰기			
ReorderReceiptRuleSet	수신 규칙 세트 내에서 수신 규칙을 재정렬합니다.	쓰기			
SendBounce	반송 메일 메시지를 생성하여 Amazon SES를 통해 받은 이메일의 발신자에게 보냅니다.	쓰기		ses:FromAddress (p. 1632)	
SendBulkTemplatedEmail	여러 대상으로 보낼 이메일 메시지를 작성합니다.	쓰기	identity* (p. 1632)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				ses:FeedbackAddress (p. 1632) ses:FromAddress (p. 1632) ses:FromDisplayName (p. 1632) ses:Recipients (p. 1632)	
SendCustomVerificationEmail	현재 AWS 리전에서 Amazon SES 계정에 대한 자격 증명의 목록에 이메일 주소를 추가하고 검증을 시도합니다.	쓰기	identity* (p. 1632)		
				ses:FeedbackAddress (p. 1632) ses:FromAddress (p. 1632) ses:FromDisplayName (p. 1632) ses:Recipients (p. 1632)	
SendEmail	입력 데이터를 기반으로 이메일 메시지를 작성한 다음 즉시 메시지를 전송하기 위한 대기열에 넣습니다.	쓰기	identity* (p. 1632)		
				ses:FeedbackAddress (p. 1632) ses:FromAddress (p. 1632) ses:FromDisplayName (p. 1632) ses:Recipients (p. 1632)	
SendRawEmail	클라이언트가 지정한 헤더 및 콘텐츠와 함께 이메일 메시지를 전송합니다.	쓰기	identity* (p. 1632)		
				ses:FeedbackAddress (p. 1632) ses:FromAddress (p. 1632) ses:FromDisplayName (p. 1632) ses:Recipients (p. 1632)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SendTemplatedEmail	이메일 템플릿을 사용하여 이메일 메시지를 작성한 다음 즉시 메시지를 전송하기 위한 대기열에 넣습니다.	쓰기	identity* (p. 1632)		
				ses:FeedbackAddress (p. 1632) ses:FromAddress (p. 1632) ses:FromDisplayName (p. 1632) ses:Recipients (p. 1632)	
SetActiveReceiptRuleSet	지정된 수신 규칙 세트를 활성화 상태의 수신 규칙 세트로 설정합니다.	쓰기			
SetIdentityDkimEnabled	자격 증명에서 전송한 이메일의 Easy DKIM 서명을 활성화하거나 비활성화합니다.	쓰기			
SetIdentityFeedbackForwardingEnabled	자격 증명(이메일 주소 또는 도메인)이 주어진 경우, Amazon SES가 반송 메일 및 수신 거부 알림을 이메일로 전달할지 여부를 활성화하거나 비활성화합니다.	쓰기			
SetIdentityHeadersInNotificationsEnabled	자격 증명(이메일 주소 또는 도메인)이 주어진 경우, Amazon SES가 지정된 유형의 Amazon Simple Notification Service(Amazon SNS) 알림에 원본 이메일 헤더를 포함할지 여부를 설정합니다.	쓰기			
SetIdentityMailFromDomain	확인 자격 증명(이메일 주소 또는 도메인)에 대한 사용자 지정 MAIL FROM 도메인 설정을 활성화하거나 비활성화합니다.	쓰기			
SetIdentityNotificationTopic	자격 증명(이메일 주소 또는 도메인)이 주어진 경우, Amazon SES가 원본으로서 해당 자격 증명과 함께 보낸 이메일에 대한 반송 메일, 수신 거부 및/또는 전송 알림을 게시할 Amazon Simple Notification Service(Amazon SNS) 주제를 설정합니다.	쓰기			
SetReceiptRulePosition	수신 규칙 세트에서 지정된 수신 규칙의 위치를 설정합니다.	쓰기			
TestRenderTemplate	템플릿 및 교체 데이터 세트와 함께 제공된 경우 이메일의 MIME 콘텐츠 미리 보기를 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateAccountSendingEnabled	현재 AWS 리전에서 Amazon SES 전체 계정에 대한 이메일 전송을 활성화하거나 비활성화합니다.	쓰기			
UpdateConfigurationSetEventDestination	구성 세트의 이벤트 대상을 업데이트합니다.	쓰기			
UpdateConfigurationSetReputationMetricsEnabled	주어진 AWS 리전에서 특정 구성 세트를 사용하여 전송되는 이메일에 대한 평판 지표의 게시를 활성화하거나 비활성화합니다.	쓰기			
UpdateConfigurationSetSendingEnabled	주어진 AWS 리전에서 특정 구성 세트를 사용하여 전송되는 메시지에 대한 이메일 전송을 활성화하거나 비활성화합니다.	쓰기			
UpdateConfigurationSetTrackingOptions	확인 및 이벤트 추적을 위한 구성 세트와 사용자 지정 도메인 간의 연결을 수정합니다.	쓰기			
UpdateCustomVerificationEmailTemplate	기존 사용자 지정 확인 이메일 템플릿을 업데이트합니다.	쓰기			
UpdateReceiptRule	수신 규칙을 업데이트합니다.	쓰기			
UpdateTemplate	이메일 템플릿을 업데이트합니다.	쓰기			
VerifyDomainDkim	도메인에 대한 DKIM 토큰 세트를 반환합니다.	Read			
VerifyDomainIdentity	도메인을 확인합니다.	Read			
VerifyEmailAddress	이메일 주소를 확인합니다. 이 작업은 확인 이메일 메시지가 지정된 주소로 전송되게 합니다. 이 작업은 초당 요청 하나로 제한됩니다.	Read			
VerifyEmailIdentity	이메일 주소를 확인합니다. 이 작업은 확인 이메일 메시지가 지정된 주소로 전송되게 합니다. 이 작업은 초당 요청 하나로 제한됩니다.	Read			

Amazon SES에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1625)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	
custom-verification-email-template	`arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${CustomVerificationEmailTemplateName}`	
event-destination	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}:event-destination/${EventDestinationName}`	
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	
receipt-filter	`arn:${Partition}:ses:${Region}:${Account}:receipt-filter/${ReceiptFilterName}`	
receipt-rule	`arn:${Partition}:ses:${Region}:${Account}:receipt-rule-set/${ReceiptRuleSetName}:receipt-rule/${ReceiptRuleName}`	
receipt-rule-set	`arn:${Partition}:ses:${Region}:${Account}:receipt-rule-set/${ReceiptRuleSetName}`	
template	`arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}`	

Amazon SES에 사용되는 조건 키

Amazon SES는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
ses:FeedbackAddress	반송 메일 및 수신 거부가 이메일 피드백 전달로 전송되는 위치를 지정하는 "Return-Path" 주소.	문자열
ses:FromAddress	메시지의 "From" 주소	문자열
ses:FromDisplayName	메시지의 표시 이름으로 사용되는 "From" 주소.	문자열
ses:Recipients	"To", "CC" 및 "BCC" 주소가 포함된 메시지의 수신자 주소.	문자열

Amazon Session Manager Message Gateway Service에 사용되는 작업, 리소스 및 조건 키

Amazon Session Manager Message Gateway Service(서비스 접두사: `ssmmessages`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Session Manager Message Gateway Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateControlChannel	인스턴스가 Systems Manager 서비스에 제어 메시지를 보낼 제어 채널을 등록합니다.	쓰기			
CreateDataChannel	인스턴스가 Systems Manager 서비스에 데이터 메시지를 보낼 데이터 채널을 등록합니다.	쓰기			
OpenControlChannel	인스턴스에서 Systems Manager 서비스까지 등록된 제어 채널 스트림에 대한 웹소켓 연결을 엽니다.	쓰기			
OpenDataChannel	인스턴스에서 Systems Manager 서비스까지 등록된 데이터 채널 스트림에 대한 웹소켓 연결을 엽니다.	쓰기			

Amazon Session Manager Message Gateway Service에서 정의한 리소스 유형

Amazon Session Manager Message Gateway Service는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Session Manager Message Gateway Service에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정합니다.

Amazon Session Manager Message Gateway Service에 사용되는 조건 키

SSM Messages에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Shield에 사용되는 작업, 리소스 및 조건 키

AWS Shield(서비스 접두사: `shield`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Shield에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateDRTLogBucket	DDoS 대응 팀이 흐름 로그가 들어 있는 지정된 Amazon S3 버킷에 액세스하도록 승인합니다.	쓰기			s3:GetBucketPolicy s3:PutBucketPolicy
AssociateDRTRole	DDoS 대응 팀이 잠재적 공격 도중 지정된 역할을 사용해 고객 AWS 계정에 액세스하여 DDoS 공격 완화를 지원하도록 승인합니다.	쓰기			iam:GetRole iam:ListAttachedRolePolic iam:PassRole

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateProtection	지정된 리소스 ARN에 대한 DDoS 보호 서비스를 활성화합니다.	쓰기	protection* (p. 1636)		
CreateSubscription	구독을 활성화합니다.	쓰기			
DeleteProtection	기존 보호를 삭제합니다.	쓰기	protection* (p. 1636)		
DeleteSubscription	구독을 비활성화합니다.	쓰기			
DescribeAttack	공격 세부 정보를 가져옵니다.	Read	attack* (p. 1636)		
DescribeDRTAccess	DDoS 대응 팀이 공격 완화를 지원하는 동안 고객 AWS 계정에 액세스하는 데 사용하는 현재 역할 및 Amazon S3 로그 버킷 목록을 반환합니다.	Read			
DescribeEmergencyContactSettings	공격이 의심될 때 DRT가 고객에게 연락하는 데 사용할 수 있는 이메일 주소를 나열합니다.	Read			
DescribeProtection	보호 세부 정보를 가져옵니다.	Read	protection* (p. 1636)		
DescribeSubscription	구독 세부 정보(예: 시작 시간)를 가져옵니다.	Read			
DisassociateDRTLogBucket	흐름 로그가 들어 있는 지정된 Amazon S3 버킷에 대한 DDoS 대응 팀의 액세스 권한을 제거합니다.	쓰기			s3:DeleteBucketPolicy s3:GetBucketPolicy s3:PutBucketPolicy
DisassociateDRTRole	사용자의 AWS 계정에 대한 DDoS 대응 팀의 액세스 권한을 제거합니다.	쓰기			
GetSubscriptionState	가입 상태를 가져옵니다.	Read			
ListAttacks	기존 공격을 모두 나열합니다.	List			
ListProtections	기존 보호를 모두 나열합니다.	List			
UpdateEmergencyContactSettings	공격이 의심될 때 DRT가 고객에게 연락하는 데 사용할 수 있는 이메일 주소 목록의 세부 정보를 업데이트합니다.	쓰기			
UpdateSubscription	기존 구독의 세부 정보를 업데이트합니다.	쓰기			

AWS Shield에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1634)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
attack	`arn:${Partition}:shield::${Account}:attack/${Id}`	
protection	`arn:${Partition}:shield::${Account}:protection/${Id}`	

AWS Shield의 조건 키

Shield에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Simple Workflow Service에 사용되는 작업, 리소스 및 조건 키

Amazon Simple Workflow Service(서비스 접두사: `swf`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Simple Workflow Service에서 정의한 작업 (p. 1636)
- Amazon Simple Workflow Service에서 정의한 리소스 유형 (p. 1643)
- Amazon Simple Workflow Service의 조건 키 (p. 1643)

Amazon Simple Workflow Service에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelTimer	CancelTimer에 대한 설명	쓰기	domain* (p. 1643)		
CancelWorkflowExecution	CancelWorkflowExecution에 대한 설명	쓰기	domain* (p. 1643)		
CompleteWorkflowExecution	CompleteWorkflowExecution에 대한 설명	쓰기	domain* (p. 1643)		
ContinueAsNewWorkflowExecution	ContinueAsNewWorkflowExecution에 대한 설명	쓰기	domain* (p. 1643)		
CountClosedWorkflowExecutions	지정된 도메인 내에서 지정된 필터링 기준을 충족하는 닫힌 워크플로 실행 수를 반환합니다.	Read	domain* (p. 1643)		
				swf:tagFilter.tag (p. 1643) swf:typeFilter.name (p. 1644) swf:typeFilter.version (p. 1644)	
CountOpenWorkflowExecutions	지정된 도메인 내에서 지정된 필터링 기준을 충족하는 열린 워크플로 실행 수를 반환합니다.	Read	domain* (p. 1643)		
				swf:tagFilter.tag (p. 1643) swf:typeFilter.name (p. 1644) swf:typeFilter.version (p. 1644)	
CountPendingActivityTasks	지정된 작업 목록에서 예상되는 활동 작업 수를 반환합니다.	Read	domain* (p. 1643)		
				swf:taskList.name (p. 1644)	
CountPendingDecisionTasks	지정된 작업 목록에서 예상되는 결정 작업 수를 반환합니다.	Read	domain* (p. 1643)		
				swf:taskList.name (p. 1644)	
DeprecateActivityType	지정된 활동 유형을 사용 중지합니다.	쓰기	domain* (p. 1643)		
				swf:activityType.name (p. 1643) swf:activityType.version (p. 1643)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeprecateDomain	지정된 도메인을 사용 중지합니다.	쓰기	domain* (p. 1643)		
DeprecateWorkflowType	지정된 워크플로 유형을 사용 중지합니다.	쓰기	domain* (p. 1643)		
				swf:workflowType.name (p. 1644) swf:workflowType.version (p. 1644)	
DescribeActivityType	지정된 활동 유형에 대한 정보를 반환합니다.	Read	domain* (p. 1643)		
				swf:activityType.name (p. 1643) swf:activityType.version (p. 1643)	
DescribeDomain	설명 및 상태를 포함하여 지정된 도메인에 대한 정보를 반환합니다.	Read	domain* (p. 1643)		
DescribeWorkflowExecution	유형 및 일부 통계를 포함하여 지정된 워크플로 실행에 대한 정보를 반환합니다.	Read	domain* (p. 1643)		
DescribeWorkflowType	지정된 워크플로 유형에 대한 정보를 반환합니다.	Read	domain* (p. 1643)		
				swf:workflowType.name (p. 1644) swf:workflowType.version (p. 1644)	
FailWorkflowExecution	FailWorkflowExecution에 대한 설명	쓰기	domain* (p. 1643)		
GetWorkflowExecutionHistory	지정된 워크플로 실행 내역을 반환합니다.	Read	domain* (p. 1643)		
ListActivityTypes	지정된 이름 및 등록 상태와 일치하는 지정된 도메인에 등록된 모든 활동에 대한 정보를 반환합니다.	List	domain* (p. 1643)		
ListClosedWorkflowExecutions	지정된 도메인에서 필터링 기준을 충족하는 닫힌 워크플로 실행의 목록을 반환합니다.	List	domain* (p. 1643)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				swf:tagFilter.tag (p. 1643) swf:typeFilter.name (p. 1644) swf:typeFilter.version (p. 1644)	
ListDomains	계정에 등록된 도메인 목록을 반환합니다.	List			
ListOpenWorkflowExecutions	지정된 도메인에서 필터링 기준을 충족하는 열린 워크플로 실행의 목록을 반환합니다.	List	domain* (p. 1643)		
				swf:tagFilter.tag (p. 1643) swf:typeFilter.name (p. 1644) swf:typeFilter.version (p. 1644)	
ListTagsForResource	이 작업은 AWS SWF 리소스에 대한 태그를 나열합니다.	List	domain (p. 1643)		
ListWorkflowTypes	지정된 도메인의 워크플로 유형에 대한 정보를 반환합니다.	List	domain* (p. 1643)		
PollForActivityTask	작업자가 지정된 활동 작업 목록에서 ActivityTask를 가져오는 데 사용됩니다.	쓰기	domain* (p. 1643)		
				swf:taskList.name (p. 1644)	
PollForDecisionTask	결정자가 지정된 결정 작업 목록에서 DecisionTask를 가져오는 데 사용됩니다.	쓰기	domain* (p. 1643)		
				swf:taskList.name (p. 1644)	
RecordActivityTaskHeartbeat	활동 작업자가 지정된 taskToken으로 표시된 ActivityTask가 여전히 진행 중임을 서비스에 보고하는 데 사용됩니다.	쓰기	domain* (p. 1643)		
RecordMarker	RecordMarker에 대한 설명	쓰기	domain* (p. 1643)		
RegisterActivityType	지정된 도메인의 구성 설정과 함께 새 활동 유형을 등록합니다.	쓰기	domain* (p. 1643)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				swf:defaultTaskList.name (p. 1643) swf:name (p. 1643) swf:version (p. 1644)	
RegisterDomain	새 도메인을 등록합니다.	쓰기		aws:TagKeys (p. 1643) aws:RequestTag/${TagKey} (p. 1643)	
RegisterWorkflowType	지정된 도메인에 새 워크플로 유형 및 구성 설정을 등록합니다.	쓰기	domain* (p. 1643)		
				swf:defaultTaskList.name (p. 1643) swf:name (p. 1643) swf:version (p. 1644)	
RequestCancelActivityTask	RequestCancelActivityTask에 대한 설명	쓰기	domain* (p. 1643)		
RequestCancelExternalWorkflowExecution	RequestCancelExternalWorkflowExecution에 대한 설명	쓰기	domain* (p. 1643)		
RequestCancelWorkflowExecution	지정된 도메인, 워크플로 ID 및 실행 ID로 식별되는 현재 실행 중인 워크플로 실행에 WorkflowExecutionCancelRequested 이벤트를 기록합니다.	쓰기	domain* (p. 1643)		
RespondActivityTaskCanceled	작업자가 taskToken으로 식별되는 ActivityTask가 성공적으로 취소되었음을 서비스에 알리는 데 사용됩니다.	쓰기	domain* (p. 1643)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RespondActivityTaskCompleted	작업자가 taskToken으로 식별되는 ActivityTask가 결과(제공된 경우)를 사용하여 성공적으로 완료되었음을 서비스에 알리는 데 사용됩니다.	쓰기	domain* (p. 1643)		
				swf:activityType.name (p. 1643) swf:activityType.version (p. 1643) swf:tagList.member.0 (p. 1643) swf:tagList.member.1 (p. 1643) swf:tagList.member.2 (p. 1643) swf:tagList.member.3 (p. 1643) swf:tagList.member.4 (p. 1644) swf:taskList.name (p. 1644) swf:workflowType.name (p. 1644) swf:workflowType.version (p. 1644)	
RespondActivityTaskFailed	작업자가 taskToken으로 식별되는 ActivityTask가 이유(지정된 경우)로 실패했음을 서비스에 알리는 데 사용됩니다.	쓰기	domain* (p. 1643)		
RespondDecisionTaskCompleted	결정자가 taskToken으로 식별되는 DecisionTask가 성공적으로 완료되었음을 서비스에 알리는 데 사용됩니다.	쓰기	domain* (p. 1643)		
ScheduleActivityTask	ScheduleActivityTask에 대한 설명	쓰기	domain* (p. 1643)		
SignalExternalWorkflowExecution	SignalExternalWorkflowExecution에 대한 설명	쓰기	domain* (p. 1643)		
SignalWorkflowExecution	워크플로 실행 내역에 WorkflowExecutionSignaled 이벤트를 기록하고 지정된 도메인, 워크플로 ID 및 실행 ID로 식별되는 워크플로 실행에 대한 결정 작업을 생성합니다.	쓰기	domain* (p. 1643)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartChildWorkflowExecution	StartChildWorkflowExecution에 대한 설명	쓰기	domain* (p. 1643)		
StartTimer	StartTimer에 대한 설명	쓰기	domain* (p. 1643)		
StartWorkflowExecution	제공된 워크플로 ID 및 입력 데이터를 사용하여 지정된 도메인에서 워크플로 유형의 실행을 시작합니다.	쓰기	domain* (p. 1643)		
				swf:tagList.member.0 (p. 1643) swf:tagList.member.1 (p. 1643) swf:tagList.member.2 (p. 1643) swf:tagList.member.3 (p. 1643) swf:tagList.member.4 (p. 1644) swf:taskList.name (p. 1644) swf:workflowType.name (p. 1644) swf:workflowType.version (p. 1644)	
TagResource	이 작업은 AWS SWF 리소스에 태그를 지정합니다.	태그 지정	domain (p. 1643)		
				aws:TagKeys (p. 1643) aws:RequestTag/${TagKey} (p. 1643)	
TerminateWorkflowExecution	WorkflowExecutionTerminated 이벤트를 기록하고 지정된 도메인, 실행 ID 및 워크플로 ID로 식별되는 워크플로 실행을 강제로 닫습니다.	쓰기	domain* (p. 1643)		
UntagResource	이 작업은 AWS SWF 리소스에서 태그를 제거합니다.	태그 지정	domain (p. 1643)		
				aws:TagKeys (p. 1643)	

Amazon Simple Workflow Service에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1636)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
domain	`arn:${Partition}:swf::${Account}:domain/${DomainName}`	aws:ResourceTag/${TagKey} (p. 1643)

Amazon Simple Workflow Service의 조건 키

Amazon Simple Workflow Service는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 대한 태그입니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 대한 태그입니다.	문자열
aws:TagKeys	키에 대한 태그입니다.	문자열
swf:activityType.name	정책 설명을 지정된 이름의 활동 유형으로만 제한합니다.	문자열
swf:activityType.version	정책 설명을 지정된 버전의 활동 유형으로만 제한합니다.	문자열
swf:defaultTaskList.name	정책 설명을 일치하는 defaultTaskList 이름을 지정하는 요청으로만 제한합니다.	문자열
swf:name	정책 설명을 지정된 이름의 활동 또는 워크플로로만 제한합니다.	문자열
swf:tagFilter.tag	정책 설명을 일치하는 tagFilter.tag 값을 지정하는 요청으로만 제한합니다.	문자열
swf:tagList.member.0	정책 설명을 지정된 태그를 포함하는 요청으로만 제한합니다.	문자열
swf:tagList.member.1	정책 설명을 지정된 태그를 포함하는 요청으로만 제한합니다.	문자열
swf:tagList.member.2	정책 설명을 지정된 태그를 포함하는 요청으로만 제한합니다.	문자열
swf:tagList.member.3	정책 설명을 지정된 태그를 포함하는 요청으로만 제한합니다.	문자열

조건 키	설명	유형
swf:tagList.member.4	정책 설명을 지정된 태그를 포함하는 요청으로만 제한합니다.	문자열
swf:taskList.name	정책 설명을 지정된 이름의 작업 목록을 지정하는 요청으로만 제한합니다.	문자열
swf:typeFilter.name	정책 설명을 지정된 이름의 유형 필터를 지정하는 요청으로만 제한합니다.	문자열
swf:typeFilter.version	정책 설명을 지정된 버전의 유형 필터를 지정하는 요청으로만 제한합니다.	문자열
swf:version	정책 설명을 지정된 버전의 활동 또는 워크플로로만 제한합니다.	문자열
swf:workflowType.name	정책 설명을 지정된 유형의 워크플로로만 제한합니다.	문자열
swf:workflowType.name	정책 설명을 지정된 이름의 워크플로 유형을 지정하는 요청으로만 제한합니다.	문자열
swf:workflowType.version	정책 설명을 지정된 버전의 워크플로 유형을 지정하는 요청으로만 제한합니다.	문자열

Amazon SimpleDB에 사용되는 작업, 리소스 및 조건 키

Amazon SimpleDB(서비스 접두사: `sdb`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon SimpleDB에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchDeleteAttributes	단일 호출에서 여러 DeleteAttributes 작업을 수행하여, 왕복 수 및 지연 시간을 줄입니다.	쓰기	domain* (p. 1645)		
BatchPutAttributes	BatchPutAttributes 작업의 경우, 단일 호출에서 여러 PutAttribute 작업을 수행할 수 있습니다. BatchPutAttributes 작업의 경우, 단일 호출에서 여러 PutAttribute 작업을 수행할 수 있습니다.	쓰기	domain* (p. 1645)		
CreateDomain	CreateDomain 작업은 새 도메인을 생성합니다.	쓰기	domain* (p. 1645)		
DeleteAttributes	항목과 연결된 하나 이상의 속성을 삭제합니다.	쓰기	domain* (p. 1645)		
DeleteDomain	DeleteDomain 작업은 도메인을 삭제합니다.	쓰기	domain* (p. 1645)		
DomainMetadata	도메인이 생성된 시점, 항목 및 속성의 수, 속성 이름 및 값의 크기를 포함하여 도메인에 대한 정보를 반환합니다.	Read	domain* (p. 1645)		
GetAttributes	항목과 연결된 모든 속성을 반환합니다.	Read	domain* (p. 1645)		
ListDomains	ListDomains에 대한 설명	List			
PutAttributes	PutAttributes 작업은 항목에서 속성을 생성하거나 대체합니다.	쓰기	domain* (p. 1645)		
Select	선택에 대한 설명	Read	domain* (p. 1645)		

Amazon SimpleDB에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1644)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
domain	`arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}`	

Amazon SimpleDB에 사용되는 조건 키

SimpleDB에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Snowball에 사용되는 작업, 리소스 및 조건 키

AWS Snowball(서비스 접두사: `snowball`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

AWS Snowball에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelCluster	클러스터 작업을 취소합니다.	쓰기			
CancelJob	지정된 작업을 취소합니다.	쓰기			
CreateAddress	Snowball을 배송할 주소를 생성합니다.	쓰기			
CreateCluster	빈 클러스터를 생성합니다.	쓰기			
CreateJob	Amazon S3와 온프레미스 데이터 센터 간에 데이터를 가져오거나 내보내는 작업을 생성합니다.	쓰기			
DescribeAddress	AddressId를 가져오고 Address 객체의 형식으로 해당 주소에 대한 특정 세부 정보를 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeAddresses	지정된 수의 ADDRESS 객체를 반환합니다.	List			
DescribeCluster	배송 정보, 클러스터 상태 및 기타 중요한 메타데이터를 포함하여 특정 클러스터에 대한 정보를 반환합니다.	Read			
DescribeJob	배송 정보, 작업 상태 및 기타 중요한 메타데이터를 포함하여 특정 작업에 대한 정보를 반환합니다.	Read			
GetJobManifest	지정된 JobId 값과 연결된 매니페스트 파일의 Amazon S3 미리 서명된 URL에 대한 링크를 반환합니다.	Read			
GetJobUnlockCode	지정된 작업에 대한 UnlockCode 코드 값을 반환합니다.	Read			
GetSnowballUsage	계정에 대한 Snowball 서비스 제한과 계정에서 사용 중인 Snowball 수에 대한 정보를 반환합니다.	Read			
ListClusterJobs	지정된 길이의 JobListEntry 객체에 대한 배열을 반환합니다.	List			
ListClusters	지정된 길이의 ClusterListEntry 객체에 대한 배열을 반환합니다.	List			
ListJobs	지정된 길이의 JobListEntry 객체에 대한 배열을 반환합니다.	List			
UpdateCluster	클러스터의 ClusterState 값이 AwaitingQuorum 상태에 있으면 클러스터와 연결된 일부 정보를 업데이트할 수 있습니다.	쓰기			
UpdateJob	작업의 JobState 값이 New이면 작업과 연결된 일부 정보를 업데이트할 수 있습니다.	쓰기			

