사용자 가이드

AWS Resource Access Manager

AWS Resource Access Manager: 사용자 가이드

Table of Contents

AWS Resource Access Manager란 무엇인가요?

AWS Resource Access Manager(AWS RAM)를 사용하면 지원되는 리소스 유형에 대해 AWS 계정 간, 조직 또는 조직 단위(OU) 내에서, 그리고 AWS Identity and Access Management(IAM) 역할 및 사용자와 리소스를 안전하게 공유할 수 있습니다. AWS 계정이 여러 개 있는 경우 리소스를 한 번 생성한 후 AWS RAM을 사용하여 다른 계정에서 해당 리소스를 사용할 수 있도록 설정할 수 있습니다. AWS Organizations에서 관리하는 계정인 경우, 조직의 다른 모든 계정과 리소스를 공유하거나 하나 이상의 지정된 조직 단위(OU)에 포함된 계정과만 리소스를 공유할 수 있습니다. 계정이 조직에 속해 있는지 여부와 관계없이 계정 ID로 특정 AWS 계정과 공유할 수도 있습니다. 지원되는 일부 리소스 유형은 지정된 IAM 역할 및 사용자와 공유할 수도 있습니다.

목차

동영상 개요

다음 동영상에서는 AWS RAM에 대한 간략한 소개와 리소스 공유를 생성하는 방법을 제공합니다. 자세한 내용은 ??? 섹션을 참조하세요.

다음 동영상에서는 AWS 관리형 권한을 AWS 리소스에 적용하는 방법을 보여줍니다. 자세한 내용은 ??? 섹션을 참조하세요.

이 동영상에서는 최소 권한 모범 사례에 따라 고객 관리형 권한을 작성하고 연결하는 방법을 보여줍니다. 자세한 내용은 ??? 섹션을 참조하세요.

AWS RAM의 이점

AWS RAM을 사용하는 이유는 무엇입니까? 다음과 같은 이점을 제공합니다.

- 운영 오버헤드 감소 - 리소스를 한 번 생성한 다음 AWS RAM을 사용하여 다른 계정과 해당 리소스를 공유할 수 있습니다. 그러면 모든 계정에서 중복된 리소스를 프로비저닝할 필요가 없으므로 운영 오버헤드가 줄어듭니다. 리소스를 소유한 계정 내에서 AWS RAM을 사용하면 자격 증명 기반 권한 정책을 사용하지 않고도 해당 계정의 모든 역할과 사용자에게 간편하게 액세스 권한을 부여할 수 있습니다.
- 보안 및 일관성 제공 - 하나의 정책 및 권한 세트를 사용하여 공유 리소스에 대한 보안 관리를 간소화할 수 있습니다. 모든 개별 계정에 중복 리소스를 생성한다면 동일한 정책과 권한을 구현한 다음 모든 계정에서 동일하게 유지해야 하는 작업이 필요합니다. 대신, AWS RAM 리소스 공유의 모든 사용자는 하나의 정책 및 권한 집합으로 관리됩니다. AWS RAM은 다양한 유형의 AWS 리소스를 공유하기 위한 일관된 환경을 제공합니다.
- 가시성 및 감사 기능 제공 - AWS RAM과 Amazon CloudWatch 및 AWS CloudTrail의 통합을 통해 공유 리소스에 대한 사용량 세부 정보를 확인할 수 있습니다. AWS RAM은 공유 리소스 및 계정에 대한 포괄적인 가시성을 제공합니다.

리소스 기반 정책을 사용한 크로스 계정 액세스

AWS 계정 외부의 AWS Identity and Access Management (IAM) 보안 주체(IAM 역할 및 사용자)를 식별하는 리소스 기반 정책을 연결하여 일부 유형의 AWS 리소스를 다른 AWS 계정과 공유할 수 있습니다. 그러나 정책을 연결하여 리소스를 공유하면 AWS RAM에서 제공하는 추가적인 이점을 활용할 수 없습니다. AWS RAM을 사용하면 다음과 같은 기능을 이용할 수 있습니다.

- 모든 AWS 계정 ID를 열거할 필요 없이 조직 또는 조직 단위(OU)와 공유할 수 있습니다.
- 사용자는 마치 해당 리소스가 사용자 계정에 직접 있는 것처럼 원래 AWS 서비스 콘솔 및 API 작업에서 직접 공유된 리소스를 볼 수 있습니다. 예를 들어 AWS RAM을 사용하여 다른 계정과 Amazon VPC 서브넷을 공유하는 경우 해당 계정의 사용자는 해당 계정에서 수행된 Amazon VPC API 작업의 결과와 Amazon VPC 콘솔에서 해당 서브넷을 볼 수 있습니다. 리소스 기반 정책을 연결하여 공유한 리소스는 이러한 방식으로 표시되지 않으며, 대신 해당 Amazon 리소스 이름(ARN)으로 리소스를 검색하고 명시적으로 참조해야 합니다.
- 리소스 소유자는 자신이 공유한 각 개별 리소스에 액세스할 수 있는 보안 주체를 확인할 수 있습니다.
- 조직에 속하지 않은 계정과 리소스를 공유하는 경우 AWS RAM에서 초대 프로세스를 시작합니다. 수신자가 초대를 수락해야 보안 주체가 공유 리소스에 액세스할 수 있습니다. 조직 내 공유 기능을 활성화하면 조직 내 계정과 공유할 때 초대가 필요하지 않습니다.

리소스 기반 권한 정책을 사용하여 공유한 리소스가 있는 경