AWS Snowball에서 정의한 리소스 유형

AWS Snowball은 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Snowball에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Snowball의 조건 키

Snowball에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon SNS에 사용되는 작업, 리소스 및 조건 키

Amazon SNS(서비스 접두사: sns)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon SNS에서 정의한 작업

IAM 정책 설명의 Action 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 Resource 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddPermission	주제의 액세스 제어 정책에 문을 추가해 지정된 작업에 지정된 AWS 계정에 대한 액세스 권한을 부여합니다.	권한 관리	topic* (p. 1651)		
CheckIfPhoneNumberIsOptedOut	전화번호를 수락하고 전화 소지자가 계정의 SMS 메시지 수신을 옵트아웃했는지 여부를 나타냅니다.	Read			
ConfirmSubscription	이전 구독 작업에서 엔드포인트로 전송한 토큰을 확인하여 메시지를 수신하기 위한 엔드포인트 소유자의 의도를 확인합니다.	쓰기	topic* (p. 1651)		
CreatePlatformApplication	디바이스 및 모바일 앱이 등록될 수 있는 지원되는 푸시 알림 서비스(예: APNS 및 GCM) 중 하나를 위해 플랫폼 애플리케이션 객체를 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreatePlatformEndpoint	지원되는 푸시 알림 서비스(예: GCM 및 APNS) 중 하나에 디바이스 및 모바일 앱을 위한 엔드포인트를 생성합니다.	쓰기			
CreateTopic	알림을 게시할 수 있는 주제를 생성합니다.	쓰기	topic* (p. 1651)		
DeleteEndpoint	Amazon SNS에서 디바이스 및 모바일 앱을 위한 엔드포인트를 삭제합니다.	쓰기			
DeletePlatformApplication	지원되는 푸시 알림 서비스(예: APNS 및 GCM) 중 하나에서 플랫폼 애플리케이션 객체를 삭제합니다.	쓰기			
DeleteTopic	주제 및 해당 주제의 모든 구독을 삭제합니다.	쓰기	topic* (p. 1651)		
GetEndpointAttributes	지원되는 푸시 알림 서비스(예: GCM 및 APNS) 중 하나에서 디바이스를 위한 엔드포인트 속성을 검색합니다.	Read			
GetPlatformApplicationAttributes	지원되는 푸시 알림 서비스(예: APNS 및 GCM) 중 하나에 대해 플랫폼 애플리케이션 객체의 속성을 검색합니다.	Read			
GetSMSAttributes	계정의 SMS 메시지를 보내는 설정을 반환합니다.	Read			
GetSubscriptionAttributes	구독의 모든 속성을 반환합니다.	Read			
GetTopicAttributes	주제의 모든 속성을 반환합니다. 반환되는 주제 속성은 사용자의 권한 부여에 따라 다를 수 있습니다.	Read	topic* (p. 1651)		
ListEndpointsByPlatformApplication	지원되는 푸시 알림 서비스(예: GCM 및 APNS)의 디바이스를 위한 엔드포인트 및 엔드포인트 속성을 나열합니다.	List			
ListPhoneNumbersOptedOut	옵트아웃되는(즉, 해당 전화번호로 SMS 메시지를 보낼 수 없음) 전화번호의 목록을 반환합니다.	Read			
ListPlatformApplications	지원되는 푸시 알림 서비스(예: APNS 및 GCM)에 대한 플랫폼 애플리케이션 객체를 나열합니다.	List			
ListSubscriptions	요청자의 구독 목록을 반환합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListSubscriptionsByTopic	특정 주제에 대한 구독 목록을 반환합니다.	List	topic* (p. 1651)		
ListTagsForResource	지정된 Amazon SNS 주제에 추가된 모든 태그를 나열합니다.	Read	topic (p. 1651)		
ListTopics	요청자의 주제 목록을 반환합니다. 각 호출은 최대 100개로 항목으로 제한된 주제 목록을 반환합니다.	List			
OptInPhoneNumber	현재 옵트아웃된 전화번호를 옵트인하여 SMS 메시지를 해당 전화번호로 다시 전송할 수 있게 합니다.	쓰기			
Publish	주제를 구독하는 모든 엔드포인트에 메시지를 전송합니다.	쓰기	topic* (p. 1651)		
RemovePermission	주제의 액세스 제어 정책에서 문을 제거합니다.	권한 관리	topic* (p. 1651)		
SetEndpointAttributes	지원되는 푸시 알림 서비스(예: GCM 및 APNS) 중 하나에서 디바이스를 위한 엔드포인트의 속성을 설정합니다.	쓰기			
SetPlatformApplicationAttributes	지원되는 푸시 알림 서비스(예: APNS 및 GCM) 중 하나에 대해 플랫폼 애플리케이션 객체의 속성을 설정합니다.	쓰기			
SetSubscriptionAttributes	구독 소유자가 주제의 속성을 새 값으로 설정할 수 있도록 허용합니다.	쓰기			
SetTopicAttributes	주제 소유자가 주제의 속성을 새 값으로 설정할 수 있도록 허용합니다.	쓰기	topic* (p. 1651)		
Subscribe	엔드포인트에 확인 메시지를 전송하여 엔드포인트에서 구독할 수 있도록 준비합니다.	쓰기	topic* (p. 1651)		
				sns:Endpoint (p. 1651) sns:Protocol (p. 1652)	
TagResource	지정된 Amazon SNS 주제에 태그를 추가합니다.	태그 지정	topic (p. 1651)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1651) aws:TagKeys (p. 1651)	
Unsubscribe	구독을 삭제합니다. 구독에 삭제 인증이 필요한 경우 구독 또는 주제의 소유자만 구독 해지가 가능하고 AWS 서명이 필요합니다.	쓰기			
UntagResource	지정된 Amazon SNS 주제에서 태그를 제거합니다.	태그 지정	topic (p. 1651)		
				aws:RequestTag/${TagKey} (p. 1651) aws:TagKeys (p. 1651)	

Amazon SNS에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1648)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	

Amazon SNS에 사용되는 조건 키

Amazon SNS는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청의 태그	문자열
aws:TagKeys	요청의 태그 키	문자열
sns:Endpoint	구독 요청 또는 기존에 확인된 구독의 URL, 이메일 주소 또는 ARN입니다.	문자열

조건 키	설명	유형
sns:Protocol	구독 요청 또는 이전에 확인된 구독의 프로토콜 값입니다.	문자열

Amazon SQS에 사용되는 작업, 리소스 및 조건 키

Amazon SQS(서비스 접두사: `sqs`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon SQS에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddPermission	특정 보안 주체에 대한 대기열에 권한을 추가합니다.	권한 관리	queue* (p. 1654)		
ChangeMessageVisibility	대기열에서 지정된 메시지의 제한 시간 초과를 새 값으로 변경합니다.	쓰기	queue* (p. 1654)		
ChangeMessageVisibilityBatch	여러 메시지의 제한 시간 초과를 변경합니다.	쓰기	queue* (p. 1654)		
CreateQueue	새 대기열을 생성하거나 기존 대기열의 URL을 반환합니다.	쓰기	queue* (p. 1654)		
DeleteMessage	지정된 대기열에서 지정된 메시지를 삭제합니다.	쓰기	queue* (p. 1654)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteMessageBatch	지정된 대기열에서 최대 10개의 메시지를 삭제합니다.	쓰기	queue* (p. 1654)		
DeleteQueue	대기열이 비어 있는지 여부에 상관없이 대기열 URL로 지정된 대기열을 삭제합니다.	쓰기	queue* (p. 1654)		
GetQueueAttributes	지정된 대기열에 대한 속성을 가져옵니다.	Read	queue* (p. 1654)		
GetQueueUrl	기존 대기열의 URL을 반환합니다.	Read	queue* (p. 1654)		
ListDeadLetterSourceQueues	배달 못한 편지 대기열로 구성된 RedrivePolicy 대기열 속성이 있는 대기열 목록을 반환합니다.	Read	queue* (p. 1654)		
ListQueueTags	SQS 대기열에 추가된 태그를 나열합니다.	Read	queue* (p. 1654)		
ListQueues	대기열 목록을 반환합니다.	List			
PurgeQueue	대기열 URL로 지정된 대기열에서 메시지를 삭제합니다.	쓰기	queue* (p. 1654)		
ReceiveMessage	지정된 대기열에서 하나 이상의 메시지(메시지 최대 한도 10개)를 검색합니다.	Read	queue* (p. 1654)		
RemovePermission	지정된 레이블 파라미터와 일치하는 대기열 정책에서 권한을 취소합니다.	권한 관리	queue* (p. 1654)		
SendMessage	메시지를 지정된 대기열에 전달합니다.	쓰기	queue* (p. 1654)		
SendMessageBatch	최대 10개의 메시지를 지정된 대기열에 전달합니다.	쓰기	queue* (p. 1654)		
SetQueueAttributes	하나 이상의 대기열 속성 값을 설정합니다.	쓰기	queue* (p. 1654)		
TagQueue	지정된 SQS 대기열에 태그를 추가합니다.	태그 지정	queue* (p. 1654)		
UntagQueue	지정된 SQS 대기열에서 태그를 제거합니다.	태그 지정	queue* (p. 1654)		

Amazon SQS에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1652)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

Note

대기열의 ARN은 IAM 권한 정책에서만 사용됩니다. API 및 CLI 호출에서는 대신 대기열의 URL을 사용합니다.

리소스 유형	ARN	조건 키
queue	`arn:${Partition}:sqs:${Region}:${Account}:${QueueName}`	

Amazon SQS의 조건 키

SQS에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS SSO에 사용되는 작업, 리소스 및 조건 키

AWS SSO(서비스 접두사: `sso`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS SSO에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateDirectory	AWS Single Sign-On에서 사용할 디렉터리를 연결합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateProfile	디렉터리 사용자 또는 그룹과 프로파일 간의 연결을 생성합니다.	쓰기			
CreateApplicationInstance	애플리케이션 인스턴스를 AWS Single Sign-On에 추가합니다.	쓰기			
CreateApplicationInstanceCertificate	애플리케이션 인스턴스에 대한 새 인증서를 추가합니다.	쓰기			
CreateManagedApplicationInstance	AWS Single Sign-On에 관리형 애플리케이션 인스턴스를 추가합니다.	쓰기			
CreatePermissionSet	권한 세트를 생성합니다.	쓰기			
CreateProfile	애플리케이션 인스턴스에 대한 프로파일을 생성합니다.	쓰기			
CreateTrust	대상 계정에서 연동 신뢰를 생성합니다.	쓰기			
DeleteApplicationInstance	애플리케이션 인스턴스를 삭제합니다.	쓰기			
DeleteApplicationInstanceCertificate	애플리케이션 인스턴스에서 비활성 또는 만료된 인증서를 삭제합니다.	쓰기			
DeleteManagedApplicationInstance	관리형 애플리케이션 인스턴스를 삭제합니다.	쓰기			
DeletePermissionSet	권한 세트를 삭제합니다.	쓰기			
DeletePermissionsPolicy	권한 세트와 연결된 권한 정책을 삭제합니다.	쓰기			
DeleteProfile	애플리케이션 인스턴스에 대한 프로파일을 삭제합니다.	쓰기			
DescribePermissionSet	권한 세트와 연결된 모든 권한 정책을 검색합니다.	Read			
DisassociateDirectory	AWS Single Sign-On에서 사용할 디렉터리를 연결 해제합니다.	쓰기			
DisassociateProfile	프로파일에서 디렉터리 사용자 또는 그룹을 연결 해제합니다.	쓰기			
GetApplicationInstance	애플리케이션 인스턴스에 대한 세부 정보를 검색합니다.	Read			
GetApplicationTemplate	애플리케이션 템플릿 세부 정보를 검색합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetManagedApplicationInstance	애플리케이션 인스턴스에 대한 세부 정보를 검색합니다.	Read			
GetMfaDeviceManagementForDirectory	디렉터리에 대한 Mfa Device Management 설정을 검색합니다.	Read			
GetPermissionSet	권한 세트의 세부 정보를 검색합니다.	Read			
GetPermissionsPolicy	권한 세트와 연결된 모든 권한 정책을 검색합니다.	Read			sso:DescribePermissionsI
GetProfile	애플리케이션 인스턴스에 대한 프로파일을 검색합니다.	Read			
GetSSOStatus	AWS Single Sign-On이 활성화되었는지 확인합니다.	Read			
GetSharedSsoConfiguration	현재 SSO 인스턴스에 대한 공유 구성을 검색합니다.	Read			
GetSsoConfiguration	현재 SSO 인스턴스에 대한 구성을 검색합니다.	Read			
GetTrust	대상 계정의 연동 신뢰를 검색합니다.	Read			
ImportApplicationInstanceServiceProviderMetadata	서비스 공급자가 제공한 애플리케이션 SAML 메타데이터 파일을 업로드하여 애플리케이션 인스턴스를 업데이트합니다.	쓰기			
ListApplicationInstanceCertificates	지정된 애플리케이션 인스턴스에 대한 모든 인증서를 검색합니다.	Read			
ListApplicationInstances	모든 애플리케이션 인스턴스를 검색합니다.	List			sso:GetApplicationInstanc
ListApplicationTemplates	지원되는 모든 애플리케이션 템플릿을 검색합니다.	Read			sso:GetApplicationTempla
ListApplications	지원되는 모든 애플리케이션을 검색합니다.	Read			
ListDirectoryAssociations	AWS Single Sign-On에 연결된 디렉터리에 대한 세부 정보를 검색합니다.	Read			
ListPermissionSets	모든 권한 세트를 검색합니다.	Read			
ListProfileAssociations	프로파일과 연결된 디렉터리 사용자 또는 그룹을 검색합니다.	Read			
ListProfiles	애플리케이션 인스턴스에 대한 모든 프로파일을 검색합니다.	Read			sso:GetProfile

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
PutMfaDeviceManagementForDirectory	디렉터리에 대한 Mfa Device Management 설정을 지정합니다.	쓰기			
PutPermissionsPolicy	정책을 권한 세트에 추가합니다.	쓰기			
StartSSO	AWS Single Sign-On을 초기화합니다.	쓰기			
UpdateApplicationInstanceActiveCertificate	인증서를 이 애플리케이션 인스턴스에 대한 활성 인증서로 설정합니다.	쓰기			
UpdateApplicationInstanceDisplayData	애플리케이션 인스턴스의 표시 데이터를 업데이트합니다.	쓰기			
UpdateApplicationInstanceResponseConfiguration	애플리케이션 인스턴스에 대한 연동 응답 구성을 업데이트합니다.	쓰기			
UpdateApplicationInstanceResponseSchemaConfiguration	애플리케이션 인스턴스에 대한 연동 응답 스키마 구성을 업데이트합니다.	쓰기			
UpdateApplicationInstanceSecurityConfiguration	애플리케이션 인스턴스에 대한 보안 세부 정보를 업데이트합니다.	쓰기			
UpdateApplicationInstanceServiceProviderConfiguration	애플리케이션 인스턴스에 대한 서비스 공급자 관련 구성을 업데이트합니다.	쓰기			
UpdateApplicationInstanceStatus	애플리케이션 인스턴스의 상태를 업데이트합니다.	쓰기			
UpdateDirectoryAssociation	연결된 디렉터리에 대한 사용자 속성 매핑을 업데이트합니다.	쓰기			
UpdateManagedApplicationInstanceStatus	관리형 애플리케이션 인스턴스의 상태를 업데이트합니다.	쓰기			
UpdatePermissionSet	권한 세트를 업데이트합니다.	쓰기			
UpdateProfile	애플리케이션 인스턴스에 대한 프로파일을 업데이트합니다.	쓰기			
UpdateSSOConfiguration	현재 SSO 인스턴스에 대한 구성을 업데이트합니다.	쓰기			
UpdateTrust	대상 계정의 연동 신뢰를 업데이트합니다.	쓰기			

AWS SSO에서 정의한 리소스 유형

AWS SSO는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS SSO에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS SSO에 사용되는 조건 키

SSO에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS SSO Directory에 사용되는 작업, 리소스 및 조건 키

AWS SSO Directory(서비스 접두사: `sso-directory`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS SSO Directory에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddMemberToGroup	AWS SSO가 기본적으로 제공하는 디렉터리의 그룹에 멤버를 추가합니다.	쓰기			
CompleteVirtualMfaDeviceRegistration	가상 MFA 디바이스의 생성 프로세스를 완료합니다.	쓰기			
CreateAlias	AWS SSO가 기본적으로 제공하는 디렉터리의 별칭을 생성합니다.	쓰기			
CreateBearerToken	주어진 프로비저닝 테넌트에 대한 보유자 토큰을 생성합니다.	쓰기			
CreateExternalIdPConfigurationForDirectory	디렉터리에 대한 외부 ID 공급자 구성을 생성합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateGroup	AWS SSO가 기본적으로 제공하는 디렉터리에서 그룹을 생성합니다.	쓰기			
CreateProvisioningTenant	지정된 디렉터리에 대한 프로비저닝 테넌트를 생성합니다.	쓰기			
CreateUser	AWS SSO가 기본적으로 제공하는 디렉터리에서 사용자를 생성합니다.	쓰기			
DeleteBearerToken	보유자 토큰을 삭제합니다.	쓰기			
DeleteExternalIdPConfigurationForDirectory	디렉터리에 연결된 외부 ID 공급자 구성을 삭제합니다.	쓰기			
DeleteGroup	AWS SSO가 기본적으로 제공하는 디렉터리에서 그룹을 삭제합니다.	쓰기			
DeleteMfaDeviceForUser	지정된 사용자의 디바이스 이름으로 MFA 디바이스를 삭제합니다.	쓰기			
DeleteProvisioningTenant	프로비저닝 테넌트를 삭제합니다.	쓰기			
DeleteUser	AWS SSO가 기본적으로 제공하는 디렉터리에서 사용자를 삭제합니다.	쓰기			
DescribeDirectory	AWS SSO가 기본적으로 제공하는 디렉터리에 대한 정보를 검색합니다.	Read			
DescribeGroups	AWS SSO가 기본적으로 제공하는 디렉터리에서 그룹에 대한 정보를 검색합니다.	List			
DescribeUsers	AWS SSO가 기본적으로 제공하는 디렉터리에서 사용자에 대한 정보를 검색합니다.	List			
DisableExternalIdPConfigurationForDirectory	외부 ID 공급자를 통해 최종 사용자의 인증을 비활성화합니다.	쓰기			
DisableUser	AWS SSO가 기본적으로 제공하는 디렉터리에서 사용자를 비활성화합니다.	쓰기			
EnableExternalIdPConfigurationForDirectory	외부 ID 공급자를 통해 최종 사용자의 인증을 활성화합니다.	쓰기			
EnableUser	AWS SSO가 기본적으로 제공하는 디렉터리에서 사용자를 활성화합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetAWSSPConfigurationForDirectory	디렉터리에 대한 AWS SSO 서비스 공급자 구성을 검색합니다.	Read			
ListBearerTokens	주어진 프로비저닝 테넌트에 대한 보유자 토큰을 나열합니다.	List			
ListExternalIdPConfigurationsForDirectory	디렉터리에 대해 생성된 모든 외부 ID 공급자 구성을 나열합니다.	List			
ListGroupsForUser	AWS SSO가 기본적으로 제공하는 디렉터리에서 사용자가 속한 그룹을 나열합니다.	List			
ListMembersInGroup	AWS SSO가 기본적으로 제공하는 디렉터리에서 그룹에 속하는 모든 멤버를 검색합니다.	List			
ListMfaDevicesForUser	사용자에 대한 모든 활성 MFA 디바이스와 해당 MFA 디바이스 메타데이터를 나열합니다.	List			
ListProvisioningTenants	주어진 디렉터리에 대한 프로비저닝 테넌트를 나열합니다.	List			
RemoveMemberFromGroup	AWS SSO가 기본적으로 제공하는 디렉터리에서 그룹에 속하는 멤버를 제거합니다.	쓰기			
SearchGroups	연결된 디렉터리에서 그룹을 검색합니다.	Read			
SearchUsers	연결된 디렉터리에서 사용자를 검색합니다.	Read			
StartVirtualMfaDeviceRegistration	가상 MFA 디바이스의 생성 프로세스를 시작합니다.	쓰기			
UpdateExternalIdPConfigurationForDirectory	디렉터리에 연결된 외부 ID 공급자 구성을 업데이트합니다.	쓰기			
UpdateGroup	AWS SSO가 기본적으로 제공하는 디렉터리의 그룹에 대한 정보를 업데이트합니다.	쓰기			
UpdatePassword	AWS SSO가 기본적으로 제공하는 디렉터리에서 사용자에게 이메일을 통해 암호 재설정 링크를 보내거나 일회용 암호를 생성하여 암호를 업데이트합니다.	쓰기			
UpdateUser	AWS SSO가 기본적으로 제공하는 디렉터리에서 사용자 정보를 업데이트합니다.	쓰기			
VerifyEmail	사용자의 이메일 주소를 확인합니다.	쓰기			

AWS SSO Directory에서 정의한 리소스 유형

AWS SSO Directory는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS SSO Directory에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS SSO Directory에 사용되는 조건 키

SSO Directory에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Step Functions에 사용되는 작업, 리소스 및 조건 키

AWS Step Functions(서비스 접두사: `states`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Step Functions에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateActivity	활동을 생성합니다. 활동은 GetActivityTask를 사용하여 Step Functions를 폴링하고 SendTask* API 호출을 사용하여 응답해야 합니다.	태그 지정	activity* (p. 1664)		
				aws:RequestTag/${TagKey} (p. 1664) aws:TagKeys (p. 1664)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateStateMachine	상태 시스템을 생성합니다.	태그 지정	statemachine* (p. 1664)		
				aws:RequestTag/${TagKey} (p. 1664) aws:TagKeys (p. 1664)	
DeleteActivity	활동을 삭제합니다.	쓰기	activity* (p. 1664)		
DeleteStateMachine	상태 시스템을 삭제합니다.	쓰기	statemachine* (p. 1664)		
DescribeActivity	활동을 설명합니다.	Read	activity* (p. 1664)		
DescribeExecution	실행을 설명합니다.	Read	execution* (p. 1664)		
DescribeStateMachine	상태 시스템을 설명합니다.	Read	statemachine* (p. 1664)		
DescribeStateMachineForExecution	실행에 대한 상태 시스템을 설명합니다.	Read	execution* (p. 1664)		
GetActivityTask	작업자가 실행 중인 상태 시스템에서 실행하도록 예약된 작업을 지정된 활동 ARN을 사용하여 검색하는 데 사용됩니다.	쓰기	activity* (p. 1664)		
GetExecutionHistory	지정된 실행 내역을 이벤트 목록으로 반환합니다. 기본적으로 결과는 이벤트 timeStamp의 오름차순으로 반환됩니다.	Read	execution* (p. 1664)		
ListActivities	기존 활동을 나열합니다. 결과는 다중 페이지로 분할할 수 있습니다.	List			
ListExecutions	필터링 기준을 충족하는 상태 시스템의 실행을 나열합니다. 결과는 다중 페이지로 분할할 수 있습니다.	Read	statemachine* (p. 1664)		
ListStateMachines	기존 상태 시스템을 나열합니다. 결과는 다중 페이지로 분할할 수 있습니다.	List			
ListTagsForResource	이 작업은 AWS Step Functions 리소스에 대한 태그를 나열합니다.	Read	activity (p. 1664)		
			statemachine (p. 1664)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SendTaskFailure	작업자가 taskToken으로 식별되는 작업이 실패했음을 보고하는 데 사용됩니다.	쓰기			
SendTaskHeartbeat	작업자가 지정된 taskToken으로 나타내는 작업이 여전히 진행 중임을 서비스에 보고하는 데 사용됩니다.	쓰기			
SendTaskSuccess	작업자가 taskToken으로 식별되는 작업이 성공적으로 완료되었음을 보고하는 데 사용됩니다.	쓰기			
StartExecution	상태 시스템 실행을 시작합니다.	쓰기	statemachine* (p. 1664)		
StopExecution	실행을 중지합니다.	쓰기			
TagResource	이 작업은 AWS Step Functions 리소스에 태그를 지정합니다.	태그 지정	activity (p. 1664)		
			statemachine (p. 1664)		
				aws:TagKeys (p. 1664) aws:RequestTag/${TagKey} (p. 1664)	
UntagResource	이 작업은 AWS Step Functions 리소스에서 태그를 제거합니다.	태그 지정	activity (p. 1664)		
			statemachine (p. 1664)		
				aws:TagKeys (p. 1664)	
UpdateStateMachine	상태 시스템을 업데이트합니다.	쓰기	statemachine* (p. 1664)		
				aws:RequestTag/${TagKey} (p. 1664) aws:TagKeys (p. 1664)	

AWS Step Functions에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1661)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
activity	`arn:${Partition}:states:${Region}:${Account}:activity:${ActivityName}`	aws:ResourceTag/${TagKey} (p. 1664)
execution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}:${ExecutionId}`	
statemachine	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}`	aws:ResourceTag/${TagKey} (p. 1664)

AWS Step Functions의 조건 키

AWS Step Functions는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 대한 태그	문자열
aws:ResourceTag/${TagKey}	리소스에 대한 태그	문자열
aws:TagKeys	키에 대한 태그	문자열

Amazon Storage Gateway에 사용되는 작업, 리소스 및 조건 키

Amazon Storage Gateway(서비스 접두사: `storagegateway`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Storage Gateway에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한

액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ActivateGateway	이 작업은 호스트에 이전에 배포된 게이트웨이를 활성화합니다.	쓰기		aws:RequestTag/${TagKey} (p. 1672) aws:TagKeys (p. 1672)	
AddCache	이 작업은 하나 이상의 게이트웨이 로컬 디스크를 캐싱 볼륨 게이트웨이의 캐시로 구성합니다.	쓰기	gateway* (p. 1672)		
AddTagsToResource	이 작업은 지정된 리소스에 하나 이상의 태그를 추가합니다.	태그 지정	gateway (p. 1672)		
			share (p. 1672)		
			tape (p. 1672)		
			volume (p. 1672)		
				aws:RequestTag/${TagKey} (p. 1672) aws:TagKeys (p. 1672)	
AddUploadBuffer	이 작업은 하나 이상의 게이트웨이 로컬 디스크를 지정된 게이트웨이용 업로드 버퍼로 구성합니다.	쓰기	gateway* (p. 1672)		
AddWorkingStorage	이 작업은 하나 이상의 게이트웨이 로컬 디스크를 게이트웨이용 작업 스토리지로 구성합니다.	쓰기	gateway* (p. 1672)		
AttachVolume	이 작업은 iSCSI 연결에 볼륨을 연결한 다음 지정된 게이트웨이에 해당 볼륨을 연결합니다.	쓰기	gateway* (p. 1672)		
			volume* (p. 1672)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelArchival	보관 프로세스가 시작된 후에는 가상 테이프 선반(VTS)에 가상 테이프의 보관을 취소합니다.	쓰기	gateway* (p. 1672)		
			tape* (p. 1672)		
CancelRetrieval	검색 프로세스가 시작된 후에는 게이트웨이에 대한 가상 테이프 선반(VTS)에서 가상 테이프의 검색을 취소합니다.	쓰기	gateway* (p. 1672)		
			tape* (p. 1672)		
CreateCachediSCSIVolume	이 작업은 지정된 캐싱 게이트웨이에 캐싱 볼륨을 생성합니다. 이 작업은 게이트웨이 캐싱 볼륨 아키텍처에만 지원됩니다.	쓰기	gateway* (p. 1672)		
			volume* (p. 1672)		
				aws:RequestTag/${TagKey} (p. 1672) aws:TagKeys (p. 1672)	
CreateNFSFileShare	이 작업은 기존 파일 게이트웨이에 NFS 파일 공유를 생성합니다.	쓰기	gateway* (p. 1672)		
				aws:RequestTag/${TagKey} (p. 1672) aws:TagKeys (p. 1672)	
CreateSMBFileShare	이 작업은 기존 파일 게이트웨이에 SMB 파일 공유를 생성합니다.	쓰기	gateway* (p. 1672)		
				aws:RequestTag/${TagKey} (p. 1672) aws:TagKeys (p. 1672)	
CreateSnapshot	이번 작업은 볼륨의 스냅샷을 시작합니다.	쓰기	volume* (p. 1672)		
CreateSnapshotFromVolumeRecoveryPoint	이 작업은 볼륨 복구 시점에서 게이트웨이의 스냅샷을 시작합니다.	쓰기	volume* (p. 1672)		
CreateStorediSCSIVolume	이 작업은 지정된 게이트웨이에 볼륨을 생성합니다.	쓰기	gateway* (p. 1672)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:RequestTag/${TagKey} (p. 1672) aws:TagKeys (p. 1672)	
CreateTapeWithBarcode	본인의 바코드를 사용하여 가상 테이프를 생성합니다.	쓰기	gateway* (p. 1672)		
				aws:RequestTag/${TagKey} (p. 1672) aws:TagKeys (p. 1672)	
CreateTapes	하나 이상의 가상 테이프를 생성합니다. 가상 테이프에 데이터를 기록한 다음 테이프를 보관합니다.	쓰기	gateway* (p. 1672)		
				aws:RequestTag/${TagKey} (p. 1672) aws:TagKeys (p. 1672)	
DeleteBandwidthRateLimit	이 작업은 게이트웨이의 대역폭 속도 제한을 삭제합니다.	쓰기	gateway* (p. 1672)		
DeleteChapCredentials	이 작업은 지정된 iSCSI 대상 및 초기자 페어에 대한 CHAP(Challenge-Handshake Authentication Protocol) 자격 증명을 삭제합니다.	쓰기	target* (p. 1672)		
DeleteFileShare	이 작업은 파일 게이트웨이에서 파일 공유를 삭제합니다.	쓰기	share* (p. 1672)		
DeleteGateway	이 작업은 게이트웨이를 삭제합니다.	쓰기	gateway* (p. 1672)		
DeleteSnapshotSchedule	이 작업은 볼륨의 스냅샷을 삭제합니다.	쓰기	volume* (p. 1672)		
DeleteTape	지정된 가상 테이프를 삭제합니다.	쓰기	gateway* (p. 1672)		
			tape* (p. 1672)		
DeleteTapeArchive	가상 테이프 선반(VTS)에서 지정된 가상 테이프를 삭제합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteVolume	이 작업은 CreateCachediSCSIVolume 또는 CreateStorediSCSIVolume API를 사용하여 이전에 생성한 지정된 게이트웨이 볼륨을 삭제합니다.	쓰기	volume* (p. 1672)		
DescribeBandwidthRateLimit	이 작업은 게이트웨이의 대역폭 속도 제한을 반환합니다.	Read	gateway* (p. 1672)		
DescribeCache	이 작업은 게이트웨이의 캐시에 대한 정보를 반환합니다. 이 작업은 게이트웨이 캐싱 볼륨 아키텍처에만 지원됩니다.	Read	gateway* (p. 1672)		
DescribeCachediSCSIVolumes	이 작업은 요청에 지정된 게이트웨이 볼륨의 설명을 반환합니다. 이 작업은 게이트웨이 캐싱 볼륨 아키텍처에만 지원됩니다.	Read	volume* (p. 1672)		
DescribeChapCredentials	이 작업은 지정된 iSCSI 대상 및 대상 초기자 페어에 대한 CHAP(Challenge-Handshake Authentication Protocol) 자격 증명 정보의 배열을 반환합니다.	Read	target* (p. 1672)		
DescribeGatewayInformation	이 작업은 이름, 네트워크 인터페이스, 구성된 시간대 및 상태(게이트웨이가 실행 중인지 여부에 관계 없이) 등 게이트웨이에 대한 메타데이터를 반환합니다.	Read	gateway* (p. 1672)		
DescribeMaintenanceStartTime	이 작업은 주중의 요일 및 시간을 포함한 게이트웨이의 주별 유지 관리 시작 시간을 반환합니다.	Read	gateway* (p. 1672)		
DescribeNFSFileShares	이 작업은 파일 게이트웨이에서 하나 이상의 파일 공유에 대한 설명을 가져옵니다.	Read	share* (p. 1672)		
DescribeSMBFileShares	이 작업은 파일 게이트웨이에서 하나 이상의 파일 공유에 대한 설명을 가져옵니다.	Read	share* (p. 1672)		
DescribeSMBSettings	이 작업은 파일 게이트웨이에서 SMB(Server Message Block) 파일 공유 설정을 가져옵니다.	Read	gateway* (p. 1672)		
DescribeSnapshotSchedule	이 작업은 지정된 게이트웨이 볼륨의 스냅샷 일정을 설명합니다.	Read	volume* (p. 1672)		
DescribeStorediSCSIVolumes	이 작업은 요청에 지정된 게이트웨이 볼륨의 설명을 반환합니다.	Read	volume* (p. 1672)		
DescribeTapeArchives	가상 테이프 선반(VTS)의 지정된 가상 테이프에 대한 설명을 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeTapeRecoveryPoints	지정된 게이트웨이-VTL에 사용 가능한 가상 테이프 복구 시점의 목록을 반환합니다.	Read	gateway* (p. 1672)		
DescribeTapes	가상 테이프의 지정된 Amazon 리소스 이름(ARN)에 대한 설명을 반환합니다.	Read	gateway* (p. 1672)		
DescribeUploadBuffer	이 작업은 게이트웨이의 업로드 버퍼에 대한 정보를 반환합니다.	Read	gateway* (p. 1672)		
DescribeVTLDevices	지정된 게이트웨이의 가상 테이프 라이브러리(VTL) 장치에 대한 설명을 반환합니다.	Read	gateway* (p. 1672)		
DescribeWorkingStorage	이 작업은 게이트웨이의 작업 스토리지에 대한 정보를 반환합니다.	Read	gateway* (p. 1672)		
DetachVolume	이 작업은 iSCSI 연결에서 볼륨을 연결 해제한 다음 지정된 게이트웨이에서 해당 볼륨을 분리합니다.	쓰기	volume* (p. 1672)		
DisableGateway	게이트웨이가 더 이상 작동하지 않을 때 게이트웨이를 비활성화합니다.	쓰기	gateway* (p. 1672)		
JoinDomain	이 작업으로 Active Directory 도메인을 조인할 수 있습니다.	쓰기	gateway* (p. 1672)		
ListFileShares	이 작업은 특정 파일 게이트웨이에 대한 파일 공유의 목록 또는 호출 사용자 계정에 속한 파일 공유의 목록을 가져옵니다.	List	gateway* (p. 1672)		
ListGateways	이 작업은 요청에 지정된 리전의 AWS 계정이 소유한 게이트웨이를 나열합니다. 반환되는 목록은 게이트웨이 ARN(Amazon 리소스 이름) 순으로 반환됩니다.	List			
ListLocalDisks	이 작업은 게이트웨이의 로컬 디스크 목록을 반환합니다.	List	gateway* (p. 1672)		
ListTagsForResource	이 작업은 지정된 리소스에 추가된 태그를 나열합니다.	Read	gateway (p. 1672)		
			share (p. 1672)		
			tape (p. 1672)		
			volume (p. 1672)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListTapes	가상 테이프 라이브러리(VTL) 및 가상 테이프 선반(VTS)의 가상 테이프를 나열합니다.	Read	tape* (p. 1672)		
ListVolumeInitiators	이 작업은 볼륨에 연결된 iSCSI 초기자를 나열합니다.	Read	volume* (p. 1672)		
ListVolumeRecoveryPoints	이 작업은 지정된 게이트웨이의 복구 시점을 나열합니다.	List	gateway* (p. 1672)		
ListVolumes	이 작업은 게이트웨이의 iSCSI 저장 볼륨을 나열합니다.	List	gateway* (p. 1672)		
NotifyWhenUploaded	이 작업은 NFS 파일 공유에 기록된 모든 파일이 Amazon S3로 업로드되면 CloudWatch Events를 통해 사용자에게 알림을 보냅니다.	쓰기	share* (p. 1672)		
RefreshCache	이 작업은 지정된 파일 공유에 대한 캐시를 새로 고칩니다.	쓰기	share* (p. 1672)		
RemoveTagsFromResource	이 작업은 지정된 리소스에서 하나 이상의 태그를 제거합니다.	태그 지정	gateway (p. 1672)		
			share (p. 1672)		
			tape (p. 1672)		
			volume (p. 1672)		
				aws:TagKeys (p. 1672)	
ResetCache	이 작업은 오류가 발생한 모든 캐시 디스크를 재설정하고 디스크를 캐시 스토리지로 재구성에 사용할 수 있게 합니다.	쓰기	gateway* (p. 1672)		
RetrieveTapeArchive	게이트웨이-VTL에 대한 가상 테이프 선반(VTS)에서 보관된 가상 테이프를 검색합니다.	쓰기	gateway* (p. 1672)		
			tape* (p. 1672)		
RetrieveTapeRecoveryPoint	지정된 가상 테이프의 복구 지점을 검색합니다.	쓰기	gateway* (p. 1672)		
			tape* (p. 1672)		
SetLocalConsolePassword	VM 로컬 콘솔의 암호를 설정합니다.	쓰기	gateway* (p. 1672)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SetSMBGuestPassword	SMB 게스트 사용자의 암호를 설정합니다.	쓰기	gateway* (p. 1672)		
ShutdownGateway	이 작업은 게이트웨이를 종료합니다.	쓰기	gateway* (p. 1672)		
StartGateway	이 작업은 이전에 종료된 게이트웨이를 시작합니다.	쓰기	gateway* (p. 1672)		
UpdateBandwidthRateLimit	이 작업은 게이트웨이의 대역폭 속도 제한을 업데이트합니다.	쓰기	gateway* (p. 1672)		
UpdateChapCredentials	이 작업은 지정된 iSCSI 대상에 대한 CHAP(Challenge-Handshake Authentication Protocol) 자격 증명을 업데이트합니다.	쓰기	target* (p. 1672)		
UpdateGatewayInformation	이 작업은 게이트웨이의 이름 및 시간대를 포함하는 게이트웨이의 메타데이터를 업데이트합니다.	쓰기	gateway* (p. 1672)		
UpdateGatewaySoftwareNow	이 작업은 게이트웨이 가상 머신(VM) 소프트웨어를 업데이트합니다.	쓰기	gateway* (p. 1672)		
UpdateMaintenanceStartTime	이 작업은 주중의 요일 및 시간을 포함한 게이트웨이의 주별 유지 관리 시작 시간 정보를 업데이트합니다. 유지 관리 시간은 게이트웨이 시간대의 시간입니다.	쓰기	gateway* (p. 1672)		
UpdateNFSFileShare	이 작업은 NFS 파일 공유를 업데이트합니다.	쓰기	share* (p. 1672)		
UpdateSMBFileShare	이 작업은 SMB 파일 공유를 업데이트합니다.	쓰기	share* (p. 1672)		
UpdateSnapshotSchedule	이 작업은 게이트웨이 볼륨에 구성된 스냅샷 일정을 업데이트합니다.	쓰기	volume* (p. 1672)		
UpdateVTLDeviceType	이 작업은 게이트웨이-VTL의 미디어 체인저의 유형을 업데이트합니다.	쓰기	device* (p. 1672)		

Amazon Storage Gateway에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1664)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
device	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/device/${Vtldevice}`	
gateway	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey} (p. 1672)
share	`arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}`	aws:ResourceTag/${TagKey} (p. 1672)
tape	`arn:${Partition}:storagegateway:${Region}:${Account}:tape/${TapeBarcode}`	aws:ResourceTag/${TagKey} (p. 1672)
target	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/target/${IscsiTarget}`	
volume	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/volume/${VolumeId}`	aws:ResourceTag/${TagKey} (p. 1672)

Amazon Storage Gateway에 사용되는 조건 키

Amazon Storage Gateway는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값의 집합에 따라 생성 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 생성 요청을 필터링합니다.	문자열

Amazon Sumerian에 사용되는 작업, 리소스 및 조건 키

Amazon Sumerian(서비스 접두사: `sumerian`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

주제

- Amazon Sumerian에서 정의한 작업 (p. 1673)

Amazon Sumerian에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
Login	Sumerian 콘솔에 대한 로그인 액세스 권한을 부여합니다.	쓰기			
ViewRelease	프로젝트 릴리스를 볼 수 있는 액세스 권한을 부여합니다.	Read	project* (p. 1673)		

Amazon Sumerian에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1673)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
project	`arn:${Partition}:sumerian:${Region}:${Account}:project:${ProjectName}`	

Amazon Sumerian의 조건 키

Sumerian에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Support에 사용되는 작업, 리소스 및 조건 키

AWS Support(서비스 접두사: `support`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.

- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Support에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

> **Note**
>
> AWS Support에서는 사례를 액세스, 수정 및 해결할 수 있을 뿐만 아니라 Trusted Advisor 작업을 사용할 수 있는 기능을 제공합니다. Support API를 사용하여 Trusted Advisor 관련 작업을 호출하는 경우 “trustedadvisor:*” 작업 중 어떤 작업도 액세스를 제한하지 않습니다. “trustedadvisor:*” 작업은 AWS 콘솔의 Trusted Advisor에만 적용됩니다.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddAttachmentsToSet	AWS Support 사례에 하나 이상의 연결을 추가합니다.	쓰기			
AddCommunicationToCase	AWS Support 사례에 고객 커뮤니케이션을 추가합니다.	쓰기			
CreateCase	새로운 AWS Support 사례를 생성합니다.	쓰기			
DescribeAttachment	연결에 대한 설명을 반환합니다.	Read			
DescribeCaseAttributes	보조 서비스가 AWS Support 사례 속성을 읽을 수 있도록 허용하는 내부 관리형 함수입니다.	Read			
DescribeCases	지정된 입력과 일치하는 AWS Support 사례 목록을 반환합니다.	Read			
DescribeCommunications	하나 이상의 AWS Support 사례에 대한 커뮤니케이션 및 연결을 반환합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeIssueTypes	AWS Support 사례의 문제 유형을 반환합니다.	Read			
DescribeServices	AWS 서비스와 각 서비스에 적용되는 카탈로그의 현재 목록을 반환합니다.	Read			
DescribeSeverityLevels	AWS Support 사례에 할당될 수 있는 심각도 수준의 목록을 반환합니다.	Read			
DescribeSupportLevel	AWS 계정 식별자에 대한 지원 수준을 반환합니다.	Read			
DescribeTrustedAdvisorCheckRefreshStatuses	점검 식별자 목록을 기준으로 Trusted Advisor 새로 고침 점검의 상태를 반환합니다.	Read			
DescribeTrustedAdvisorCheckResult	지정된 점검 식별자가 있는 Trusted Advisor 점검의 결과를 반환합니다.	Read			
DescribeTrustedAdvisorCheckSummaries	지정된 점검 식별자가 있는 Trusted Advisor 점검의 결과에 대한 요약을 반환합니다.	Read			
DescribeTrustedAdvisorChecks	이름, 식별자, 범주 및 설명을 포함하여 사용 가능한 모든 Trusted Advisor 점검 목록을 반환합니다.	Read			
InitiateCallForCase	AWS 지원 센터에서 호출을 시작하는 내부 관리형 함수입니다.	쓰기			
InitiateChatForCase	AWS 지원 센터에서 채팅을 시작하는 내부 관리형 함수입니다.	쓰기			
PutCaseAttributes	보조 서비스가 AWS Support 사례에 속성을 연결할 수 있도록 허용하는 내부 관리형 함수입니다.	쓰기			
RateCaseCommunication	AWS Support 사례 커뮤니케이션을 평가합니다.	쓰기			
RefreshTrustedAdvisorCheck	지정된 점검 식별자가 있는 Trusted Advisor 점검의 새로 고침을 요청합니다.	쓰기			
ResolveCase	AWS Support 사례를 해결합니다.	쓰기			
SearchForCases	지정된 입력과 일치하는 AWS Support 사례 목록을 반환합니다.	Read			

AWS Support에서 정의한 리소스 유형

AWS Support는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. AWS Support에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

AWS Support에 사용되는 조건 키

Support에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Systems Manager에 사용되는 작업, 리소스 및 조건 키

AWS Systems Manager(서비스 접두사: `ssm`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Systems Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddTagsToResource	지정된 AWS 리소스에 대해 하나 이상의 태그를 추가 또는 덮어쓸 수 있는 권한을 부여합니다.	태그 지정	document (p. 1687)		
			maintenancewindow (p. 1687)		
			managed-instance (p. 1687)		
			parameter (p. 1688)		
			patchbaseline (p. 1688)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CancelCommand	지정된 Run Command 명령을 취소할 수 있는 권한을 부여합니다.	쓰기			
CancelMaintenanceWindowExecution	진행 중인 유지 관리 기간 실행을 취소할 수 있는 권한을 부여합니다.	쓰기			
CreateActivation	온프레미스 서버 및 가상 머신(VM)을 Systems Manager에 등록하는 데 사용되는 활성화를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateAssociation	지정된 Systems Manager 문서를 지정된 인스턴스 또는 다른 대상과 연결할 수 있는 권한을 부여합니다.	쓰기	document* (p. 1687)		
CreateAssociationBatch	단일 명령으로 여러 CreateAssociation 작업의 항목을 결합할 수 있는 권한을 부여합니다.	쓰기	document* (p. 1687)		
CreateDocument	Systems Manager SSM 문서를 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/ ${TagKey} (p. 1688) aws:TagKeys (p. 1688)	iam:PassRole
CreateMaintenanceWindow	유지 관리 기간을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/ ${TagKey} (p. 1688) aws:TagKeys (p. 1688)	
CreateOpsItem	OpsCenter에서 OpsItem을 생성할 수 있는 권한을 부여합니다.	쓰기			
CreatePatchBaseline	패치 기준을 생성할 수 있는 권한을 부여합니다.	쓰기		aws:RequestTag/ ${TagKey} (p. 1688) aws:TagKeys (p. 1688)	
CreateResourceDataSync	리소스 데이터 동기화 구성을 생성할 수 있는 권한을 부여합니다. 이 권한은 관리형 인스턴스에서 인벤토리 데이터를 정기적으로 수집하고 Amazon S3 버킷에서 해당 데이터를 업데이트합니다.	쓰기	resourcedatasync* (p. 1688)		
				ssm:SyncType (p. 1689)	
DeleteActivation	관리형 인스턴스에 대해 지정된 활성화를 삭제할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteAssociation	지정된 인스턴스에서 지정된 SSM 문서의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기	document* (p. 1687)		
DeleteDocument	지정된 SSM 문서와 해당 인스턴스 연결을 삭제할 수 있는 권한을 부여합니다.	쓰기	document* (p. 1687)		
DeleteInventory	지정된 사용자 지정 인벤토리 유형 또는 사용자 지정 인벤토리 유형과 연결된 데이터를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteMaintenanceWindow	지정된 유지 관리 기간을 삭제할 수 있는 권한을 부여합니다.	쓰기	maintenancewindow* (p. 1687)		
DeleteParameter	지정된 SSM 파라미터를 삭제할 수 있는 권한을 부여합니다.	쓰기	parameter* (p. 1688)		
DeleteParameters	여러 개의 지정된 SSM 파라미터를 삭제할 수 있는 권한을 부여합니다.	쓰기	parameter* (p. 1688)		
DeletePatchBaseline	지정된 패치 기준을 삭제할 수 있는 권한을 부여합니다.	쓰기	patchbaseline* (p. 1688)		
DeleteResourceDataSync	지정된 리소스 데이터 동기화를 삭제할 수 있는 권한을 부여합니다.	쓰기	resourcedatasync* (p. 1688)		
				ssm:SyncType (p. 1689)	
DeregisterManagedInstance	Systems Manager에서 지정된 온프레미스 서버 또는 가상 머신(VM)의 등록을 취소할 수 있는 권한을 부여합니다.	쓰기	managed-instance* (p. 1687)		
DeregisterPatchBaselineForPatchGroup	지정된 패치 기준이 지정된 패치 그룹의 기본 패치 기준이 되지 않도록 등록을 취소할 수 있는 권한을 부여합니다.	쓰기	patchbaseline* (p. 1688)		
DeregisterTargetFromMaintenanceWindow	유지 관리 기간에서 지정된 대상의 등록을 취소할 수 있는 권한을 부여합니다.	쓰기	maintenancewindow* (p. 1687)		
DeregisterTaskFromMaintenanceWindow	유지 관리 기간에서 지정된 작업의 등록을 취소할 수 있는 권한을 부여합니다.	쓰기	maintenancewindow* (p. 1687)		
DescribeActivations	지정된 관리형 인스턴스 활성화에 대한 세부 정보(예: 생성 시점 및 활성화를 사용하여 등록된 인스턴스 수)를 볼 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeAssociation	지정된 인스턴스 또는 대상의 지정된 연결에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	document* (p. 1687)		
DescribeAssociationExecutionTargets	지정된 연결 실행에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read			
DescribeAssociationExecutions	지정된 연결에 대한 모든 실행을 볼 수 있는 권한을 부여합니다.	Read			
DescribeAutomationExecutions	모든 활성 및 종료된 자동화 실행에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
DescribeAutomationStepExecutions	자동화 워크플로에서 모든 활성 및 종료된 단계 실행에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read			
DescribeAvailablePatches	패치 기준에 포함할 수 있는 모든 패치를 볼 수 있는 권한을 부여합니다.	Read			
DescribeDocument	지정된 SSM 문서에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	document* (p. 1687)		
DescribeDocumentParameters	Systems Manager 콘솔에서 SSM 문서 파라미터에 대한 정보를 표시할 수 있는 권한을 부여합니다(내부 Systems Manager 작업).	Read	document* (p. 1687)		
DescribeDocumentPermission	지정된 SSM 문서에 대한 권한을 볼 수 있는 권한을 부여합니다.	Read	document* (p. 1687)		
DescribeEffectiveInstanceAssociations	지정된 인스턴스에 대한 모든 현재 연결을 볼 수 있는 권한을 부여합니다.	Read			
DescribeEffectivePatchesForPatchBaseline	지정된 패치 기준과 현재 연결된 패치에 대한 세부 정보를 볼 수 있는 권한을 부여합니다(Windows에만 해당).	Read	patchbaseline* (p. 1688)		
DescribeInstanceAssociationsStatus	지정된 인스턴스에 대한 연결 상태를 볼 수 있는 권한을 부여합니다.	Read			
DescribeInstanceInformation	지정된 인스턴스에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
DescribeInstancePatchStates	지정된 인스턴스의 패치에 대한 상태 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeInstancePatchStatesForPatchGroup	지정된 패치 그룹의 인스턴스에 대한 상위 수준 패치 상태를 설명할 수 있는 권한을 부여합니다.	Read			
DescribeInstancePatches	지정된 인스턴스의 패치에 대한 일반 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
DescribeInstanceProperties	사용자의 Amazon EC2 콘솔에 관리형 인스턴스의 노드를 렌더링할 수 있는 권한을 부여합니다.	Read			
DescribeInventoryDeletions	지정된 인벤토리 삭제에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
DescribeMaintenanceWindowExecutionTaskInvocations	유지 관리 기간에 대해 지정된 작업 실행의 세부 정보를 볼 수 있는 권한을 부여합니다.	List			
DescribeMaintenanceWindowExecutionTasks	지정된 유지 관리 기간 실행 중에 실행된 작업에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	List			
DescribeMaintenanceWindowExecutions	지정된 유지 관리 기간의 실행을 볼 수 있는 권한을 부여합니다.	List	maintenancewindow* (p. 1687)		
DescribeMaintenanceWindowSchedule	지정된 유지 관리 기간의 예정된 실행에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	List			
DescribeMaintenanceWindowTargets	지정된 유지 관리 기간과 연결된 대상 등록을 볼 수 있는 권한을 부여합니다.	List	maintenancewindow* (p. 1687)		
DescribeMaintenanceWindowTasks	지정된 유지 관리 기간과 연결된 작업 등록을 볼 수 있는 권한을 부여합니다.	List	maintenancewindow* (p. 1687)		
DescribeMaintenanceWindows	모든 유지 관리 기간 또는 지정된 유지 관리 기간에 대한 정보를 볼 수 있는 권한을 부여합니다.	List			
DescribeMaintenanceWindowsForTarget	지정된 인스턴스와 연결된 유지 관리 기간 대상 및 작업에 대한 정보를 볼 수 있는 권한을 부여합니다.	List			
DescribeOpsItems	지정된 OpsItems에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
DescribeParameters	지정된 SSM 파라미터에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribePatchBaselines	지정된 조건을 충족하는 패치 기준에 대한 정보를 볼 수 있는 권한을 부여합니다.	List			
DescribePatchGroupState	지정된 패치 그룹에 대한 패치의 전체 상태 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
DescribePatchGroups	지정된 패치 그룹의 패치 기준에 대한 정보를 볼 수 있는 권한을 부여합니다.	List			
DescribePatchProperties	지정된 운영 체제 및 패치 속성에 대해 사용 가능한 패치의 세부 정보를 볼 수 있는 권한을 부여합니다.	List			
DescribeSessions	지정된 검색 조건을 충족하는 최근 Session Manager 세션 목록을 볼 수 있는 권한을 부여합니다.	List			
GetAutomationExecution	지정된 자동화 실행의 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
GetCommandInvocation	지정된 호출 또는 플러그인의 명령 실행에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
GetConnectionStatus	지정된 관리형 인스턴스에 대한 Session Manager 연결 상태를 볼 수 있는 권한을 부여합니다.	Read			
GetDefaultPatchBaseline	지정된 운영 체제 유형에 대한 현재 기본 패치 기준을 볼 수 있는 권한을 부여합니다.	Read	patchbaseline* (p. 1688)		
GetDeployablePatchSnapshotForInstance	지정된 인스턴스에 대한 현재 패치 기준 스냅샷을 검색할 수 있는 권한을 부여합니다.	Read			
GetDocument	지정된 SSM 문서의 콘텐츠를 볼 수 있는 권한을 부여합니다.	Read	document* (p. 1687)		
GetInventory	지정된 기준에 따라 인스턴스 인벤토리 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
GetInventorySchema	지정된 인벤토리 항목 유형에 대한 인벤토리 유형 또는 속성 이름 목록을 볼 수 있는 권한을 부여합니다.	Read			
GetMaintenanceWindow	지정된 유지 관리 기간에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	maintenancewindow* (p. 1687)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetMaintenanceWindowExecution	지정된 유지 관리 기간 실행에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
GetMaintenanceWindowExecutionTask	지정된 유지 관리 기간 실행 작업에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
GetMaintenanceWindowExecutionTaskInvocation	특정 대상에서 실행 중인 특정 유지 관리 기간 작업에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read			
GetMaintenanceWindowTask	지정된 유지 관리 기간에 등록된 작업에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	maintenancewindow* (p. 1687)		
GetManifest	Systems Manager 및 SSM 에이전트가 인스턴스에 대한 패키지 설치 요구 사항을 결정하는 데 사용합니다(내부 Systems Manager 호출).	Read			
GetOpsItem	지정된 OpsItem에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read			
GetOpsSummary	지정된 필터 및 수집기를 기준으로 OpsItem에 대한 요약 정보를 볼 수 있는 권한을 부여합니다.	Read	resourcedatasync* (p. 1688)		
GetParameter	지정된 파라미터에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read	parameter* (p. 1688)		
GetParameterHistory	지정된 파라미터에 대한 세부 정보 및 변경 사항을 볼 수 있는 권한을 부여합니다.	Read	parameter* (p. 1688)		
GetParameters	지정된 여러 파라미터에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read	parameter* (p. 1688)		
GetParametersByPath	지정된 계층 구조의 파라미터에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read	parameter* (p. 1688)		
GetPatchBaseline	지정된 패치 기준에 대한 정보를 볼 수 있는 권한을 부여합니다.	Read	patchbaseline* (p. 1688)		
GetPatchBaselineForPatchGroup	지정된 패치 그룹에 대한 현재 패치 기준의 ID를 볼 수 있는 권한을 부여합니다.	Read	patchbaseline* (p. 1688)		
GetServiceSetting	AWS 서비스에 대한 계정 수준 설정을 볼 수 있는 권한을 부여합니다.	Read	servicesetting* (p. 1688)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
LabelParameterVersion	파라미터의 지정된 버전에 식별 레이블을 적용할 수 있는 권한을 부여합니다.	쓰기	parameter* (p. 1688)		
ListAssociationVersions	지정된 연결의 버전을 나열할 수 있는 권한을 부여합니다.	List			
ListAssociations	지정된 SSM 문서 또는 관리형 인스턴스에 대한 연결을 나열할 수 있는 권한을 부여합니다.	List			
ListCommandInvocations	지정된 인스턴스로 전송된 명령 호출에 대한 정보를 나열할 수 있는 권한을 부여합니다.	Read			
ListCommands	지정된 인스턴스에 전송된 명령을 나열할 수 있는 권한을 부여합니다.	Read			
ListComplianceItems	지정된 리소스의 지정된 리소스 유형에 대한 규정 준수 상태를 나열할 수 있는 권한을 부여합니다.	List			
ListComplianceSummaries	지정된 규정 준수 유형에 대한 규정 준수 및 비준수 리소스의 요약 수를 나열할 수 있는 권한을 부여합니다.	List			
ListDocumentVersions	지정된 문서의 모든 버전을 나열할 수 있는 권한을 부여합니다.	List	document* (p. 1687)		
ListDocuments	지정된 SSM 문서에 대한 정보를 볼 수 있는 권한을 부여합니다.	List			
ListInstanceAssociations	새 State Manager 연결을 확인하기 위해 SSM Agent에서 사용됩니다(내부 Systems Manager 호출).	List			
ListInventoryEntries	지정된 인스턴스에 대해 지정된 인벤토리 유형 목록을 볼 수 있는 권한을 부여합니다.	List			
ListResourceComplianceSummaries	리소스 수준 요약 개수를 나열할 수 있는 권한을 부여합니다.	List			
ListResourceDataSync	계정의 리소스 데이터 동기화 구성에 대한 정보를 나열할 수 있는 권한을 부여합니다.	List		ssm:SyncType (p. 1689)	
ListTagsForResource	지정된 리소스에 대한 리소스 태그 목록을 볼 수 있는 권한을 부여합니다.	Read	document (p. 1687)		
			maintenancewindow (p. 1687)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			managed-instance (p. 1687)		
			parameter (p. 1688)		
			patchbaseline (p. 1688)		
ModifyDocumentPermission	사용자 지정 SSM 문서를 특정 AWS 계정과 공개 또는 비공개로 공유할 수 있는 권한을 부여합니다.	쓰기	document* (p. 1687)		
PutComplianceItems	지정된 리소스에 규정 준수 유형 및 기타 규정 준수 세부 정보를 등록할 수 있는 권한을 부여합니다.	쓰기			
PutConfigurePackageResult	SSM 에이전트에서 특정 에이전트 업데이트 결과 보고서를 생성하는 데 사용됩니다(내부 Systems Manager 호출).	Read			
PutInventory	지정된 여러 관리형 인스턴스에서 인벤토리 항목을 추가하거나 업데이트할 수 있는 권한을 부여합니다.	쓰기			
PutParameter	SSM 파라미터를 생성할 수 있는 권한을 부여합니다.	쓰기	parameter* (p. 1688)		
				aws:RequestTag/${TagKey} (p. 1688) aws:TagKeys (p. 1688)	
RegisterDefaultPatchBaseline	운영 체제 유형에 대한 기본 패치 기준을 지정할 수 있는 권한을 부여합니다.	쓰기	patchbaseline* (p. 1688)		
RegisterPatchBaselineForPatchGroup	지정된 패치 그룹에 대한 기본 패치 기준을 지정할 수 있는 권한을 부여합니다.	쓰기	patchbaseline* (p. 1688)		
RegisterTargetWithMaintenanceWindow	지정된 유지 관리 기간에 대상을 등록할 수 있는 권한을 부여합니다.	쓰기	maintenancewindow* (p. 1687)		
RegisterTaskWithMaintenanceWindow	지정된 유지 관리 기간에 작업을 등록할 수 있는 권한을 부여합니다.	쓰기	maintenancewindow* (p. 1687)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RemoveTagsFromResource	지정된 리소스에서 지정된 태그 키를 제거할 수 있는 권한을 부여합니다.	태그 지정	document (p. 1687)		
			maintenancewindow (p. 1687)		
			managed-instance (p. 1687)		
			parameter (p. 1688)		
			patchbaseline (p. 1688)		
ResetServiceSetting	AWS 계정의 서비스 설정을 기본값으로 재설정할 수 있는 권한을 부여합니다.	쓰기	servicesetting* (p. 1688)		
ResumeSession	관리형 인스턴스에 Session Manager 세션을 다시 연결할 수 있는 권한을 부여합니다.	쓰기	session* (p. 1688)		
SendAutomationSignal	지정된 자동화 실행의 현재 동작 또는 상태를 변경하기 위한 신호를 보낼 수 있는 권한을 부여합니다.	쓰기			
SendCommand	하나 이상의 지정된 관리형 인스턴스에서 명령을 실행할 수 있는 권한을 부여합니다.	쓰기	document* (p. 1687)		
			instance (p. 1687)		
			managed-instance (p. 1687)		
				aws:ResourceTag/${TagKey} (p. 1688) ssm:resourceTag/tag-key (p. 1689)	
StartAssociationsOnce	지정된 연결을 수동으로 실행할 수 있는 권한을 부여합니다.	쓰기			
StartAutomationExecution	자동화 문서의 실행을 시작할 수 있는 권한을 부여합니다.	쓰기	document* (p. 1687)		
StartSession	Session Manager 세션에 대해 지정된 대상에 대한 연결을 시작할 수 있는 권한을 부여합니다.	쓰기	instance* (p. 1687)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			document (p. 1687)		
				ssm:SessionDocumentAccessCheck (p. 1689)	
StopAutomationExecution	이미 진행 중인 지정된 자동화 실행을 중지할 수 있는 권한을 부여합니다.	쓰기			
TerminateSession	인스턴스에 대한 Session Manager 연결을 영구적으로 종료할 수 있는 권한을 부여합니다.	쓰기	session* (p. 1688)		
UpdateAssociation	연결을 업데이트하고 지정된 대상에서 연결을 즉시 실행할 수 있는 권한을 부여합니다.	쓰기			
UpdateAssociationStatus	지정된 인스턴스와 연결된 SSM 문서의 상태를 업데이트할 수 있는 권한을 부여합니다.	쓰기	document (p. 1687)		
UpdateDocument	SSM 문서에 대해 하나 이상의 값을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateDocumentDefaultVersion	SSM 문서의 기본 버전을 변경할 수 있는 권한을 부여합니다.	쓰기			
UpdateInstanceAssociationStatus	SSM 에이전트가 현재 실행 중인 연결 상태를 업데이트하는 데 사용합니다(내부 Systems Manager 호출).	쓰기			
UpdateInstanceInformation	SSM 에이전트가 클라우드의 Systems Manager 서비스에 하트비트 신호를 보내는 데 사용합니다.	쓰기			
UpdateMaintenanceWindow	지정된 유지 관리 기간을 업데이트할 수 있는 권한을 부여합니다.	쓰기	maintenancewindow* (p. 1687)		
UpdateMaintenanceWindowTarget	지정된 유지 관리 기간 대상을 업데이트할 수 있는 권한을 부여합니다.	쓰기	maintenancewindow* (p. 1687)		
UpdateMaintenanceWindowTask	지정된 유지 관리 기간 작업을 업데이트할 수 있는 권한을 부여합니다.	쓰기	maintenancewindow* (p. 1687)		
UpdateManagedInstanceRole	지정된 관리형 인스턴스에 할당된 IAM 역할을 할당하거나 변경할 수 있는 권한을 부여합니다.	쓰기	managed-instance* (p. 1687)		
UpdateOpsItem	OpsItem을 편집하거나 변경할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdatePatchBaseline	지정된 패치 기준을 업데이트할 수 있는 권한을 부여합니다.	쓰기	patchbaseline* (p. 1688)		
UpdateResourceDataSync	리소스 데이터 동기화를 업데이트할 수 있는 권한을 부여합니다.	쓰기	resourcedatasync* (p. 1688)		
				ssm:SyncType (p. 1689)	
UpdateServiceSetting	AWS 계정의 서비스 설정을 업데이트할 수 있는 권한을 부여합니다.	쓰기	servicesetting* (p. 1688)		

AWS Systems Manager에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1676)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
association	`arn:${Partition}:ssm:${Region}:${Account}:association/${AssociationId}`	
automation-execution	`arn:${Partition}:ssm:${Region}:${Account}:automation-execution/${AutomationExecutionId}`	
automation-definition	`arn:${Partition}:ssm:${Region}:${Account}:automation-definition/${AutomationDefinitionName:VersionId}`	
document	`arn:${Partition}:ssm:${Region}:${Account}:document/${DocumentName}`	aws:ResourceTag/${TagKey} (p. 1688) ssm:resourceTag/tag-key (p. 1689)
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey} (p. 1688) ssm:resourceTag/tag-key (p. 1689)
maintenancewindow	`arn:${Partition}:ssm:${Region}:${Account}:maintenancewindow/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1688) ssm:resourceTag/tag-key (p. 1689)
managed-instance	`arn:${Partition}:ssm:${Region}:${Account}:managed-instance/${ManagedInstanceName}`	aws:ResourceTag/${TagKey} (p. 1688)

리소스 유형	ARN	조건 키
		ssm:resourceTag/tag-key (p. 1689)
managed-instance-inventory	arn:${Partition}:ssm:${Region}:${Account}:managed-instance-inventory/${InstanceId}	
opsitem	arn:${Partition}:ssm:${Region}:${Account}:opsitem/${ResourceId}	
parameter	arn:${Partition}:ssm:${Region}:${Account}:parameter/${FullyQualifiedParameterName}	aws:ResourceTag/${TagKey} (p. 1688) ssm:resourceTag/tag-key (p. 1689)
patchbaseline	arn:${Partition}:ssm:${Region}:${Account}:patchbaseline/${PatchBaselineIdResourceId}	aws:ResourceTag/${TagKey} (p. 1688) ssm:resourceTag/tag-key (p. 1689)
session	arn:${Partition}:ssm:${Region}:${Account}:session/${SessionId}	
resourcedatasync	arn:${Partition}:ssm:${Region}:${Account}:resource-data-sync/${SyncName}	
servicesetting	arn:${Partition}:ssm:${Region}:${Account}:servicesetting/${ResourceId}	
windowtarget	arn:${Partition}:ssm:${Region}:${Account}:windowtarget/${WindowTargetId}	
windowtask	arn:${Partition}:ssm:${Region}:${Account}:windowtask/${WindowTaskId}	

AWS Systems Manager에 사용되는 조건 키

AWS Systems Manager는 IAM 정책의 Condition 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	지정된 태그에 허용되는 값 세트를 기준으로 '생성' 요청을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	AWS 리소스에 할당된 태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열
aws:TagKeys	필수 태그가 요청에 포함되는지 여부를 기준으로 '생성' 요청을 필터링합니다.	문자열

조건 키	설명	유형
ssm:Overwrite	지정된 리소스의 값을 덮어쓸 수 있는지 여부를 제어하여 액세스를 필터링합니다.	문자열
ssm:Recursive	계층 구조에서 생성된 리소스에 대한 액세스를 필터링합니다.	문자열
ssm:SessionDocumentAccessCheck	사용자에게도 기본 Session Manager 구성 문서에 대한 액세스 권한이 있는지 확인하여 액세스를 필터링합니다.	부울
ssm:SyncType	사용자가 요청에 지정된 ResourceDataSync SyncType에도 액세스할 수 있는지 확인하여 액세스를 필터링합니다.	문자열
ssm:resourceTag/tag-key	Systems Manager 리소스에 할당된 태그 키-값 페어를 기준으로 액세스를 필터링합니다.	문자열

Amazon Textract에 사용되는 작업, 리소스 및 조건 키

Amazon Textract(서비스 접두사: `textract`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Textract에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AnalyzeDocument	입력으로 제공된 이미지에서 실제 문서 개체의 인스턴스를 감지합니다.	Read			s3:GetObject

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DetectDocumentText	문서 이미지에서 텍스트를 감지합니다.	Read			s3:GetObject
GetDocumentAnalysis	문서 분석 작업에 대한 정보를 반환합니다.	Read			
GetDocumentTextDetection	문서 텍스트 감지 작업에 대한 정보를 반환합니다.	Read			
StartDocumentAnalysis	입력으로 제공된 이미지 또는 PDF에서 실제 문서 개체의 인스턴스를 감지하는 비동기 작업을 시작합니다.	쓰기			s3:GetObject
StartDocumentTextDetection	문서 이미지 또는 PDF에서 텍스트를 감지하는 비동기 작업을 시작합니다.	쓰기			s3:GetObject

Amazon Textract에서 정의한 리소스 유형

Amazon Textract는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Textract에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Textract에 사용되는 조건 키

Textract에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon Transcribe에 사용되는 작업, 리소스 및 조건 키

Amazon Transcribe(서비스 접두사: `transcribe`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon Transcribe에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateVocabulary	Amazon Transcribe가 오디오 파일의 트랜스크립션을 처리하는 방식을 변경하는 데 사용할 수 있는 새 사용자 지정 어휘를 생성합니다.	쓰기			s3:GetObject
CreateVocabularyFilter	Amazon Transcribe에서 생성된 오디오 파일의 트랜스크립션에서 단어를 필터링하는 데 사용할 수 있는 새 어휘 필터를 생성합니다.	쓰기			s3:GetObject
DeleteTranscriptionJob	이전에 제출한 트랜스크립션 작업을 다른 생성된 결과(트랜스크립션, 모델 등)와 함께 삭제합니다.	쓰기			
DeleteVocabulary	Amazon Transcribe에서 어휘를 삭제합니다.	쓰기			
DeleteVocabularyFilter	Amazon Transcribe에서 어휘 필터를 삭제합니다.	쓰기			
GetTranscriptionJob	트랜스크립션 작업에 대한 정보를 반환합니다.	Read			
GetVocabulary	어휘에 대한 정보를 가져옵니다.	Read			
GetVocabularyFilter	어휘 필터에 대한 정보를 가져옵니다.	Read			
ListTranscriptionJobs	지정된 상태와 함께 트랜스크립션 작업을 나열합니다.	List			
ListVocabularies	지정된 기준과 일치하는 어휘의 목록을 반환합니다. 기준이 지정되지 않은 경우 전체 어휘 목록을 반환합니다.	List			
ListVocabularyFilters	지정된 기준과 일치하는 어휘 필터의 목록을 반환합니다. 조건을 지정하지 않으면 최대 5개의 어휘 필터를 반환합니다.	List			
StartMedicalStreamTranscription	프로토콜을 시작하여 오디오를 Transcribe Medical로 스트리밍하고 트랜스크립션 결과를 애플리케이션으로 스트리밍합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartStreamTranscription	양방향 HTTP2 스트림을 시작하여 실시간으로 음성을 텍스트로 트랜스크립션합니다.	쓰기			
StartTranscriptionJob	비동기 작업을 시작하여 음성을 텍스트로 트랜스크립션합니다.	쓰기			s3:GetObject
UpdateVocabulary	기존 어휘를 새 값으로 업데이트합니다. UpdateVocabulary 작업은 사용자가 요청에서 제공한 새 값으로 모든 기존 정보를 덮어씁니다.	쓰기			s3:GetObject
UpdateVocabularyFilter	기존 어휘 필터를 새 값으로 업데이트합니다. UpdateVocabularyFilter 작업은 사용자가 요청에서 제공한 새 값으로 모든 기존 정보를 덮어쓰기합니다.	쓰기			s3:GetObject

Amazon Transcribe에서 정의한 리소스 유형

Amazon Transcribe는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Transcribe에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Transcribe에 사용되는 조건 키

Transcribe에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Transfer for SFTP에 사용되는 작업, 리소스 및 조건 키

AWS Transfer for SFTP(서비스 접두사: `transfer`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.

주제

AWS Transfer for SFTP에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateServer	호출자가 서버를 생성할 수 있습니다.	쓰기		aws:TagKeys (p. 1695) aws:RequestTag/${TagKey} (p. 1695)	
CreateUser	호출자가 서버와 연결된 사용자를 추가할 수 있습니다.	쓰기	server* (p. 1694)		iam:PassRole
				aws:TagKeys (p. 1695) aws:RequestTag/${TagKey} (p. 1695)	
DeleteServer	호출자가 서버를 삭제할 수 있습니다.	쓰기	server* (p. 1694)		
DeleteSshPublicKey	호출자가 사용자에게서 SSH 퍼블릭 키를 삭제할 수 있습니다.	쓰기	user* (p. 1694)		
DeleteUser	호출자가 서버와 연결된 사용자를 삭제할 수 있습니다.	쓰기	user* (p. 1694)		
DescribeServer	호출자가 서버를 설명할 수 있습니다.	Read	server* (p. 1694)		
DescribeUser	호출자가 서버와 연결된 사용자를 설명할 수 있습니다.	Read	user* (p. 1694)		
ImportSshPublicKey	호출자가 사용자에게 SSH 퍼블릭 키를 추가할 수 있습니다.	쓰기	user* (p. 1694)		
ListServers	호출자가 서버를 나열할 수 있습니다.	List			
ListTagsForResource	호출자가 서버 또는 사용자에 대한 태그를 나열할 수 있습니다.	Read	server (p. 1694)		
			user (p. 1694)		
ListUsers	호출자가 서버와 연결된 사용자를 나열할 수 있습니다.	List	user* (p. 1694)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
StartServer	호출자가 서버를 시작할 수 있습니다.	쓰기	server* (p. 1694)		
StopServer	호출자가 서버를 중지할 수 있습니다.	쓰기	server* (p. 1694)		
TagResource	호출자가 서버 또는 사용자에 태그를 지정할 수 있습니다.	태그 지정	server (p. 1694)		
			user (p. 1694)		
				aws:TagKeys (p. 1695) aws:RequestTag/${TagKey} (p. 1695)	
TestIdentityProvider	호출자가 서버의 사용자 지정 자격 증명 공급자를 테스트할 수 있습니다.	Read	server* (p. 1694)		
UntagResource	호출자가 서버 또는 사용자에서 태그를 제거할 수 있습니다.	태그 지정	server (p. 1694)		
			user (p. 1694)		
				aws:TagKeys (p. 1695)	
UpdateServer	호출자가 서버의 구성을 업데이트할 수 있습니다.	쓰기	server* (p. 1694)		
UpdateUser	호출자가 사용자의 구성을 업데이트할 수 있습니다.	쓰기	server* (p. 1694)		
			user* (p. 1694)		

AWS Transfer for SFTP에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1692)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
user	`arn:${Partition}:transfer:${region}:${account}:user/${serverId}/${username}`	aws:ResourceTag/${TagKey} (p. 1695)
server	`arn:${Partition}:transfer:${region}:${account}:server/${serverId}`	aws:ResourceTag/${TagKey} (p. 1695)

AWS Transfer for SFTP에 사용되는 조건 키

AWS Transfer for SFTP는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	사용자의 요청에 있는 키입니다.	문자열
aws:ResourceTag/${TagKey}	사용자가 만드는 리소스에 있는 키입니다.	문자열
aws:TagKeys	요청의 리소스와 연결된 모든 태그 키 이름의 목록입니다.	문자열

Amazon Translate에 사용되는 작업, 리소스 및 조건 키

Amazon Translate(서비스 접두사: `translate`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon Translate에서 정의한 작업 (p. 1695)
- Amazon Translate에서 정의한 리소스 유형 (p. 1696)
- Amazon Translate에 사용되는 조건 키 (p. 1696)

Amazon Translate에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteTerminology	사용자 지정 용어를 삭제하는 동기식 작업입니다.	쓰기			
DescribeTextTranslationJob	이름, ID, 상태, 소스 언어와 대상 언어, 입력/출력 S3 버킷 등을 포함하여 비동기식 배치 번역 작업과 관련된 속성을 가져옵니다.	Read			
GetTerminology	사용자 지정 용어를 삭제합니다.	Read			
ImportTerminology	지정된 용어 이름이 이미 존재하는지 여부에 따라 사용자 지정 용어를 생성하거나 업데이트합니다.	쓰기			
ListTerminologies	계정과 연결된 사용자 지정 용어의 목록을 제공합니다.	Read			
ListTextTranslationJobs	제출한 배치 번역 작업의 목록을 가져옵니다.	Read			
StartTextTranslationJob	비동기식 배치 번역 작업을 시작합니다. 배치 번역 작업을 사용하여 여러 문서에서 대량의 텍스트를 한 번에 번역할 수 있습니다.	쓰기			
StopTextTranslationJob	진행 중인 비동기식 배치 번역 작업을 중지합니다.	쓰기			
TranslateText	소스 언어의 텍스트를 대상 언어로 번역합니다.	Read			

Amazon Translate에서 정의한 리소스 유형

Amazon Translate는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon Translate에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon Translate에 사용되는 조건 키

Translate에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS Trusted Advisor에 사용되는 작업, 리소스 및 조건 키

AWS Trusted Advisor(서비스 접두사: `trustedadvisor`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에서 사용할 수 있는 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Trusted Advisor에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeAccount	지원 플랜 및 다양한 TA 기본 설정을 봅니다.	Read			
DescribeAccountAccess	계정에서 Trusted Advisor가 비활성화되었는지 여부를 확인합니다.	Read			
DescribeCheckItems	점검 항목에 대한 세부 정보를 봅니다.	Read	checks* (p. 1698)		
DescribeCheckRefreshStatuses	점검 새로 고침 상태를 설명합니다.	Read	checks* (p. 1698)		
DescribeCheckSummaries	점검의 요약을 설명합니다.	Read	checks* (p. 1698)		
DescribeChecks	유효한 Trusted Advisor 점검 항목 및 세부 정보를 나열합니다.	Read			
DescribeNotificationPreferences	계정에 대한 알림 기본 설정을 설명합니다.	Read			
ExcludeCheckItems	지정된 고객의 점검에 대한 권장 사항을 제외합니다.	쓰기	checks* (p. 1698)		
IncludeCheckItems	지정된 고객의 점검에 대한 권장 사항을 포함합니다.	쓰기	checks* (p. 1698)		
RefreshCheck	지정된 점검을 위한 새로 고침을 대기열에 넣습니다.	쓰기	checks* (p. 1698)		
SetAccountAccess	계정에서 TrustedAdvisor 활성화/비활성화 사이를 전환합니다.	쓰기			
UpdateNotificationPreferences	알림 기본 설정을 업데이트합니다.	쓰기			

AWS Trusted Advisor에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1697)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
checks	`arn:${Partition}:trustedadvisor:${Region}:${Account}:checks/${CategoryCode}/${CheckId}`	

AWS Trusted Advisor에 사용되는 조건 키

Trusted Advisor에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS WAF에 사용되는 작업, 리소스 및 조건 키

AWS WAF(서비스 접두사: `waf`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- AWS WAF에서 정의한 작업 (p. 1698)
- AWS WAF에서 정의한 리소스 유형 (p. 1705)
- AWS WAF의 조건 키 (p. 1705)

AWS WAF에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateByteMatchSet	ByteMatchSet를 생성합니다.	쓰기	bytematchset* (p. 1705)		
CreateGeoMatchSet	요청이 시작되는 국가를 기반으로 허용하거나 차단하려는 웹 요청을 지정하는 데 사용하는 GeoMatchSet를 생성합니다.	쓰기	geomatchset* (p. 1705)		
CreateIPSet	요청이 시작되는 IP 주소를 기반으로 허용하거나 차단하려는 웹 요청을 지정하는 데 사용하는 IPSet를 생성합니다.	쓰기	ipset* (p. 1705)		
CreateRateBasedRule	AWS WAF가 지정된 IP 주소로부터 5분간 허용하는 최대 요청 수를 지정하는 RateLimit를 포함하는 RateBasedRule를 생성합니다.	쓰기	ratebasedrule* (p. 1705)		
				aws:RequestTag/${TagKey} (p. 1705) aws:TagKeys (p. 1706)	
CreateRegexMatchSet	RegexPatternSet에서 지정한 정규식 패턴을 기반으로 허용하거나 차단하려는 웹 요청을 지정하는 데 사용하는 RegexMatchSet를 생성합니다.	쓰기	regexmatchset* (p. 1705)		
CreateRegexPatternSet	AWS WAF에서 검색할 정규식(regex) 패턴을 지정하는 데 사용하는 RegexPatternSet를 생성합니다.	쓰기	regexpatternset* (p. 1705)		
CreateRule	차단하려는 요청을 식별하는 IPSet 객체, ByteMatchSet 객체 및 기타 조건자를 포함하는 규칙을 생성합니다.	쓰기	rule* (p. 1705)		
				aws:RequestTag/${TagKey} (p. 1705) aws:TagKeys (p. 1706)	
CreateRuleGroup	RuleGroup을 생성합니다. 규칙 그룹은 WebACL에 추가하는 미리 정의된 규칙의 모음입니다.	쓰기	rulegroup* (p. 1705)		
				aws:RequestTag/${TagKey} (p. 1705) aws:TagKeys (p. 1706)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateSizeConstraintSet	길이를 확인하려는 웹 요청의 부분을 식별하는 데 사용하는 SizeConstraintSet를 생성합니다.	쓰기	sizeconstraintset* (p. 1705)		
CreateSqlInjectionMatchSet	웹 요청의 특정 부분에 SQL 코드의 조각이 포함된 요청을 허용, 차단 또는 계산하는 데 사용하는 SqlInjectionMatchSet를 생성합니다.	쓰기	sqlinjectionmatchset* (p. 1705)		
CreateWebACL	허용, 차단 또는 계산하려는 CloudFront 웹 요청을 식별하는 규칙을 포함하는 WebACL을 생성합니다.	권한 관리	webacl* (p. 1705)		
				aws:RequestTag/${TagKey} (p. 1705) aws:TagKeys (p. 1706)	
CreateXssMatchSet	웹 요청의 특정 부분에 교차 사이트 스크립팅 공격이 포함된 요청을 허용, 차단 또는 계산하는 데 사용하는 XssMatchSet를 생성합니다.	쓰기	xssmatchset* (p. 1705)		
DeleteByteMatchSet	ByteMatchSet를 영구적으로 삭제합니다.	쓰기	bytematchset* (p. 1705)		
DeleteGeoMatchSet	GeoMatchSet를 영구적으로 삭제합니다.	쓰기	geomatchset* (p. 1705)		
DeleteIPSet	IPSet를 영구적으로 삭제합니다.	쓰기	ipset* (p. 1705)		
DeleteLoggingConfiguration	지정된 웹 ACL에서 LoggingConfiguration을 영구적으로 삭제합니다.	쓰기	webacl* (p. 1705)		
DeletePermissionPolicy	지정된 RuleGroup에서 IAM 정책을 영구적으로 삭제합니다.	권한 관리	rulegroup* (p. 1705)		
DeleteRateBasedRule	RateBasedRule을 영구적으로 삭제합니다.	쓰기	ratebasedrule* (p. 1705)		
DeleteRegexMatchSet	RegexMatchSet를 영구적으로 삭제합니다.	쓰기	regexmatchset* (p. 1705)		
DeleteRegexPatternSet	RegexPatternSet를 영구적으로 삭제합니다.	쓰기	regexpatternset* (p. 1705)		
DeleteRule	Rule을 영구적으로 삭제합니다.	쓰기	rule* (p. 1705)		
DeleteRuleGroup	RuleGroup을 영구적으로 삭제합니다.	쓰기	rulegroup* (p. 1705)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteSizeConstraintSet	SizeConstraintSet를 영구적으로 삭제합니다.	쓰기	sizeconstraintset* (p. 1705)		
DeleteSqlInjectionMatchSet	SqlInjectionMatchSet를 영구적으로 삭제합니다.	쓰기	sqlinjectionmatchset* (p. 1705)		
DeleteWebACL	WebACL을 영구적으로 삭제합니다.	권한 관리	webacl* (p. 1705)		
DeleteXssMatchSet	XssMatchSet를 영구적으로 삭제합니다.	쓰기	xssmatchset* (p. 1705)		
GetByteMatchSet	ByteMatchSetId로 지정된 ByteMatchSet를 반환합니다.	Read	bytematchset* (p. 1705)		
GetChangeToken	AWS WAF 객체를 생성, 업데이트 또는 삭제하려는 경우, 교환 토큰을 가져와서 생성, 업데이트 삭제 요청에 교환 토큰을 포함시킵니다.	Read			
GetChangeTokenStatus	GetChangeToken을 호출하여 가져온 ChangeToken의 상태를 반환합니다.	Read			
GetGeoMatchSet	GeoMatchSetId로 지정된 GeoMatchSet를 반환합니다.	Read	geomatchset* (p. 1705)		
GetIPSet	IPSetId로 지정된 IPSet를 반환합니다.	Read	ipset* (p. 1705)		
GetLoggingConfiguration	지정된 웹 ACL에 대한 LoggingConfiguration을 반환합니다.	Read	webacl* (p. 1705)		
GetPermissionPolicy	RuleGroup에 연결된 IAM 정책을 반환합니다.	Read	rulegroup* (p. 1705)		
GetRateBasedRule	GetRateBasedRule 요청에 포함한 RuleId로 지정된 RateBasedRule을 반환합니다.	Read	ratebasedrule* (p. 1705)		
GetRateBasedRuleManagedKeys	RuleId로 지정된 RateBasedRule에 의해 현재 차단된 IP 주소의 배열을 반환합니다.	Read	ratebasedrule* (p. 1705)		
GetRegexMatchSet	RegexMatchSetId로 지정된 RegexMatchSet를 반환합니다.	Read	regexmatchset* (p. 1705)		
GetRegexPatternSet	RegexPatternSetId로 지정된 RegexPatternSet를 반환합니다.	Read	regexpatternset* (p. 1705)		
GetRule	GetRule 요청에 포함한 RuleId로 지정된 Rule을 반환합니다.	Read	rule* (p. 1705)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetRuleGroup	GetRuleGroup 요청에 포함한 RuleGroupId로 지정된 RuleGroup을 반환합니다.	Read	rulegroup* (p. 1705)		
GetSampledRequests	AWS 리소스가 선택된 일정 시간 동안에 받은 처음 5,000개의 요청 중에서 AWS WAF가 임의로 선택하는 지정된 요청 수(샘플)에 대한 세부 정보를 가져옵니다.	Read	rule (p. 1705)		
			webacl (p. 1705)		
GetSizeConstraintSet	SizeConstraintSetId로 지정된 SizeConstraintSet를 반환합니다.	Read	sizeconstraintset* (p. 1705)		
GetSqlInjectionMatchSet	SqlInjectionMatchSetId로 지정된 SqlInjectionMatchSet를 반환합니다.	Read	sqlinjectionmatchset* (p. 1705)		
GetWebACL	WebACLId로 지정된 WebACL을 반환합니다.	Read	webacl* (p. 1705)		
GetXssMatchSet	XssMatchSetId로 지정된 XssMatchSet를 반환합니다.	Read	xssmatchset* (p. 1705)		
ListActivatedRulesInRuleGroup	ActivatedRule 객체의 배열을 반환합니다.	List			
ListByteMatchSets	ByteMatchSetSummary 객체의 배열을 반환합니다.	List			
ListGeoMatchSets	GeoMatchSetSummary 객체의 배열을 반환합니다.	List			
ListIPSets	응답에서 IPSetSummary 객체의 배열을 반환합니다.	List			
ListLoggingConfigurations	LoggingConfiguration 객체의 배열을 반환합니다.	List			
ListRateBasedRules	RuleSummary 객체의 배열을 반환합니다.	List			
ListRegexMatchSets	RegexMatchSetSummary 객체의 배열을 반환합니다.	List			
ListRegexPatternSets	RegexPatternSetSummary 객체의 배열을 반환합니다.	List			
ListRuleGroups	RuleGroup 객체의 배열을 반환합니다.	List			
ListRules	RuleSummary 객체의 배열을 반환합니다.	List			
ListSizeConstraintSets	SizeConstraintSetSummary 객체의 배열을 반환합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListSqlInjectionMatchSets	SqlInjectionMatchSet 객체의 배열을 반환합니다.	List			
ListSubscribedRuleGroups	구독하는 RuleGroup 객체의 배열을 반환합니다.	List			
ListTagsForResource	지정된 리소스에 대한 태그를 나열합니다.	Read	ratebasedrule (p. 1705)		
			rule (p. 1705)		
			rulegroup (p. 1705)		
			webacl (p. 1705)		
ListWebACLs	응답에서 WebACLSummary 객체의 배열을 반환합니다.	List			
ListXssMatchSets	XssMatchSet 객체의 배열을 반환합니다.	List			
PutLoggingConfiguration	LoggingConfiguration을 지정된 웹 ACL과 연결합니다.	쓰기	webacl* (p. 1705)		iam:CreateServiceLinkedI
PutPermissionPolicy	IAM 정책을 지정된 리소스에 연결합니다. 이 작업은 계정 간에 RuleGroup을 공유하는 경우에만 지원됩니다.	권한 관리	rulegroup* (p. 1705)		
TagResource	지정된 리소스에 태그를 추가합니다.	태그 지정	ratebasedrule (p. 1705)		
			rule (p. 1705)		
			rulegroup (p. 1705)		
			webacl (p. 1705)		
				aws:RequestTag/${TagKey} (p. 1705) aws:TagKeys (p. 1706)	
UntagResource	지정된 리소스에서 태그를 제거합니다.	태그 지정	ratebasedrule (p. 1705)		
			rule (p. 1705)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			rulegroup (p. 1705)		
			webacl (p. 1705)		
				aws:TagKeys (p. 1706)	
UpdateByteMatchSet	ByteMatchSet에서 ByteMatchTuple 객체(필터)를 삽입 또는 삭제합니다.	쓰기	bytematchset* (p. 1705)		
UpdateGeoMatchSet	GeoMatchSet에서 GeoMatchConstraint 객체를 삽입 또는 삭제합니다.	쓰기	geomatchset* (p. 1705)		
UpdateIPSet	IPSet에서 IPSetDescriptor 객체를 삽입 또는 삭제합니다.	쓰기	ipset* (p. 1705)		
UpdateRateBasedRule	Rule에서 Predicate 객체를 삽입 또는 삭제하고 Rule에서 RateLimit를 업데이트합니다.	쓰기	ratebasedrule* (p. 1705)		
UpdateRegexMatchSet	RegexMatchSet에서 RegexMatchTuple 객체(필터)를 삽입 또는 삭제합니다.	쓰기	regexmatchset* (p. 1705)		
UpdateRegexPatternSet	RegexPatternSet에서 RegexPatternStrings를 삽입 또는 삭제합니다.	쓰기	regexpatternset* (p. 1705)		
UpdateRule	Rule에서 Predicate 객체를 삽입 또는 삭제합니다.	쓰기	rule* (p. 1705)		
UpdateRuleGroup	RuleGroup에서 ActivatedRule 객체를 삽입 또는 삭제합니다.	쓰기	rulegroup* (p. 1705)		
UpdateSizeConstraintSet	SizeConstraintSet에서 SizeConstraint 객체(필터)를 삽입 또는 삭제합니다.	쓰기	sizeconstraintset* (p. 1705)		
UpdateSqlInjectionMatchSet	SqlInjectionMatchSet에서 SqlInjectionMatchTuple 객체(필터)를 삽입 또는 삭제합니다.	쓰기	sqlinjectionmatchset* (p. 1705)		
UpdateWebACL	WebACL에서 ActivatedRule 객체를 삽입 또는 삭제합니다.	권한 관리	webacl* (p. 1705)		
UpdateXssMatchSet	XssMatchSet에서 XssMatchTuple 객체(필터)를 삽입 또는 삭제합니다.	쓰기	xssmatchset* (p. 1705)		

AWS WAF에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1698)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
bytematchset	`arn:${Partition}:waf::${Account}:bytematchset/${Id}`	
ipset	`arn:${Partition}:waf::${Account}:ipset/${Id}`	
ratebasedrule	`arn:${Partition}:waf::${Account}:ratebasedrule/${Id}`	aws:ResourceTag/${TagKey} (p. 1706)
rule	`arn:${Partition}:waf::${Account}:rule/${Id}`	aws:ResourceTag/${TagKey} (p. 1706)
sizeconstraintset	`arn:${Partition}:waf::${Account}:sizeconstraintset/${Id}`	
sqlinjectionmatchset	`arn:${Partition}:waf::${Account}:sqlinjectionmatchset/${Id}`	
webacl	`arn:${Partition}:waf::${Account}:webacl/${Id}`	aws:ResourceTag/${TagKey} (p. 1706)
xssmatchset	`arn:${Partition}:waf::${Account}:xssmatchset/${Id}`	
regexmatchset	`arn:${Partition}:waf::${Account}:regexmatch/${Id}`	
regexpatternset	`arn:${Partition}:waf::${Account}:regexpatternset/${Id}`	
geomatchset	`arn:${Partition}:waf::${Account}:geomatchset/${Id}`	
rulegroup	`arn:${Partition}:waf::${Account}:rulegroup/${Id}`	aws:ResourceTag/${TagKey} (p. 1706)

AWS WAF의 조건 키

AWS WAF는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열

조건 키	설명	유형
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS WAF Regional에 사용되는 작업, 리소스 및 조건 키

AWS WAF Regional(서비스 접두사: `waf-regional`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS WAF Regional에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateWebACL	WebACL을 리소스와 연결합니다.	쓰기	loadbalancer/app/* (p. 1713)		
			webacl* (p. 1713)		
CreateByteMatchSet	ByteMatchSet를 생성합니다.	쓰기	bytematchset* (p. 1713)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateGeoMatchSet	요청이 시작되는 국가를 기반으로 허용하거나 차단하려는 웹 요청을 지정하는 데 사용하는 GeoMatchSet를 생성합니다.	쓰기	geomatchset* (p. 1713)		
CreateIPSet	요청이 시작되는 IP 주소를 기반으로 허용하거나 차단하려는 웹 요청을 지정하는 데 사용하는 IPSet를 생성합니다.	쓰기	ipset* (p. 1713)		
CreateRateBasedRule	AWS WAF가 지정된 IP 주소로부터 5분간 허용하는 최대 요청 수를 지정하는 RateLimit를 포함하는 RateBasedRule을 생성합니다.	쓰기	ratebasedrule* (p. 1713)		
				aws:RequestTag/${TagKey} (p. 1714) aws:TagKeys (p. 1714)	
CreateRegexMatchSet	egexPatternSet에서 지정한 정규 표현식 패턴을 기반으로 허용하거나 차단하려는 웹 요청을 지정하는 데 사용하는 RegexMatchSet를 생성합니다.	쓰기	regexmatchset* (p. 1713)		
CreateRegexPatternSet	AWS WAF에서 검색할 정규식(regex) 패턴을 지정하는 데 사용하는 RegexPatternSet를 생성합니다.	쓰기	regexpatternset* (p. 1713)		
CreateRule	차단하려는 요청을 식별하는 IPSet 객체, ByteMatchSet 객체 및 기타 조건자를 포함하는 Rule을 생성합니다.	쓰기	rule* (p. 1713)		
				aws:RequestTag/${TagKey} (p. 1714) aws:TagKeys (p. 1714)	
CreateRuleGroup	RuleGroup을 생성합니다. 규칙 그룹은 WebACL에 추가하는 미리 정의된 규칙의 모음입니다.	쓰기	rulegroup* (p. 1713)		
				aws:RequestTag/${TagKey} (p. 1714) aws:TagKeys (p. 1714)	
CreateSizeConstraintSet	길이를 확인하려는 웹 요청의 부분을 식별하는 데 사용하는 SizeConstraintSet를 생성합니다.	쓰기	sizeconstraintset* (p. 1713)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateSqlInjectionMatchSet	웹 요청의 지정된 부분에 SQL 코드 삽입 조건을 포함하는 요청을 허용, 차단 또는 계산하는 데 사용하는 SqlInjectionMatchSet를 생성합니다.	쓰기	sqlinjectionmatchset* (p. 1713)		
CreateWebACL	허용, 차단 또는 계산하려는 CloudFront 웹 요청을 식별하는 규칙을 포함하는 WebACL을 생성합니다.	권한 관리	webacl* (p. 1713)		
				aws:RequestTag/${TagKey} (p. 1714) aws:TagKeys (p. 1714)	
CreateXssMatchSet	웹 요청의 지정된 부분에 교차 사이트 스크립팅 공격을 포함하는 요청을 허용, 차단 또는 계산하는 데 사용하는 XssMatchSet를 생성합니다.	쓰기	xssmatchset* (p. 1713)		
DeleteByteMatchSet	ByteMatchSet를 영구적으로 삭제합니다.	쓰기	bytematchset* (p. 1713)		
DeleteGeoMatchSet	GeoMatchSet를 영구적으로 삭제합니다.	쓰기	geomatchset* (p. 1713)		
DeleteIPSet	IPSet를 영구적으로 삭제합니다.	쓰기	ipset* (p. 1713)		
DeleteLoggingConfiguration	지정된 웹 ACL에서 LoggingConfiguration을 영구적으로 삭제합니다.	쓰기	webacl* (p. 1713)		
DeletePermissionPolicy	지정된 RuleGroup에서 IAM 정책을 영구적으로 삭제합니다.	권한 관리	rulegroup* (p. 1713)		
DeleteRateBasedRule	RateBasedRule을 영구적으로 삭제합니다.	쓰기	ratebasedrule* (p. 1713)		
DeleteRegexMatchSet	RegexMatchSet를 영구적으로 삭제합니다.	쓰기	regexmatchset* (p. 1713)		
DeleteRegexPatternSet	RegexPatternSet를 영구적으로 삭제합니다.	쓰기	regexpatternset* (p. 1713)		
DeleteRule	Rule을 영구적으로 삭제합니다.	쓰기	rule* (p. 1713)		
DeleteRuleGroup	RuleGroup을 영구적으로 삭제합니다.	쓰기	rulegroup* (p. 1713)		
DeleteSizeConstraintSet	SizeConstraintSet를 영구적으로 삭제합니다.	쓰기	sizeconstraintset* (p. 1713)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteSqlInjectionMatchSet	SqlInjectionMatchSet를 영구적으로 삭제합니다.	쓰기	sqlinjectionmatchset* (p. 1713)		
DeleteWebACL	WebACL을 영구적으로 삭제합니다.	권한 관리	webacl* (p. 1713)		
DeleteXssMatchSet	XssMatchSet를 영구적으로 삭제합니다.	쓰기	xssmatchset* (p. 1713)		
DisassociateWebACL	지정된 리소스에서 WebACL을 제거합니다.	쓰기	loadbalancer/app/* (p. 1713)		
GetByteMatchSet	ByteMatchSetId로 지정된 ByteMatchSet를 반환합니다.	Read	bytematchset* (p. 1713)		
GetChangeToken	AWS WAF 객체를 생성, 업데이트 또는 삭제하려는 경우 교환 토큰을 가져와서 생성, 업데이트 또는 삭제 요청에 교환 토큰을 포함시킵니다.	Read			
GetChangeTokenStatus	GetChangeToken을 호출하여 가져온 ChangeToken의 상태를 반환합니다.	Read			
GetGeoMatchSet	GeoMatchSetId로 지정된 GeoMatchSet를 반환합니다.	Read	geomatchset* (p. 1713)		
GetIPSet	IPSetId로 지정된 IPSet를 반환합니다.	Read	ipset* (p. 1713)		
GetLoggingConfiguration	지정된 웹 ACL에 대한 LoggingConfiguration을 반환합니다.	Read	webacl* (p. 1713)		
GetPermissionPolicy	RuleGroup에 연결된 IAM 정책을 반환합니다.	Read	rulegroup* (p. 1713)		
GetRateBasedRule	GetRateBasedRule 요청에 포함한 RuleId로 지정된 RateBasedRule을 반환합니다.	Read	ratebasedrule* (p. 1713)		
GetRateBasedRuleManagedKeys	RuleId로 지정된 RateBasedRule에 의해 현재 차단된 IP 주소의 배열을 반환합니다.	Read	ratebasedrule* (p. 1713)		
GetRegexMatchSet	RegexMatchSetId로 지정된 RegexMatchSet를 반환합니다.	Read	regexmatchset* (p. 1713)		
GetRegexPatternSet	RegexPatternSetId로 지정된 RegexPatternSet를 반환합니다.	Read	regexpatternset* (p. 1713)		
GetRule	GetRule 요청에 포함한 RuleId로 지정된 Rule을 반환합니다.	Read	rule* (p. 1713)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetRuleGroup	GetRuleGroup 요청에 포함한 RuleGroupId로 지정된 RuleGroup을 반환합니다.	Read	rulegroup* (p. 1713)		
GetSampledRequests	AWS 리소스가 선택한 시간 범위 중에 받은 처음 5,000개의 요청 중에서 AWS WAF가 임의로 선택하는 지정된 요청 수(샘플)에 대한 세부 정보를 가져옵니다.	Read	rule (p. 1713)		
			webacl (p. 1713)		
GetSizeConstraintSet	SizeConstraintSetId로 지정된 SizeConstraintSet를 반환합니다.	Read	sizeconstraintset* (p. 1713)		
GetSqlInjectionMatchSet	SqlInjectionMatchSetId로 지정된 SqlInjectionMatchSet를 반환합니다.	Read	sqlinjectionmatchset* (p. 1713)		
GetWebACL	WebACLId로 지정된 WebACL을 반환합니다.	Read	webacl* (p. 1713)		
GetWebACLForResource	지정된 리소스에 대한 WebACL을 반환합니다.	Read	loadbalancer/app/* (p. 1713)		
GetXssMatchSet	XssMatchSetId로 지정된 XssMatchSet를 반환합니다.	Read	xssmatchset* (p. 1713)		
ListActivatedRulesInRuleGroup	ActivatedRule 객체의 배열을 반환합니다.	List			
ListByteMatchSets	ByteMatchSetSummary 객체의 배열을 반환합니다.	List			
ListGeoMatchSets	GeoMatchSetSummary 객체의 배열을 반환합니다.	List			
ListIPSets	응답에서 IPSetSummary 객체의 배열을 반환합니다.	List			
ListLoggingConfigurations	LoggingConfiguration 객체의 배열을 반환합니다.	List			
ListRateBasedRules	RuleSummary 객체의 배열을 반환합니다.	List			
ListRegexMatchSets	RegexMatchSetSummary 객체의 배열을 반환합니다.	List			
ListRegexPatternSets	RegexPatternSetSummary 객체의 배열을 반환합니다.	List			
ListResourcesForWebACL	지정된 WebACL과 연결된 리소스의 배열을 반환합니다.	List	webacl* (p. 1713)		
ListRuleGroups	RuleGroup 객체의 배열을 반환합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListRules	RuleSummary 객체의 배열을 반환합니다.	List			
ListSizeConstraintSets	SizeConstraintSetSummary 객체의 배열을 반환합니다.	List			
ListSqlInjectionMatchSets	SqlInjectionMatchSet 객체의 배열을 반환합니다.	List			
ListSubscribedRuleGroups	구독하는 RuleGroup 객체의 배열을 반환합니다.	List			
ListTagsForResource	지정된 리소스에 대한 태그를 나열합니다.	Read	ratebasedrule (p. 1713)		
			rule (p. 1713)		
			rulegroup (p. 1713)		
			webacl (p. 1713)		
ListWebACLs	응답에서 WebACLSummary 객체의 배열을 반환합니다.	List			
ListXssMatchSets	XssMatchSet 객체의 배열을 반환합니다.	List			
PutLoggingConfiguration	LoggingConfiguration을 지정된 웹 ACL과 연결합니다.	쓰기	webacl* (p. 1713)		iam:CreateServiceLinkedI
PutPermissionPolicy	IAM 정책을 지정된 리소스에 연결합니다. 이 작업은 계정 간에 RuleGroup을 공유하는 경우에만 지원됩니다.	권한 관리	rulegroup* (p. 1713)		
TagResource	지정된 리소스에 태그를 추가합니다.	태그 지정	ratebasedrule (p. 1713)		
			rule (p. 1713)		
			rulegroup (p. 1713)		
			webacl (p. 1713)		
				aws:RequestTag/${TagKey} (p. 1714) aws:TagKeys (p. 1714)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UntagResource	지정된 리소스에서 태그를 제거합니다.	태그 지정	ratebasedrule (p. 1713)		
			rule (p. 1713)		
			rulegroup (p. 1713)		
			webacl (p. 1713)		
				aws:TagKeys (p. 1714)	
UpdateByteMatchSet	ByteMatchSet에서 ByteMatchTuple 객체(필터)를 삽입 또는 삭제합니다.	쓰기	bytematchset* (p. 1713)		
UpdateGeoMatchSet	GeoMatchSet에서 GeoMatchConstraint 객체를 삽입 또는 삭제합니다.	쓰기	geomatchset* (p. 1713)		
UpdateIPSet	IPSet에서 IPSetDescriptor 객체를 삽입 또는 삭제합니다.	쓰기	ipset* (p. 1713)		
UpdateRateBasedRule	Rule에서 Predicate 객체를 삽입 또는 삭제하고 Rule에서 RateLimit를 업데이트합니다.	쓰기	ratebasedrule* (p. 1713)		
UpdateRegexMatchSet	RegexMatchSet에서 RegexMatchTuple 객체(필터)를 삽입 또는 삭제합니다.	쓰기	regexmatchset* (p. 1713)		
UpdateRegexPatternSet	RegexPatternSet에서 RegexPatternStrings를 삽입 또는 삭제합니다.	쓰기	regexpatternset* (p. 1713)		
UpdateRule	Rule에서 Predicate 객체를 삽입 또는 삭제합니다.	쓰기	rule* (p. 1713)		
UpdateRuleGroup	RuleGroup에서 ActivatedRule 객체를 삽입 또는 삭제합니다.	쓰기	rulegroup* (p. 1713)		
UpdateSizeConstraintSet	SizeConstraintSet에서 SizeConstraint 객체(필터)를 삽입 또는 삭제합니다.	쓰기	sizeconstraintset* (p. 1713)		
UpdateSqlInjectionMatchSet	SqlInjectionMatchSet에서 SqlInjectionMatchTuple 객체(필터)를 삽입 또는 삭제합니다.	쓰기	sqlinjectionmatchset* (p. 1713)		
UpdateWebACL	WebACL에서 ActivatedRule 객체를 삽입 또는 삭제합니다.	권한 관리	webacl* (p. 1713)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
UpdateXssMatchSet	XssMatchSet에서 XssMatchTuple 객체(필터)를 삽입 또는 삭제합니다.	쓰기	xssmatchset* (p. 1713)		

AWS WAF Regional에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1706)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
bytematchset	`arn:${Partition}:waf-regional:${Region}:${Account}:bytematchset/${Id}`	
ipset	`arn:${Partition}:waf-regional:${Region}:${Account}:ipset/${Id}`	
loadbalancer/app/	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}`	
ratebasedrule	`arn:${Partition}:waf-regional:${Region}:${Account}:ratebasedrule/${Id}`	aws:ResourceTag/${TagKey} (p. 1714)
rule	`arn:${Partition}:waf-regional:${Region}:${Account}:rule/${Id}`	aws:ResourceTag/${TagKey} (p. 1714)
sizeconstraintset	`arn:${Partition}:waf-regional:${Region}:${Account}:sizeconstraintset/${Id}`	
sqlinjectionmatchset	`arn:${Partition}:waf-regional:${Region}:${Account}:sqlinjectionmatchset/${Id}`	
webacl	`arn:${Partition}:waf-regional:${Region}:${Account}:webacl/${Id}`	aws:ResourceTag/${TagKey} (p. 1714)
xssmatchset	`arn:${Partition}:waf-regional:${Region}:${Account}:xssmatchset/${Id}`	
regexmatchset	`arn:${Partition}:waf-regional:${Region}:${Account}:regexmatch/${Id}`	
regexpatternset	`arn:${Partition}:waf-regional:${Region}:${Account}:regexpatternset/${Id}`	
geomatchset	`arn:${Partition}:waf-regional:${Region}:${Account}:geomatchset/${Id}`	
rulegroup	`arn:${Partition}:waf-regional:${Region}:${Account}:rulegroup/${Id}`	aws:ResourceTag/${TagKey} (p. 1714)

AWS WAF Regional의 조건 키

AWS WAF Regional은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS WAF V2F에 사용되는 작업, 리소스 및 조건 키

AWS WAF V2(서비스 접두사: `wafv2`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS WAF V2에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateWebACL	WebACL을 리소스와 연결할 수 있는 권한을 부여합니다.	쓰기	webacl* (p. 1719)		
			apigateway (p. 1720)		
			loadbalancer/app/ (p. 1719)		
CheckCapacity	지정된 범위와 규칙 집합에 대한 웹 ACL 용량 단위(WCU) 요구 사항을 계산할 수 있는 권한을 부여합니다.	Read			
CreateIPSet	IPSet를 생성할 수 있는 권한을 부여합니다.	쓰기	ipset* (p. 1719)		
				aws:RequestTag/${TagKey} (p. 1720) aws:TagKeys (p. 1720)	
CreateRegexPatternSet	RegexPatternSet를 생성할 수 있는 권한을 부여합니다.	쓰기	regexpatternset* (p. 1719)		
				aws:RequestTag/${TagKey} (p. 1720) aws:TagKeys (p. 1720)	
CreateRuleGroup	RuleGroup을 생성할 수 있는 권한을 부여합니다.	쓰기	rulegroup* (p. 1719)		
				aws:RequestTag/${TagKey} (p. 1720) aws:TagKeys (p. 1720)	
CreateWebACL	WebACL을 생성할 수 있는 권한을 부여합니다.	권한 관리	webacl* (p. 1719)		
				aws:RequestTag/${TagKey} (p. 1720) aws:TagKeys (p. 1720)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteIPSet	지정된 IPSet를 삭제할 수 있는 권한을 부여합니다.	쓰기	ipset* (p. 1719)		
DeleteLoggingConfiguration	지정된 WebACL에서 LoggingConfiguration을 삭제할 수 있는 권한을 부여합니다.	쓰기	webacl* (p. 1719)		
DeleteRegexPatternSet	지정된 RegexPatternSet를 삭제할 수있는 권한을 부여합니다.	쓰기	regexpatternset* (p. 1719)		
DeleteRuleGroup	지정된 RuleGroup을 삭제할 수 있는 권한을 부여합니다.	쓰기	rulegroup* (p. 1719)		
DeleteWebACL	지정된 WebACL을 삭제할 수 있는 권한을 부여합니다.	권한 관리	webacl* (p. 1719)		
DescribeManagedRuleGroup	관리형 규칙 그룹에 대한 상위 수준 정보를 볼 수 있는 권한을 부여합니다.	List			
DisassociateWebACL	애플리케이션 리소스에서 WebACL의 연결을 해제할 수 있는 권한을 부여합니다.	쓰기	apigateway (p. 1720)		
			loadbalancer/app/ (p. 1719)		
GetIPSet	지정된 IPSet에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	ipset* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	
GetLoggingConfiguration	지정된 WebACL에 대한 LoggingConfiguration을 볼 수 있는 권한을 부여합니다.	Read	webacl* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	
GetRateBasedStatementManagedKeys	비율 기반 규칙에 의해 현재 차단된 키를 볼 수 있는 권한을 부여합니다.	Read	webacl* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	
GetRegexPatternSet	지정된 RegexPatternSet에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	regexpatternset* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetRuleGroup	지정된 RuleGroup에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	rulegroup* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	
GetSampledRequests	선택한 일정 시간 동안 AWS 리소스가 수신한 처음 5,000개의 요청 중에서 AWS WAF가 임의로 선택하는 지정된 요청 수(샘플)에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	webacl* (p. 1719)		
GetWebACL	지정된 GetWebACL에 대한 세부 정보를 볼 수 있는 권한을 부여합니다.	Read	webacl* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	
GetWebACLForResource	지정된 리소스에 대한 WebACL을 볼 수 있는 권한을 부여합니다.	Read	apigateway (p. 1720)		
			loadbalancer/app/ (p. 1719)		
ListAvailableManagedRuleGroups	사용할 수 있는 관리형 규칙 그룹의 배열을 볼 수 있는 권한을 부여합니다.	List			
ListIPSets	관리하는 IP 집합에 대한 IPSetSummary 객체 배열을 볼 수 있는 권한을 부여합니다.	List			
ListLoggingConfigurations	LoggingConfiguration 객체의 배열을 볼 수 있는 권한을 부여합니다.	List			
ListRegexPatternSets	관리하는 정규식 패턴 집합에 대한 RegexPatternSetSummary 객체의 배열을 볼 수 있는 권한을 부여합니다.	List			
ListResourcesForWebACL	지정된 웹 ACL과 연결된 리소스에 대한 Amazon 리소스 이름(ARN) 배열을 볼 수 있는 권한을 부여합니다.	List	webacl* (p. 1719)		
ListRuleGroups	관리하는 규칙 그룹에 대한 RuleGroupSummary 객체 배열을 볼 수 있는 권한을 부여합니다.	List			
ListTagsForResource	지정된 리소스에 대한 태그를 나열할 수 있는 권한을 부여합니다.	Read	ipset (p. 1719)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
			regexpatternset (p. 1719)		
			rulegroup (p. 1719)		
			webacl (p. 1719)		
				aws:ResourceTag/ ${TagKey} (p. 1720)	
ListWebACLs	관리하는 웹 ACL에 대한 WebACLSummary 객체 배열을 볼 수 있는 권한을 부여합니다.	List			
PutLoggingConfiguration	지정된 LoggingConfiguration을 활성화하고 웹 ACL에서 로깅을 시작할 수 있는 권한을 부여합니다.	쓰기	webacl* (p. 1719)		iam:CreateServiceLinkedI
TagResource	태그를 지정된 AWS 리소스와 연결할 수 있는 권한을 부여합니다.	태그 지정	ipset (p. 1719)		
			regexpatternset (p. 1719)		
			rulegroup (p. 1719)		
			webacl (p. 1719)		
				aws:TagKeys (p. 1720) aws:RequestTag/ ${TagKey} (p. 1720) aws:ResourceTag/ ${TagKey} (p. 1720)	
UntagResource	AWS 리소스에서 태그의 연결을 해제할 수 있는 권한을 부여합니다.	태그 지정	ipset (p. 1719)		
			regexpatternset (p. 1719)		
			rulegroup (p. 1719)		
			webacl (p. 1719)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
				aws:TagKeys (p. 1720)	
UpdateIPSet	지정된 IPSet를 업데이트할 수 있는 권한을 부여합니다.	쓰기	ipset* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	
UpdateRegexPatternSet	지정된 RegexPatternSet를 업데이트할 수 있는 권한을 부여합니다.	쓰기	regexpatternset* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	
UpdateRuleGroup	지정된 RuleGroup을 업데이트할 수 있는 권한을 부여합니다.	쓰기	rulegroup* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	
UpdateWebACL	지정된 WebACL을 업데이트할 수 있는 권한을 부여합니다.	권한 관리	webacl* (p. 1719)		
				aws:ResourceTag/${TagKey} (p. 1720)	

AWS WAF V2에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. Actions table(작업 테이블) (p. 1714)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	aws:ResourceTag/${TagKey} (p. 1720)
ipset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/ipset/${Name}/${Id}`	aws:ResourceTag/${TagKey} (p. 1720)
rulegroup	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/rulegroup/${Name}/${Id}`	aws:ResourceTag/${TagKey} (p. 1720)
regexpatternset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/regexpatternset/${Name}/${Id}`	aws:ResourceTag/${TagKey} (p. 1720)
loadbalancer/app/	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}`	

리소스 유형	ARN	조건 키
apigateway	`arn:${Partition}:apigateway:${Region}::/restapis/${ApiId}/stages/prod`	

AWS WAF V2의 조건 키

AWS WAF V2는 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	각 태그에 허용되는 값 집합을 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스와 연결된 태그-값을 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 필수 태그가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

AWS Well-Architected Tool에 사용되는 작업, 리소스 및 조건 키

AWS Well-Architected Tool(서비스 접두사: `wellarchitected`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS Well-Architected Tool에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업

은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateWorkload	새로운 워크로드를 생성합니다.	쓰기			
CreateWorkloadShare	워크로드를 다른 계정과 공유합니다.	쓰기	workload* (p. 1721)		
DeleteWorkload	기존 워크로드를 삭제합니다.	쓰기	workload* (p. 1721)		
GetWorkload	지정된 워크로드를 검색합니다.	Read	workload* (p. 1721)		
ListWorkloads	이 계정의 워크로드를 나열합니다.	List			

AWS Well-Architected Tool에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1720)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
workload	`arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}`	

AWS Well-Architected Tool에 사용되는 조건 키

Well-Architected Tool에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon WorkDocs에 사용되는 작업, 리소스 및 조건 키

Amazon WorkDocs(서비스 접두사: `workdocs`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon WorkDocs에서 정의한 작업 (p. 1722)

Amazon WorkDocs에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AbortDocumentVersionUpload	InitiateDocumentVersionUpload에 의해 이전에 시작된 지정된 문서 버전의 업로드를 중단할 수 있는 권한을 부여합니다.	쓰기			
ActivateUser	지정된 사용자를 활성화할 수 있는 권한을 부여합니다. 활성 사용자만 Amazon WorkDocs에 액세스할 수 있습니다.	쓰기			
AddResourcePermissions	지정된 폴더 또는 문서에 대한 권한 세트를 생성할 수 있는 권한을 부여합니다.	쓰기			
AddUserToGroup [권한만 해당]	그룹에 사용자를 추가할 수 있는 권한을 부여합니다.	쓰기			
CheckAlias [권한만 해당]	별칭을 확인할 수 있는 권한을 부여합니다.	Read			
CreateComment	지정된 문서 버전에 새 의견을 추가할 수 있는 권한을 부여합니다.	쓰기			
CreateCustomMetadata	지정된 리소스에 하나 이상의 사용자 지정 속성을 추가할 수 있는 권한을 부여합니다.	쓰기			
CreateFolder	지정된 이름 및 상위 폴더로 폴더를 생성할 수 있는 권한을 부여합니다.	쓰기			
CreateInstance [권한만 해당]	인스턴스를 생성할 수 있는 권한을 부여합니다.	쓰기			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateLabels	지정된 리소스에 레이블을 추가할 수 있는 권한을 부여합니다.	쓰기			
CreateNotificationSubscription	Amazon SNS 알림을 사용하기 위해 WorkDocs를 구성할 수 있는 권한을 부여합니다.	쓰기			
CreateUser	Simple AD 또는 Microsoft AD 디렉터리에서 사용자를 생성할 수 있는 권한을 부여합니다.	쓰기			
DeactivateUser	지정된 사용자를 비활성화하여 Amazon WorkDocs에 대한 사용자의 액세스 권한을 취소할 수 있는 권한을 부여합니다.	쓰기			
DeleteComment	문서 버전에서 지정된 의견을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteCustomMetadata	지정된 리소스에서 사용자 지정 메타데이터를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteDocument	지정된 문서 및 연결된 메타데이터를 영구적으로 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteFolder	지정된 폴더 및 그 내용을 영구적으로 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteFolderContents	지정된 폴더의 내용을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteInstance [권한만 해당]	인스턴스를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteLabels	리소스에서 하나 이상의 레이블을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteNotificationSubscription	지정된 조직에서 지정된 구독을 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeleteUser	Simple AD 또는 Microsoft AD 디렉터리에서 지정된 사용자를 삭제할 수 있는 권한을 부여합니다.	쓰기			
DeregisterDirectory [권한만 해당]	디렉터리를 등록 취소할 수 있는 권한을 부여합니다.	쓰기			
DescribeActivities	지정된 기간의 사용자 활동을 가져올 수 있는 권한을 부여합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeAvailableDirectories [권한만 해당]	사용 가능한 디렉터리를 설명할 수 있는 권한을 부여합니다.	List			
DescribeComments	지정된 문서 버전에 대한 모든 의견을 나열할 수 있는 권한을 부여합니다.	List			
DescribeDocumentVersions	지정된 문서의 문서 버전을 검색할 수 있는 권한을 부여합니다.	List			
DescribeFolderContents	문서 및 하위 폴더를 포함한 지정된 폴더의 내용을 설명할 수 있는 권한을 부여합니다.	List			
DescribeGroups	사용자 그룹을 설명할 수 있는 권한을 부여합니다.	List			
DescribeInstances [권한만 해당]	인스턴스를 설명할 수 있는 권한을 부여합니다.	List			
DescribeNotificationSubscriptions	지정된 알림 구독을 나열할 수 있는 권한을 부여합니다.	List			
DescribeResourcePermissions	지정된 리소스의 권한에 대한 설명을 볼 수 있는 권한을 부여합니다.	List			
DescribeRootFolders	루트 폴더를 설명할 수 있는 권한을 부여합니다.	List			
DescribeUsers	지정된 사용자에 대한 설명을 볼 수 있는 권한을 부여합니다. 모든 사용자를 설명하거나 결과를 필터링할 수 있습니다(예: 상태별 또는 조직별 필터링).	List			
DownloadDocumentVersion [권한만 해당]	지정된 문서 버전을 다운로드할 수 있는 권한을 부여합니다.	Read			
GetCurrentUser	현재 사용자의 세부 정보를 검색할 수 있는 권한을 부여합니다.	Read			
GetDocument	지정된 문서 객체를 검색할 수 있는 권한을 부여합니다.	Read			
GetDocumentPath	요청된 문서에 대한 경로 정보(루트 폴더의 계층 구조)를 검색할 수 있는 권한을 부여합니다.	Read			
GetDocumentVersion	지정된 문서의 버전 메타데이터를 검색할 수 있는 권한을 부여합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetFolder	지정된 폴더의 메타데이터를 검색할 수 있는 권한을 부여합니다.	Read			
GetFolderPath	지정된 문서에 대한 경로 정보(루트 폴더의 계층 구조)를 검색할 수 있는 권한을 부여합니다.	Read			
GetResources	리소스 모음을 가져올 수 있는 권한을 부여합니다.	Read			
InitiateDocumentVersionUpload	새 문서 객체 및 버전 객체를 생성할 수 있는 권한을 부여합니다.	쓰기			
RegisterDirectory [권한만 해당]	디렉터리를 등록할 수 있는 권한을 부여합니다.	쓰기			
RemoveAllResourcePermissions	지정된 리소스에서 모든 권한을 제거할 수 있는 권한을 부여합니다.	쓰기			
RemoveResourcePermission	지정된 리소스에서 지정된 보안 주체의 권한을 제거할 수 있는 권한을 부여합니다.	쓰기			
UpdateDocument	지정된 문서의 지정된 속성을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateDocumentVersion	문서 버전의 상태를 ACTIVE로 변경할 수 있는 권한을 부여합니다.	쓰기			
UpdateFolder	지정된 폴더의 지정된 속성을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateInstanceAlias [권한만 해당]	인스턴스 별칭을 업데이트할 수 있는 권한을 부여합니다.	쓰기			
UpdateUser	지정된 사용자의 지정된 속성을 업데이트하고, Amazon WorkDocs 사이트에 대한 관리 권한을 부여하거나 취소할 수 있는 권한을 부여합니다.	쓰기			

Amazon WorkDocs에서 정의한 리소스 유형

Amazon WorkDocs는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon WorkDocs에 대한 액세스를 허용하려면 정책에서 `"Resource": "*"`를 지정하십시오.

Amazon WorkDocs에 사용되는 조건 키

WorkDocs에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon WorkLink에 사용되는 작업, 리소스 및 조건 키

Amazon WorkLink(서비스 접두사: `worklink`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon WorkLink에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateDomain	도메인을 Amazon WorkLink 플릿과 연결할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
AssociateWebsiteAuthorizationProvider	웹사이트 권한 부여 공급자를 Amazon WorkLink 플릿과 연결할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
AssociateWebsiteCertificateAuthority	웹사이트 인증 기관을 Amazon WorkLink 플릿과 연결할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
CreateFleet	Amazon WorkLink 플릿을 생성할 수 있는 권한을 부여합니다.	쓰기			
DeleteFleet	Amazon WorkLink 플릿을 삭제할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
DescribeAuditStreamConfiguration	Amazon WorkLink 플릿에 대한 감사 스트림 구성을 설명할 수 있는 권한을 부여합니다.	Read	fleet* (p. 1728)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeCompanyNetworkConfiguration	Amazon WorkLink 플릿에 대한 회사 네트워크 구성을 설명할 수 있는 권한을 부여합니다.	Read	fleet* (p. 1728)		
DescribeDevice	Amazon WorkLink 플릿과 연결된 디바이스 세부 정보를 설명할 수 있는 권한을 부여합니다.	Read	fleet* (p. 1728)		
DescribeDevicePolicyConfiguration	Amazon WorkLink 플릿에 대한 디바이스 정책 구성을 설명할 수 있는 권한을 부여합니다.	Read	fleet* (p. 1728)		
DescribeDomain	Amazon WorkLink 플릿과 연결된 도메인에 대한 세부 정보를 설명할 수 있는 권한을 부여합니다.	Read	fleet* (p. 1728)		
DescribeFleetMetadata	Amazon WorkLink 플릿의 메타데이터를 설명할 수 있는 권한을 부여합니다.	Read	fleet* (p. 1728)		
DescribeIdentityProviderConfiguration	Amazon WorkLink 플릿에 대한 자격 증명 공급자 구성을 설명할 수 있는 권한을 부여합니다.	Read	fleet* (p. 1728)		
DescribeWebsiteCertificateAuthority	Amazon WorkLink 플릿과 연결된 웹사이트 인증 기관을 설명할 수 있는 권한을 부여합니다.	Read	fleet* (p. 1728)		
DisassociateDomain	Amazon WorkLink 플릿에서 도메인을 연결 해제할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
DisassociateWebsiteAuthorizationProvider	Amazon WorkLink 플릿에서 웹사이트 권한 부여 공급자를 연결 해제할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
DisassociateWebsiteCertificateAuthority	Amazon WorkLink 플릿에서 웹사이트 인증 기관을 연결 해제할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
ListDevices	Amazon WorkLink 플릿과 연결된 디바이스를 나열할 수 있는 권한을 부여합니다.	List	fleet* (p. 1728)		
ListDomains	Amazon WorkLink 플릿에 연결된 도메인을 나열할 수 있는 권한을 부여합니다.	List	fleet* (p. 1728)		
ListFleets	계정과 연결된 Amazon WorkLink 플릿을 나열할 수 있는 권한을 부여합니다.	List			
ListWebsiteAuthorizationProviders	Amazon WorkLink 플릿에 대한 웹사이트 권한 부여 공급자를 나열할 수 있는 권한을 부여합니다.	List	fleet* (p. 1728)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListWebsiteCertificateAuthorities	Amazon WorkLink 플릿과 연결된 웹사이트 인증 기관을 나열할 수 있는 권한을 부여합니다.	List	fleet* (p. 1728)		
RestoreDomainAccess	Amazon WorkLink 플릿과 연결된 도메인에 대한 액세스 권한을 복원할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
RevokeDomainAccess	Amazon WorkLink 플릿과 연결된 도메인에 대한 액세스 권한을 취소할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
SignOutUser	Amazon WorkLink 플릿에서 사용자를 로그아웃시킬 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
UpdateAuditStreamConfiguration	Amazon WorkLink 플릿에 대한 감사 스트림 구성을 업데이트할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
UpdateCompanyNetworkConfiguration	Amazon WorkLink 플릿에 대한 회사 네트워크 구성을 업데이트할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
UpdateDevicePolicyConfiguration	Amazon WorkLink 플릿에 대한 디바이스 정책 구성을 업데이트할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
UpdateDomainMetadata	Amazon WorkLink 플릿과 연결된 도메인에 대한 메타데이터를 업데이트할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
UpdateFleetMetadata	Amazon WorkLink 플릿의 메타데이터를 업데이트할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		
UpdateIdentityProviderConfiguration	Amazon WorkLink 플릿에 대한 자격 증명 공급자 구성을 업데이트할 수 있는 권한을 부여합니다.	쓰기	fleet* (p. 1728)		

Amazon WorkLink에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1726)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
fleet	`arn:${Partition}:worklink::${Account}:fleet/${fleetName}`	

Amazon WorkLink에 사용되는 조건 키

WorkLink에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon WorkMail에 사용되는 작업, 리소스 및 조건 키

Amazon WorkMail(서비스 접두사: `workmail`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon WorkMail에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AddMembersToGroup [권한만 해당]	멤버(사용자 또는 그룹) 목록을 그룹에 추가합니다.	쓰기	organization* (p. 1736)		
AssociateDelegateToResource	멤버(사용자 또는 그룹)를 리소스의 대리인 집합에 추가합니다.	쓰기	organization* (p. 1736)		
AssociateMemberToGroup	멤버(사용자 또는 그룹)를 그룹의 집합에 추가합니다.	쓰기	organization* (p. 1736)		
CreateAlias	별칭을 WorkMail의 지정된 멤버(사용자 또는 그룹) 집합에 추가합니다.	쓰기	organization* (p. 1736)		
CreateGroup	RegisterToWorkMail 작업을 호출하여 WorkMail에서 사용할 수 있는 그룹을 생성합니다.	쓰기	organization* (p. 1736)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
CreateInboundMailFlowRule [권한만 해당]	조직에 보낸 모든 이메일에 적용되는 인바운드 이메일 흐름 규칙을 생성합니다.	쓰기	organization* (p. 1736)		
CreateMailDomain [권한만 해당]	메일 도메인을 생성합니다.	쓰기	organization* (p. 1736)		
CreateMailUser [권한만 해당]	디렉터리 및 WorkMail 스토리지에 사용자를 생성합니다. 단, 메일에서는 해당 사용자를 활성화하지 않습니다.	쓰기	organization* (p. 1736)		
CreateOrganization [권한만 해당]	기존 디렉터리를 사용하여 조직을 생성하거나 새 디렉터리를 즉시 생성합니다. 또한 상호 보완적 메일 도메인을 생성하고 활성화합니다. 선택적으로 KMS 키를 생성합니다.	쓰기			
CreateOutboundMailFlowRule [권한만 해당]	조직에서 보낸 모든 이메일에 적용되는 아웃바운드 이메일 흐름 규칙을 생성합니다.	쓰기	organization* (p. 1736)		
CreateResource	새로운 WorkMail 리소스를 생성합니다.	쓰기	organization* (p. 1736)		
CreateSmtpGateway [권한만 해당]	WorkMail 조직에 대해 SMTP 디바이스를 등록합니다.	쓰기	organization* (p. 1736)		
CreateUser	RegisterToWorkMail 작업을 호출하여 WorkMail에서 사용할 수 있는 사용자를 생성합니다.	쓰기	organization* (p. 1736)		
DeleteAccessControlRule	지정된 WorkMail 조직에 대한 액세스 제어 규칙을 삭제합니다.	쓰기	organization* (p. 1736)		
DeleteAlias	지정된 사용자 별칭 집합에서 지정된 별칭을 1개 이상 제거합니다.	쓰기	organization* (p. 1736)		
DeleteGroup	그룹을 WorkMail에서 삭제합니다.	쓰기	organization* (p. 1736)		
DeleteInboundMailFlowRule [권한만 해당]	조직에 보낸 이메일에 더 이상 적용되지 않도록 인바운드 이메일 흐름 규칙을 제거합니다.	쓰기	organization* (p. 1736)		
DeleteMailDomain [권한만 해당]	사용하지 않는 메일 도메인을 조직에서 제거합니다.	쓰기	organization* (p. 1736)		
DeleteMailboxPermissions	멤버(사용자 또는 그룹)에게 부여된 권한을 삭제합니다.	쓰기	organization* (p. 1736)		
DeleteMobileDevice [권한만 해당]	사용자에게서 모바일 디바이스를 제거합니다.	쓰기	organization* (p. 1736)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DeleteOrganization [권한만 해당]	조직을 계정에서 제거합니다. 이때 디렉터리까지 디렉터리 서비스에서 제거하거나 나중에 사용할 수 있도록 남겨 놓습니다.	쓰기	organization* (p. 1736)		
DeleteOutboundMailFlowRule [권한만 해당]	조직에서 보낸 이메일에 더 이상 적용되지 않도록 아웃바운드 이메일 흐름 규칙을 제거합니다.	쓰기	organization* (p. 1736)		
DeleteResource	지정된 리소스를 삭제합니다.	쓰기	organization* (p. 1736)		
DeleteSmtpGateway [권한만 해당]	조직에서 SMTP 디바이스를 제거합니다.	쓰기	organization* (p. 1736)		
DeleteUser	WorkMail과 이후 모든 시스템에서 사용자를 삭제합니다. 이 작업은 실행 취소할 수 없습니다.	쓰기	organization* (p. 1736)		
DeregisterFromWorkMail	사용자, 그룹 또는 리소스를 WorkMail에서 더 이상 사용하지 않는 것으로 표시합니다.	쓰기	organization* (p. 1736)		
DescribeDirectories [권한만 해당]	조직을 생성할 때 사용할 수 있는 디렉터리 목록을 표시합니다.	List			
DescribeGroup	그룹에 사용할 수 있는 데이터를 반환합니다.	List	organization* (p. 1736)		
DescribeInboundMailFlowRule [권한만 해당]	조직에 대해 구성된 인바운드 메일 흐름 규칙의 세부 정보를 반환합니다.	Read	organization* (p. 1736)		
DescribeKmsKeys [권한만 해당]	조직을 생성할 때 사용할 수 있는 KMS 키 목록을 표시합니다.	List			
DescribeMailDomains [권한만 해당]	조직과 연결된 모든 메일 도메인의 세부 정보를 표시합니다.	List	organization* (p. 1736)		
DescribeMailGroups [권한만 해당]	조직과 연결된 모든 그룹의 세부 정보를 표시합니다.	List	organization* (p. 1736)		
DescribeMailUsers [권한만 해당]	조직과 연결된 모든 사용자의 세부 정보를 표시합니다.	List	organization* (p. 1736)		
DescribeOrganization	식별자를 기준으로 지정된 조직에 대한 정보를 추가로 제공합니다.	List	organization* (p. 1736)		
DescribeOrganizations [권한만 해당]	계정과 연결된 모든 조직을 요약하여 표시합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeOutboundMailFlowRules [권한만 해당]	조직에 대해 구성된 아웃바운드 메일 흐름 규칙의 세부 정보를 반환합니다.	Read	organization* (p. 1736)		
DescribeResource	리소스에 사용할 수 있는 데이터를 반환합니다.	List	organization* (p. 1736)		
DescribeSmtpGateway [권한만 해당]	조직에 대해 등록된 SMTP 디바이스의 세부 정보를 반환합니다.	Read	organization* (p. 1736)		
DescribeUser	사용자에 대한 정보를 제공합니다.	List	organization* (p. 1736)		
DisableMailGroups [권한만 해당]	사용하지 않는 메일 그룹을 비활성화하여 삭제할 수 있도록 허용합니다.	쓰기	organization* (p. 1736)		
DisableMailUsers [권한만 해당]	사용하지 않는 사용자 메일박스를 비활성화하여 삭제할 수 있도록 허용합니다.	쓰기	organization* (p. 1736)		
DisassociateDelegateFromResource	리소스의 대리인 집합에서 멤버를 제거합니다.	쓰기	organization* (p. 1736)		
DisassociateMemberFromGroup	그룹에서 멤버를 제거합니다.	쓰기	organization* (p. 1736)		
EnableMailDomain [권한만 해당]	조직의 메일 도메인을 활성화합니다.	쓰기	organization* (p. 1736)		
EnableMailGroups [권한만 해당]	생성된 메일 그룹을 활성화하여 메일을 수신할 수 있도록 허용합니다.	쓰기	organization* (p. 1736)		
EnableMailUsers [권한만 해당]	생성된 사용자의 메일박스를 활성화하여 메일을 수신할 수 있도록 허용합니다.	쓰기	organization* (p. 1736)		
GetAccessControlEffect	조직의 액세스 제어 규칙이 지정된 IPv4 주소, 액세스 프로토콜 작업 또는 사용자 ID에 적용될 때 미치는 영향을 가져옵니다.	Read	organization* (p. 1736)		
GetJournalingRules [권한만 해당]	이메일 저널링에 대해 구성된 저널링 및 폴백 이메일 주소를 반환합니다.	Read	organization* (p. 1736)		
GetMailDomainDetails [권한만 해당]	메일 도메인의 세부 정보를 가져옵니다.	Read	organization* (p. 1736)		
GetMailGroupDetails [권한만 해당]	메일 그룹의 세부 정보를 가져옵니다.	Read	organization* (p. 1736)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetMailUserDetails [권한만 해당]	사용자의 메일박스 및 계정에 대한 세부 정보를 가져옵니다.	Read	organization* (p. 1736)		
GetMailboxDetails	사용자의 메일박스에 대한 세부 정보를 반환합니다.	Read	organization* (p. 1736)		
GetMobileDeviceDetails [권한만 해당]	모바일 디바이스의 세부 정보를 가져옵니다.	Read	organization* (p. 1736)		
GetMobileDevicesForUser [권한만 해당]	사용자와 연결된 모바일 디바이스 목록을 가져옵니다.	Read	organization* (p. 1736)		
GetMobilePolicyDetails [권한만 해당]	조직과 연결된 모바일 디바이스 정책의 세부 정보를 가져옵니다.	Read	organization* (p. 1736)		
ListAccessControlRules	지정된 조직에 대한 액세스 제어 규칙을 나열합니다.	List	organization* (p. 1736)		
ListAliases	페이지가 매겨진 호출을 생성하여 지정된 개체와 연결된 별칭을 나열합니다.	List	organization* (p. 1736)		
ListGroupMembers	그룹 구성원에 대한 개요를 반환합니다. 사용자와 그룹이 그룹 멤버가 될 수 있습니다.	List	organization* (p. 1736)		
ListGroups	조직 그룹을 요약하여 반환합니다.	List	organization* (p. 1736)		
ListInboundMailFlowRules [권한만 해당]	조직에 대해 구성된 인바운드 메일 흐름 규칙의 목록을 반환합니다.	List	organization* (p. 1736)		
ListMailboxPermissions	사용자, 그룹 또는 리소스 메일박스와 연결된 메일박스 권한을 나열합니다.	List	organization* (p. 1736)		
ListMembersInMailGroup [권한만 해당]	메일 그룹에 속한 모든 멤버 목록을 가져옵니다.	Read	organization* (p. 1736)		
ListOrganizations	삭제되지 않은 고객의 조직을 요약하여 반환합니다.	List			
ListOutboundMailFlowRules [권한만 해당]	조직에 대해 구성된 아웃바운드 메일 흐름 규칙의 목록을 반환합니다.	List	organization* (p. 1736)		
ListResourceDelegates	리소스와 연결된 대리인을 나열합니다.	List	organization* (p. 1736)		
ListResources	조직의 리소스를 요약하여 반환합니다.	List	organization* (p. 1736)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
ListSmtpGateways [권한만 해당]	조직에 대해 등록된 SMTP 디바이스 목록을 반환합니다.	List	organization* (p. 1736)		
ListTagsForResource	Amazon WorkMail 조직 리소스에 적용된 태그를 나열할 수 있는 권한을 부여합니다.	List	organization* (p. 1736)		
ListUsers	조직의 사용자를 요약하여 반환합니다.	List	organization* (p. 1736)		
PutAccessControlRule	지정된 조직에 대한 새 액세스 제어 규칙을 추가합니다. 이 규칙은 지정된 IPv4 주소, 액세스 프로토콜 작업 및 사용자 ID에 대한 조직의 액세스를 허용하거나 거부합니다. 기존 규칙과 이름이 같은 새 규칙을 추가하면 이전 규칙이 대체됩니다.	쓰기	organization* (p. 1736)		
PutMailboxPermissions	사용자, 그룹 또는 리소스에 대한 권한을 설정합니다. 그러면 기존에 존재하던 권한을 모두 대체하게 됩니다.	쓰기	organization* (p. 1736)		
RegisterToWorkMail	기존에 비활성화된 사용자, 그룹 또는 리소스를 사용할 수 있도록 메일박스와 일정 관리 기능을 연결하여 등록합니다.	쓰기	organization* (p. 1736)		
RemoveMembersFromGroup [권한만 해당]	메일 그룹에서 멤버를 제거합니다.	쓰기	organization* (p. 1736)		
ResetPassword	관리자에게 사용자 암호를 재설정할 수 있도록 허용합니다.	쓰기	organization* (p. 1736)		
ResetUserPassword [권한만 해당]	사용자 계정 암호를 재설정합니다.	쓰기	organization* (p. 1736)		
SearchMembers [권한만 해당]	검색에 접두사를 추가하여 메일 그룹에서 특정 사용자를 찾습니다.	Read	organization* (p. 1736)		
SetAdmin [권한만 해당]	사용자를 관리자로 표시합니다.	쓰기	organization* (p. 1736)		
SetDefaultMailDomain [권한만 해당]	조직의 기본 메일 도메인을 설정합니다.	쓰기	organization* (p. 1736)		
SetJournalingRule [권한만 해당]	이메일 저널링에 대한 저널링 및 폴백 이메일 주소를 설정합니다.	쓰기	organization* (p. 1736)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
SetMailGroupDetails [권한만 해당]	방금 생성된 메일 그룹의 세부 정보를 설정합니다.	쓰기	organization* (p. 1736)		
SetMailUserDetails [권한만 해당]	방금 생성된 사용자 계정의 세부 정보를 설정합니다.	쓰기	organization* (p. 1736)		
SetMobilePolicyDetails [권한만 해당]	조직과 연결된 모바일 정책의 세부 정보를 설정합니다.	쓰기	organization* (p. 1736)		
TagResource	지정된 Amazon WorkMail 조직 리소스에 태그를 지정할 권한을 부여합니다.	태그 지정	organization* (p. 1736)		
TestInboundMailFlowRules [권한만 해당]	지정된 발신자 및 수신자가 있는 이메일에 적용할 인바운드 규칙을 테스트합니다.	쓰기	organization* (p. 1736)		
TestOutboundMailFlowRules [권한만 해당]	지정된 발신자 및 수신자가 있는 이메일에 적용할 아웃바운드 규칙을 테스트합니다.	쓰기	organization* (p. 1736)		
UntagResource	지정된 Amazon WorkMail 조직 리소스의 태그를 해제할 권한을 부여합니다.	태그 지정	organization* (p. 1736)		
UpdateInboundMailFlowRule [권한만 해당]	조직에 보낸 모든 이메일에 적용되는 인바운드 이메일 흐름 규칙의 세부 정보를 업데이트합니다.	쓰기	organization* (p. 1736)		
UpdateMailboxQuota	사용자 메일박스의 최대 크기(MB)를 업데이트합니다.	쓰기	organization* (p. 1736)		
UpdateOutboundMailFlowRule [권한만 해당]	조직에서 보낸 모든 이메일에 적용되는 아웃바운드 이메일 흐름 규칙의 세부 정보를 업데이트합니다.	쓰기	organization* (p. 1736)		
UpdatePrimaryEmailAddress	사용자, 그룹 또는 리소스의 기본 이메일을 업데이트합니다.	쓰기	organization* (p. 1736)		
UpdateResource	리소스 날짜를 업데이트합니다. 최신 정보를 가져오려면 DescribeResource 호출이 선행되어야 합니다.	쓰기	organization* (p. 1736)		
UpdateSmtpGateway [권한만 해당]	조직에 대해 등록된 기존 SMTP 디바이스의 세부 정보를 업데이트합니다.	쓰기	organization* (p. 1736)		
WipeMobileDevice [권한만 해당]	사용자 계정과 연결된 모바일 디바이스를 원격으로 삭제합니다.	쓰기	organization* (p. 1736)		

Amazon WorkMail에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1729)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
organization	`arn:${Partition}:workmail:${Region}:${Account}:organization/${ResourceId}`	aws:ResourceTag/${TagKey} (p. 1736)

Amazon WorkMail의 조건 키

Amazon WorkMail은 IAM 정책의 `Condition` 요소에 사용할 수 있는 다음과 같은 조건 키를 정의합니다. 이러한 키를 사용하여 정책 설명이 적용되는 조건을 추가로 재정의할 수 있습니다. 다음 테이블의 열에 대한 자세한 내용은 조건 키 테이블 (p. 674) 단원을 참조하십시오.

모든 서비스에 사용할 수 있는 글로벌 조건 키를 보려면 IAM 정책 참조의 사용 가능한 글로벌 조건 키를 참조하십시오.

조건 키	설명	유형
aws:RequestTag/${TagKey}	요청에 태그 키-값 페어가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열
aws:ResourceTag/${TagKey}	리소스에 연결된 태그 키-값 페어를 기준으로 작업을 필터링합니다.	문자열
aws:TagKeys	요청에 태그 키가 있는지 여부를 기준으로 작업을 필터링합니다.	문자열

Amazon WorkMail 메시지 흐름에 사용되는 작업, 리소스 및 조건 키

Amazon WorkMail 메시지 흐름(서비스 접두사: `workmailmessageflow`)은 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

- Amazon WorkMail 메시지 흐름에 의해 정의된 작업 (p. 1737)
- Amazon WorkMail Message Flow에서 정의한 리소스 유형 (p. 1737)
- Amazon WorkMail 메시지 흐름에 사용되는 조건 키 (p. 1737)

Amazon WorkMail 메시지 흐름에 의해 정의된 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetRawMessageContent	지정된 메시지 ID를 사용하여 이메일 메시지의 콘텐츠를 읽을 수 있는 권한을 부여합니다.	Read	RawMessage* (p. 1737)		

Amazon WorkMail Message Flow에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1737)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
RawMessage	`arn:${Partition}:workmailmessageflow:${Region}:${Account}:message/${OrganizationId}/${Context}/${MessageId}`	

Amazon WorkMail 메시지 흐름에 사용되는 조건 키

WorkMail 메시지 흐름에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon WorkSpaces에 사용되는 작업, 리소스 및 조건 키

Amazon WorkSpaces(서비스 접두사: `workspaces`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon WorkSpaces에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AssociateIpGroups	지정된 IP 액세스 제어 그룹을 지정된 디렉터리와 연결합니다.	쓰기			
AuthorizeIpRules	지정된 IP 액세스 제어 그룹에 하나 이상의 규칙을 추가합니다.	쓰기	workspaceipgroup* (p. 1740)		
CreateIpGroup	IP 액세스 제어 그룹을 생성합니다.	쓰기			
CreateTags	WorkSpace에 대해 태그를 생성합니다.	태그 지정			
CreateWorkspaces	하나 이상의 WorkSpaces를 생성합니다.	쓰기	directoryid* (p. 1740)		
			workspacebundle* (p. 1740)		
DeleteIpGroup	지정된 IP 액세스 제어 그룹을 삭제합니다.	쓰기	workspaceipgroup* (p. 1740)		
DeleteTags	WorkSpace에서 태그를 삭제합니다.	쓰기			
DeleteWorkspaceImage	지정된 작업 영역 이미지를 삭제합니다.	쓰기			
DescribeAccount	지정된 계정의 기존 보유 라이선스 사용(BYOL) 구성을 설명하는 목록을 검색합니다.	List			
DescribeAccountModifications	지정된 계정의 기존 보유 라이선스 사용(BYOL) 구성에 대한 수정을 설명하는 목록을 검색합니다.	List			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
DescribeClientProperties	지정된 리소스에 대한 클라이언트 속성을 설명합니다.	List	directoryid* (p. 1740)		
DescribeIpGroups	리전 내 사용자 계정의 IP 액세스 제어 그룹에 대한 정보를 검색합니다.	List	workspaceipgroup* (p. 1740)		
DescribeTags	WorkSpace에 대한 태그를 설명합니다.	List			
DescribeWorkspaceBundles	지정된 리전에서 계정이 사용할 수 있는 WorkSpace 번들에 대한 정보를 가져옵니다.	List	workspacebundle* (p. 1740)		
DescribeWorkspaceDirectories	Amazon WorkSpaces에 등록되어 있고 계정이 사용할 수 있는 리전의 AWS Directory Service 디렉터리에 대한 정보를 검색합니다.	List			
DescribeWorkspaceImages	하나 이상의 지정된 이미지를 설명하는 목록을 검색합니다.	List			
DescribeWorkspaces	지정된 WorkSpaces에 대한 정보를 가져옵니다.	List			
DescribeWorkspacesConnectionStatus	지정된 WorkSpace의 연결 상태를 설명합니다.	Read			
DisassociateIpGroups	지정된 디렉터리에서 지정된 IP 액세스 제어 그룹을 연결 해제합니다.	쓰기			
ImportWorkspaceImage	라이선스가 부여된 EC2 이미지를 Amazon WorkSpaces로 가져옵니다.	쓰기			
ListAvailableManagementCidrRanges	CIDR 범위 제약 조건에 대해 사용 가능한 CIDR 범위를 나열합니다	List			
ModifyAccount	지정된 계정의 기존 보유 라이선스 사용(BYOL) 구성을 수정합니다.	쓰기			
ModifyClientProperties	지정된 리소스의 클라이언트 속성을 수정합니다.	쓰기	directoryid* (p. 1740)		
ModifyWorkspaceProperties	실행 모드 및 AutoStop 시간을 포함한 WorkSpace 속성을 수정합니다.	쓰기	workspaceid* (p. 1740)		
ModifyWorkspaceState	지정된 WorkSpaces의 상태를 수정합니다.	쓰기	workspaceid* (p. 1740)		
RebootWorkspaces	지정된 WorkSpaces를 재부팅합니다.	쓰기	workspaceid* (p. 1740)		

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
RebuildWorkspaces	지정된 WorkSpaces를 재구축합니다.	쓰기	workspaceid* (p. 1740)		
RevokeIpRules	지정된 IP 액세스 제어 그룹에서 하나 이상의 규칙을 제거합니다.	쓰기	workspaceipgroup* (p. 1740)		
StartWorkspaces	지정된 WorkSpaces를 시작합니다.	쓰기	workspaceid* (p. 1740)		
StopWorkspaces	지정된 WorkSpaces를 중지합니다.	쓰기	workspaceid* (p. 1740)		
TerminateWorkspaces	지정된 WorkSpaces를 종료합니다.	쓰기	workspaceid* (p. 1740)		
UpdateRulesOfIpGroup	지정된 IP 액세스 제어 그룹의 현재 규칙을 지정된 규칙으로 대체합니다.	쓰기	workspaceipgroup* (p. 1740)		

Amazon WorkSpaces에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1738)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
workspacebundle	`arn:${Partition}:workspaces:${Region}:${Account}:workspacebundle/${BundleId}`	
workspaceipgroup	`arn:${Partition}:workspaces:${Region}:${Account}:workspaceipgroup/${GroupId}`	
directoryid	`arn:${Partition}:workspaces:${Region}:${Account}:directory/${DirectoryId}`	
workspaceid	`arn:${Partition}:workspaces:${Region}:${Account}:workspace/${WorkspaceId}`	

Amazon WorkSpaces에 사용되는 조건 키

WorkSpaces에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

Amazon WorkSpaces Application Manager에 사용되는 작업, 리소스 및 조건 키

Amazon WorkSpaces Application Manager(서비스 접두사: `wam`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

Amazon WorkSpaces Application Manager에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
AuthenticatePackage [권한만 해당]	Amazon WAM 패키징 인스턴스가 애플리케이션 패키지 카탈로그에 액세스할 수 있도록 허용합니다.	쓰기			

Amazon WorkSpaces Application Manager에서 정의한 리소스 유형

Amazon WorkSpaces Application Manager는 IAM 정책 문의 `Resource` 요소에 리소스 ARN을 지정하는 기능을 지원하지 않습니다. Amazon WorkSpaces Application Manager에 대한 액세스를 허용하려면 정책에 `"Resource": "*"`를 지정합니다.

Amazon WorkSpaces Application Manager에 사용되는 조건 키

WAM에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

AWS X-Ray에 사용되는 작업, 리소스 및 조건 키

AWS X-Ray(서비스 접두사: `xray`)는 IAM 권한 정책에 사용할 수 있는 다음과 같은 서비스별 리소스, 작업 및 조건 컨텍스트 키를 제공합니다.

참조:

- 이 서비스를 구성하는 방법을 알아봅니다.
- 이 서비스에 사용 가능한 API 작업의 목록을 봅니다.
- IAM 권한 정책을 사용하여 이 서비스와 리소스를 보호하는 방법을 알아봅니다.

주제

AWS X-Ray에서 정의한 작업

IAM 정책 설명의 `Action` 요소에서 다음 작업을 지정할 수 있습니다. 정책을 사용하여 AWS에서 작업할 수 있는 권한을 부여합니다. 정책에서 작업을 사용하면 일반적으로 이름이 같은 API 작업 또는 CLI 명령에 대한 액세스를 허용하거나 거부합니다. 그러나 경우에 따라 하나의 작업으로 둘 이상의 작업에 대한 액세스가 제어됩니다. 또는 일부 작업을 수행하려면 다양한 작업이 필요합니다.

리소스 유형 열에는 각 작업이 리소스 수준 권한을 지원하는지 여부가 표시됩니다. 리소스 열에 값이 없으면 정책 문의 `Resource` 요소에서 모든 리소스("*")를 지정해야 합니다. 리소스 열에 리소스 유형이 포함되어 있으면 해당 작업 시 문에서 해당 유형의 ARN을 지정할 수 있습니다. 필수 리소스는 테이블에서 별표(*)로 표시됩니다. 이 작업을 사용해 문에서 리소스 레벨 권한 ARN을 지정할 경우 이 유형이 되어야 합니다. 일부 작업은 다수의 리소스 유형을 지원합니다. 리소스 유형이 옵션(필수 리소스로 표시되지 않은 경우)인 경우에는 한 가지를 선택할 수 있지만 나머지는 선택하지 못합니다.

다음 테이블의 열에 대한 자세한 내용은 작업 테이블 (p. 674) 단원을 참조하십시오.

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
BatchGetTraces	ID로 지정된 트레이스의 목록을 검색합니다. 각 트레이스는 단일 요청에서 시작되는 세그먼트 문서의 모음입니다. GetTraceSummaries를 사용하여 트레이스 ID의 목록을 가져옵니다.	Read			
CreateGroup	이름 및 필터 표현식으로 그룹 리소스를 생성합니다.	쓰기	group* (p. 1744)		
CreateSamplingRule	계측된 애플리케이션에 대한 샘플링 동작을 제어하는 규칙을 생성합니다.	쓰기	sampling-rule* (p. 1744)		
DeleteGroup	그룹 리소스를 삭제합니다.	쓰기	group* (p. 1744)		
DeleteSamplingRule	샘플링 규칙을 삭제합니다.	쓰기	sampling-rule* (p. 1744)		
GetEncryptionConfig	X-Ray 데이터에 대한 현재 암호화 구성을 검색합니다.	권한 관리			
GetGroup	그룹 리소스 세부 정보를 검색합니다.	Read	group* (p. 1744)		
GetGroups	모든 활성 그룹 세부 정보를 검색합니다.	Read			
GetSamplingRules	모든 샘플링 규칙을 검색합니다.	Read			

Actions	설명	액세스 레벨	리소스 유형(*필수)	조건 키	종속 작업
GetSamplingStatisticSummaries	모든 샘플링 규칙의 최근 샘플링 결과에 대한 정보를 검색합니다.	Read			
GetSamplingTargets	서비스가 요청을 샘플링하기 위해 사용하는 규칙에 대한 샘플링 할당량을 요청합니다.	Read			
GetServiceGraph	수신 요청을 처리하는 서비스와 결과로 호출되는 다운스트림 서비스를 설명하는 문서를 검색합니다.	Read			
GetTimeSeriesServiceStatistics	시간 간격으로 버킷팅된 특정 시간 범위에 의해 정의되는 서비스 통계의 집계를 가져옵니다.	Read			
GetTraceGraph	하나 이상의 특정 트레이스 ID에 대한 서비스 그래프를 검색합니다.	Read			
GetTraceSummaries	선택 사항인 필터를 사용하여 지정된 기간에 사용할 수 있는 트레이스에 대한 ID 및 메타데이터를 검색합니다. 전체 트레이스를 가져오려면 트레이스 ID를 BatchGetTraces에 전달합니다.	Read			
PutEncryptionConfig	X-Ray 데이터에 대한 암호화 구성을 업데이트합니다.	권한 관리			
PutTelemetryRecords	AWS X-Ray 데몬에서 원격 측정을 서비스로 전송하는 데 사용됩니다.	쓰기			
PutTraceSegments	세그먼트 문서를 AWS X-Ray에 업로드합니다. X-Ray SDK는 세그먼트 문서를 생성하고 이를 X-Ray 데몬으로 전송하여 일괄적으로 업로드합니다.	쓰기			
UpdateGroup	그룹 리소스를 업데이트합니다.	쓰기	group* (p. 1744)		
UpdateSamplingRule	샘플링 규칙의 구성을 수정합니다	쓰기	sampling-rule* (p. 1744)		

AWS X-Ray에서 정의한 리소스 유형

다음 리소스 유형은 이 서비스에서 정의되며 IAM 권한 정책 설명의 `Resource` 요소에서 사용할 수 있습니다. 작업 테이블 (p. 1742)의 각 작업은 해당 작업으로 지정할 수 있는 리소스 유형을 식별합니다. 리소스 유형은 정책에 포함할 수 있는 조건 키를 정의할 수도 있습니다. 이러한 키는 테이블의 마지막 열에 표시됩니다. 다음 테이블의 열에 대한 자세한 내용은 리소스 유형 테이블 (p. 674) 단원을 참조하십시오.

리소스 유형	ARN	조건 키
group	`arn:${Partition}:xray:${Region}:${Account}:group/${GroupName}/${Id}`	
sampling-rule	`arn:${Partition}:xray:${Region}:${Account}:sampling-rule/${SamplingRuleName}`	

AWS X-Ray에 사용되는 조건 키

X-Ray에는 정책 설명의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. 모든 서비스에 사용할 수 있는 글로벌 컨텍스트 키의 목록은 IAM 정책 참조의 사용 가능한 조건 키를 참조하십시오.

리소스

IAM은 풍부한 기능을 갖춘 제품이며, IAM으로 AWS 계정 및 리소스를 보호하는 방법이 자세히 설명된 리소스가 많이 있습니다.

주제

사용자 및 그룹

사용자 및 그룹을 생성하고, 관리하고, 사용하는 방법은 다음 리소스를 참조하십시오.

- 첫 번째 IAM 관리자 및 그룹 생성 (p. 20) – IAM 사용자를 생성하고 권한을 할당하는 방법을 보여 주는 단계별 절차입니다.
- 자격 증명(사용자, 그룹, 및 역할) (p. 83) – IAM 사용자 및 그룹 관리 방법을 심층적으로 다룹니다.
- 계정, 사용자 및 그룹을 사용하는 경우에 대한 지침 – AWS 보안 블로그 게시물로, IAM 사용자 및 그룹이 단일 계정을 사용하거나 별도의 AWS 계정을 사용하도록 사용자 액세스를 구성하는 방법을 다룹니다.

자격 증명(암호, 액세스 키 및 MFA 디바이스)

AWS 계정 및 IAM 사용자의 암호를 관리하는 방법은 다음 가이드를 검토하십시오. AWS에 대한 프로그래밍 호출을 하는 데 사용되는 보안 키인 액세스 키에 대한 정보도 찾을 수 있습니다.

- AWS 보안 자격 증명 – Amazon Web Services에 액세스하는 데 사용되는 자격 증명의 유형을 설명하고, 자격 증명을 생성 및 관리하는 방법을 살펴보고, 액세스 키를 안전하게 관리하기 위한 권장 사항을 소개합니다.
- 암호 관리 (p. 100) 및 IAM 사용자의 액세스 키 관리 (p. 111) – 계정의 IAM 사용자에 대한 자격 증명 관리 옵션을 설명합니다.
- AWS에서 멀티 팩터 인증(MFA) 사용하기 (p. 119) – 디바이스에서 암호와 일회용 코드를 둘 다 입력해야 로그인이 허용되도록 계정 및 IAM 사용자를 구성하는 방법을 설명합니다. (이를 이중 인증이라고도 부릅니다.)

권한 및 정책

IAM 정책 내부의 작동 방식과 함께 가장 효과적으로 권한을 부여하는 방법도 알아보십시오.

- 정책 및 권한 (p. 349) – 권한을 정의하는 데 사용되는 정책 언어를 소개합니다. 사용자나 그룹에 또는 일부 AWS 제품의 경우 리소스 자체에 권한을 연결하는 방법을 설명합니다.
- IAM JSON 정책 요소 참조 (p. 586) – 각 정책 언어 요소에 대한 설명과 예제를 소개합니다.

- IAM 자격 증명 기반 정책 예제 (p. 387) – 다양한 AWS 제품의 일반적인 작업에 대한 몇 가지 정책 예제를 보여 줍니다.
- AWS 정책 생성기 – 목록에서 제품과 작업을 선택하여 사용자 지정 정책을 생성합니다.
- IAM 정책 시뮬레이터 – 정책에서 AWS에 대한 특정 요청을 허용할지 아니면 거부할지 여부를 테스트합니다.

연동 및 위임

다른 곳에서 인증된(로그인한) 사용자에게 AWS 계정의 리소스에 대한 액세스 권한을 부여할 수 있습니다. 여기에는 다른 AWS 계정의 IAM 사용자(위임), 해당 조직의 로그인 프로세스를 통해 인증된 사용자, Login with Amazon, Facebook, Google 또는 기타 OpenID Connect(OIDC) 호환 자격 증명 공급자 등 인터넷 자격 증명 공급자의 사용자가 포함될 수 있습니다. 이 경우 사용자는 AWS 리소스에 액세스할 수 있는 임시 보안 자격 증명을 받게 됩니다.

- 자습서: IAM 역할을 사용한 AWS 계정 간 액세스 권한 위임 (p. 30) – 다른 AWS 계정의 IAM 사용자에게 교차 계정 액세스 권한을 부여하는 방법을 설명합니다.
- 임시 자격 증명과 관련된 일반적인 시나리오 (p. 302) – AWS 외부에서 인증된 사용자를 AWS로 연동하는 방법을 설명합니다.
- Web Identity Federation Playground – Login with Amazon, Google 또는 Facebook을 사용하여 Amazon S3에 인증한 다음 호출해 봅니다.

IAM 및 기타 AWS 제품

대부분의 AWS 제품은 IAM과 통합되므로 IAM 기능을 사용하여 그러한 제품의 리소스에 대한 액세스를 보호할 수 있습니다. 다음 리소스에서는 IAM 및 가장 인기 있는 일부 AWS 제품의 보안을 다룹니다. IAM을 사용하는 전체 제품 목록과 각각의 추가 정보 링크는 IAM로 작업하는 AWS 서비스 (p. 573) 단원을 참조하십시오.

Using IAM with Amazon EC2

- Amazon EC2 리소스에 대한 액세스 제어 – 사용자가 Amazon EC2 인스턴스, 볼륨 등을 관리할 수 있도록 IAM 기능으로 허용하는 방법을 설명합니다.
- 인스턴스 프로파일 사용 (p. 271) – IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되면서 다른 AWS 제품에 액세스해야 하는 애플리케이션에 안전하게 자격 증명을 제공하는 방법을 설명합니다.

Using IAM with Amazon S3

- Amazon S3 리소스에 대한 액세스 권한 관리 – Amazon S3 정책을 포함하여 버킷 및 객체에 대한 IAM 보안 모델을 다룹니다.
- IAM 정책 작성: Amazon S3 버킷의 사용자별 폴더에 대한 액세스 권한 부여 – 사용자가 Amazon S3의 자체 폴더를 직접 보호하는 방법을 다룹니다. (Amazon S3 및 IAM에 대한 게시물을 더 보려면 블로그 게시물 제목 아래에서 S3 태그를 선택하십시오.)

Using IAM with Amazon RDS

- AWS Identity and Access Management(IAM)를 사용하여 Amazon RDS 리소스에 대한 액세스 관리 – IAM을 사용하여 데이터베이스 인스턴스, 데이터베이스 스냅샷 등에 대한 액세스 권한을 제어하는 방법을 설명합니다.

- RDS 리소스 수준 권한에 대한 소개 – IAM을 사용하여 특정 Amazon RDS 인스턴스에 대한 액세스를 제어하는 방법을 다룹니다.

Using IAM with Amazon DynamoDB

- IAM을 사용하여 DynamoDB 리소스에 대한 액세스 제어 – 사용자가 DynamoDB 테이블과 인덱스를 관리할 수 있도록 IAM으로 허용하는 방법을 설명합니다.
- 다음 동영상(8:55)에서는 개별 DynamoDB 데이터베이스 항목이나 속성(또는 둘 다)에 대한 액세스 제어를 제공하는 방법을 설명합니다.

  Getting Started with Fine-Grained Access Control for DynamoDB

일반 보안 사례

AWS 계정과 리소스를 보호하는 가장 좋은 방법에 대한 전문적인 팁과 지침을 찾아보십시오.

- AWS 보안 모범 사례(PDF) – AWS 계정과 제품 전반에서 보안을 관리하는 방법을 비롯하여 보안 아키텍처, IAM 사용, 암호화 및 데이터 보안 등에 대한 권장 사항을 자세하게 살펴 봅니다.
- IAM 모범 사례 (p. 60) – IAM을 사용하여 AWS 계정과 리소스를 보호하는 방법에 대한 권장 사항을 제시합니다.
- AWS CloudTrail User Guide – AWS CloudTrail을 사용하여 AWS에 대한 API 호출 기록을 추적하고 로그 파일에 해당 정보를 저장합니다. 이를 통해 계정의 리소스에 액세스한 사용자와 계정, 호출이 발생한 시기, 요청된 작업 등을 확인할 수 있습니다.

일반 리소스

다음 리소스에서 IAM 및 AWS에 대해 자세히 알아보십시오.

- IAM에 대한 제품 정보 – AWS Identity and Access Management 제품에 대한 일반 정보입니다.
- AWS Identity and Access Management 토론 포럼 – IAM과 관련된 기술적 질문에 대해 토론할 수 있는 고객을 위한 커뮤니티 포럼입니다.

- 교육 및 워크숍 – 역할 기반의 과정 및 전문 과정은 물론 자습형 실습에 대한 링크를 통해 AWS 기술을 연마하고 실용적인 경험을 쌓을 수 있습니다.
- AWS 개발자 도구 – AWS 애플리케이션을 개발 및 관리하기 위한 개발자 도구, SDK, IDE 도구 키트 및 명령줄 도구 링크.
- AWS 백서 – AWS 솔루션 아키텍트 또는 기타 기술 전문가가 아키텍처, 보안 및 경제 등의 주제에 대해 작성한 포괄적 AWS 기술 백서 목록의 링크.
- AWS Support 센터 – AWS 지원 사례를 생성 및 관리하는 허브. 또한 포럼, 기술 FAQ, 서비스 상태 및 AWS Trusted Advisor 등의 기타 유용한 자료에 대한 링크가 있습니다.
- AWS Support – 클라우드에서 1대 1로 애플리케이션을 구축 및 실행하도록 지원하는 빠른 응답 지원 채널인 AWS Support에 대한 정보가 포함된 기본 웹 페이지.
- 문의처 – AWS 결제, 계정, 이벤트, 침해 및 기타 문제에 대해 문의할 수 있는 중앙 연락 창구입니다.
- AWS 사이트 약관 – 저작권 및 상표, 사용자 계정, 라이선스 및 사이트 액세스와 기타 주제에 대한 세부 정보.

HTTP 쿼리 요청을 통한 API 호출

주제

이 단원에는 Query API for AWS Identity and Access Management(IAM) 및 AWS Security Token Service(AWS STS) 사용에 대한 일반적인 정보가 포함되어 있습니다. API 작업 및 오류에 대한 자세한 내용은 IAM API Reference 또는 AWS Security Token Service API Reference를 참조하십시오.

> **Note**
>
> IAM 또는 AWS STS API 작업을 직접 호출하는 대신 AWS SDK 중 하나를 사용할 수 있습니다. AWS SDK는 다양한 프로그래밍 언어 및 플랫폼(Java, Ruby, .NET, iOS, Android 등)을 위한 라이브러리와 샘플 코드로 구성되어 있습니다. SDK를 사용하면 편리하게 IAM 및 AWS에 프로그래밍 방식으로 액세스할 수 있습니다. 예를 들어 SDK는 요청에 암호화 방식으로 서명(아래 참조), 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. 다운로드 및 설치 방법을 비롯하여 AWS SDK에 대한 자세한 내용은 Amazon Web Services용 도구 페이지를 참조하십시오.

Query API for IAM 및 AWS STS를 사용하면 서비스 작업을 호출할 수 있습니다. 쿼리 API 요청은 수행할 작업을 나타내기 위해 `Action` 파라미터를 포함해야 하는 HTTPS 요청입니다. IAM 및 AWS STS에서는 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. 이 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 IAM API Reference 또는 AWS Security Token Service API Reference의 개별 작업 페이지를 참조하십시오.

엔드포인트

IAM 및 AWS STS에는 전역적 엔드포인트가 하나씩 있습니다.

- (IAM) https://iam.amazonaws.com
- (AWS STS) https://sts.amazonaws.com

> **Note**
>
> AWS STS에서는 전역 엔드포인트 외에 리전 엔드포인트로 요청을 보내는 작업도 지원됩니다. 한 리전에서 AWS STS를 사용하려면 먼저 해당 리전에서 본인의 AWS 계정에 대해 STS를 활성화해야 합니다. AWS STS에 대해 추가 리전을 활성화하는 방법은 AWS 리전에서 AWS STS 관리 (p. 326) 단원을 참조하십시오.

모든 서비스용 AWS 엔드포인트 및 리전에 대한 자세한 내용은 AWS General Reference의 리전 및 엔드포인트를 참조하십시오.

HTTPS 필요

쿼리 API는 보안 자격 증명과 같이 민감한 정보를 반환하므로 모든 API 요청에 HTTPS를 사용해야 합니다.

IAM API 요청에 서명

액세스 키 ID와 보안 액세스 키를 사용하여 요청에 서명해야 합니다. IAM에서의 일상적인 작업에는 AWS 계정 루트 사용자 자격 증명을 사용하지 않는 것이 좋습니다. IAM 사용자용 자격 증명을 사용하거나 AWS STS를 사용하여 임시 보안 자격 증명을 생성할 수 있습니다.

API 요청에 서명하려면 AWS 서명 버전 4를 사용하는 것이 좋습니다. 서명 버전 4 사용에 대한 자세한 내용은 AWS 일반 참조의 서명 버전 4 서명 프로세스를 참조하십시오.

서명 버전 2를 사용해야 할 경우 서명 버전 2 사용에 대한 자세한 내용은 AWS 일반 참조를 참조하십시오.

자세한 내용은 다음 자료를 참조하십시오.

- AWS 보안 자격 증명. AWS 액세스에 사용되는 자격 증명 유형에 대한 일반적인 정보를 제공합니다.
- IAM 모범 사례 (p. 60)를 선택하십시오. IAM 서비스를 사용하여 AWS 리소스를 보호하기 위한 제안 사항의 목록을 제공합니다.
- 임시 보안 자격 증명 (p. 302)를 선택하십시오. 임시 보안 자격 증명을 만들고 사용하는 방법에 대해 설명합니다.

IAM 문서 기록

다음 표에서는 본 IAM 관련 주요 설명서 업데이트를 설명합니다.

update-history-change	update-history-description	update-history-date
AWS 로그인 페이지 업데이트	기본 AWS 로그인 페이지에서 로그인할 때 AWS 계정 루트 사용자 또는 IAM 사용자로 로그인하도록 선택할 수 없습니다. 이렇게 하면 페이지의 레이블에 루트 사용자 이메일 주소 또는 IAM 사용자 계정 정보를 제공해야 한다고 표시됩니다. 이 설명서에는 AWS 로그인 페이지를 이해하는 데 도움이 되는 업데이트된 화면 캡처가 포함되어 있습니다.	March 4, 2020
aws:ViaAWSService and aws:CalledVia 조건 키	이제 서비스가 IAM 보안 주체(사용자 또는 역할)를 대신하여 요청을 수행할 수 있는지 여부를 제한하는 정책을 작성할 수 있습니다. 보안 주체가 AWS 서비스에 요청을 하면 해당 서비스는 보안 주체의 자격 증명을 사용하여 다른 서비스에 대한 후속 요청을 수행할 수 있습니다. 서비스가 보안 주체의 자격 증명을 사용하여 요청을 하는 경우, `aws:ViaAWSService` 조건 키를 사용하여 일치시킵니다. 특정 서비스가 보안 주체의 자격 증명을 사용하여 요청하는 경우 `aws:CalledVia` 조건 키를 사용하여 일치시킵니다.	February 20, 2020
정책 시뮬레이터에서 권한 경계에 대한 지원 추가	이제 IAM 정책 시뮬레이터를 사용하여 IAM 엔터티에 대한 권한 경계의 효과를 테스트할 수 있습니다.	January 23, 2020
교차 계정 정책 평가	이제 AWS에서 교차 계정 액세스에 대한 정책을 평가하는 방법을 알아볼 수 있습니다. 교차 계정 액세스는 신뢰하는 계정의 리소스에 다른 계정의 보안 주체가 리소스에 액세스할 수 있도록 허용하는 리소스 기반 정책이 포함된 경우 발생합니다. 두 계정 모두에서 요청이 허용되어야 합니다.	January 2, 2020
세션 태그	이제 AWS STS에서 역할을 수임하거나 사용자를 연동할 때 태그를 포함할 수 있습니다. `AssumeRole` 또는	November 22, 2019

	`GetFederationToken` 작업을 수행할 때 세션 태그를 속성으로 전달할 수 있습니다. `AssumeRoleWithSAML` 또는 `AssumeRoleWithWebIdentity` 작업을 수행할 때 회사 자격 증명의 속성을 AWS로 전달할 수 있습니다.	
AWS Organizations의 AWS 계정 그룹에 대한 액세스 제어	이제 IAM 정책의 AWS Organizations에서 조직 단위(OU)를 참조할 수 있습니다. 조직를 사용하여 계정을 OU로 구성하는 경우 리소스에 대한 액세스 권한을 부여하기 전에 보안 주체가 특정 OU에 속하도록 요구할 수 있습니다. 보안 주체에는 AWS 계정 루트 사용자, IAM 사용자 및 IAM 역할이 포함됩니다. 이렇게 하려면 정책의 `aws:PrincipalOrgPaths` 조건 키에 OU 경로를 지정합니다.	November 20, 2019
마지막으로 사용된 역할	이제 역할이 마지막으로 사용된 날짜, 시간 및 리전을 볼 수 있습니다. 이 정보는 또한 계정에서 사용되지 않은 역할을 식별하는 데 도움이 됩니다. AWS Management 콘솔, AWS CLI 및 AWS API를 사용하여 역할이 마지막으로 사용된 시기에 대한 정보를 볼 수 있습니다.	November 19, 2019
전역 조건 컨텍스트 키 페이지로 업데이트	이제 각 전역 조건 키가 요청 컨텍스트에 포함되는 시기를 알 수 있습니다. 또한 페이지 TOC(목차)를 사용하여 각 키를 보다 쉽게 탐색할 수 있습니다. 이 페이지의 정보는 보다 정확한 정책을 작성하는 데 도움이 됩니다. 예를 들어 직원이 IAM 역할과의 연동을 사용하는 경우 `aws:userName` 키가 아닌 `aws:userId` 키를 사용해야 합니다. `aws:userName` 키는 IAM 사용자에게만 적용되며 역할에는 적용되지 않습니다.	October 6, 2019

AWS의 ABAC	태그를 사용하여 속성 기반 액세스 제어(ABAC)가 AWS에서 작동하는 방식 및 이러한 방식을 기존 AWS 권한 부여 모델과 비교하는 방식을 알아봅니다. ABAC 자습서를 사용하여 보안 주체 태그가 있는 IAM 역할이 태그가 일치하는 리소스에 액세스할 수 있도록 허용하는 정책을 생성하고 테스트하는 방법을 알아봅니다. 이 전략을 통해 개인이 자신의 작업에 필요한 AWS 리소스만 보거나 편집하도록 할 수 있습니다.	October 3, 2019
AWS STS GetAccessKeyInfo 작업	코드에서 AWS 액세스 키를 살펴보면 키가 자신의 계정에 속한 것인지 알 수 있습니다. 액세스 키 ID는 `aws sts get-access-key-info` AWS CLI 명령 또는 `GetAccessKeyInfo` AWS API 작업을 사용해 전달할 수 있습니다.	July 24, 2019
IAM에서 조직 서비스에서 마지막으로 액세스한 데이터 보기	IAM 콘솔의 AWS Organizations 섹션에서 서비스가 마지막으로 액세스한 AWS Organizations 엔터티 또는 정책용 데이터를 볼 수 있습니다. AWS CLI 또는 AWS API를 사용하여 데이터 보고서를 검색할 수도 있습니다. 이 데이터에는 조직 계정의 보안 주체가 마지막으로 액세스를 시도한 허용된 서비스와 그 시기에 대한 정보가 있습니다. 이 정보를 사용하여 불필요한 권한을 확인할 수 있으므로 조직 정책을 미세 조정함으로써 최소 권한의 원칙을 보다 잘 준수할 수 있습니다.	June 20, 2019
관리형 정책을 세션 정책으로 사용	역할을 수임할 때 최대 10개의 관리형 정책 ARN을 전달할 수 있습니다. 이를 통해 역할의 임시 자격 증명에 대한 권한을 제한할 수 있습니다.	May 7, 2019
전역 엔드포인트에 대한 세션 토큰의 AWS STS 리전 호환성	이제 전역 엔드포인트 토큰의 버전 1 또는 버전 2 사용 여부를 선택할 수 있습니다. 버전 1 토큰은 기본적으로 이용 가능한 AWS 리전에서만 유효합니다. 이러한 토큰은 아시아 태평양(홍콩)과 같이 수동으로 활성화된 리전에서 작동하지 않습니다. 버전 2는 모든 리전에서 유효합니다. 하지만 버전 2 토큰은 더 길고 일시적으로 토큰을 저장하는 시스템에 영향을 미칠 수 있습니다.	April 26, 2019

AWS 리전 활성화 및 비활성화 허용	이제 관리자가 아시아 태평양(홍콩) 리전(ap-east-1)을 활성화 및 비활성화할 수 있도록 허용하는 정책을 생성할 수 있습니다.	April 24, 2019
IAM 사용자 내 보안 자격 증명 페이지	이제 IAM 사용자는 My Security Credentials(내 보안 자격 증명) 페이지에서 자신의 모든 자격 증명을 관리할 수 있습니다. 이 AWS Management 콘솔 페이지에는 계정 ID 및 정식 사용자 ID와 같은 계정 정보가 표시됩니다. 또한 사용자는 자신의 암호, 액세스 키, X.509 인증서, SSH 키, Git 자격 증명을 보고 편집할 수 있습니다.	January 24, 2019
액세스 관리자 API	이제 AWS CLI 및 AWS API를 사용하여 서비스에서 마지막으로 액세스한 데이터를 볼 수 있습니다.	December 7, 2018
IAM 사용자 및 역할 태그 지정	이제 IAM 태그를 사용하여 태그 키-값 페어를 통해 사용자 지정 속성을 자격 증명(IAM 사용자 또는 역할)에 추가할 수 있습니다. 태그를 사용하여 리소스에 대한 자격 증명의 액세스를 제어하거나 자격 증명에 연결할 수 있는 태그를 제어할 수도 있습니다.	November 14, 2018
U2F 보안 키	이제 AWS Management 콘솔에 로그인할 때 멀티 팩터 인증(MFA) 옵션으로 U2F 보안 키를 사용할 수 있습니다.	September 25, 2018
Amazon VPC 엔드포인트에 대한 지원	이제 미국 서부(오레곤) 리전에서 VPC와 AWS STS 간에 프라이빗 연결을 설정할 수 있습니다.	July 31, 2018
권한 경계	새 기능을 사용하면 IAM 권한을 관리할 수 있는 권한을 신뢰할 수 있는 직원에게 부여하는 작업이 더 간편해질 뿐 아니라 IAM 관리자 액세스 권한 전체를 부여하지 않아도 됩니다.	July 12, 2018
aws:PrincipalOrgID	새로운 조건 키는 IAM 보안 주체의 AWS 조직을 지정하여 AWS 리소스로의 액세스를 제어하는 쉬운 방법을 제공합니다.	May 17, 2018
aws:RequestedRegion	새로운 조건 키는 IAM 정책을 사용하여 AWS 리전으로의 액세스를 제어하는 쉬운 방법을 제공합니다.	April 25, 2018
IAM 역할에 대한 섹션 기간 증가	이제 IAM 역할은 12시간의 세션 기간을 가질 수 있습니다.	March 28, 2018

역할 생성된 워크플로우 업데이트	새로운 워크플로우는 신뢰 관계를 생성하고 권한을 역할에 연결하는 과정을 개선합니다.	September 8, 2017
AWS 계정 로그인 절차	AWS 로그인 경험을 업데이트 하여 루트 사용자와 IAM 사용자 모두가 AWS Management 콘솔 콘솔 홈페이지의 Sign In to the Console(콘솔로 로그인) 링크를 사용할 수 있도록 허용합니다.	August 25, 2017
IAM 정책 예제	30 가지의 예제 정책이 넘는 설명서 업데이트 기능.	August 2, 2017
IAM 모범 사례	IAM 콘솔의 사용자 섹션에 추가된 정보는 IAM 모범 사례를 쉽게 따라할 수 있게 만듭니다.	July 5, 2017
Auto Scaling 리소스	리소스 수준 권한은 Auto Scaling 리소스로의 액세스 및 권한을 제어할 수 있습니다.	May 16, 2017
MySQL 및 Amazon Aurora 데이터베이스를 위한 Amazon RDS	데이터베이스 관리자는 데이터베이스 사용자를 IAM 사용자 및 역할과 연관시킬 수 있어 사용자가 단일 위치에서 모든 AWS 리소스로의 사용자 액세스를 관리할 수 있습니다.	April 24, 2017
서비스 연결 역할	서비스 링크된 역할은 AWS 서비스로 권한을 위임하는 더욱 쉽고 보안한 방법을 제공합니다.	April 19, 2017
정책 요약	새로운 정책 요약을 통해 IAM 정책의 권한을 더욱 손쉽게 이해할 수 있습니다.	March 23, 2017

AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the AWS General Reference.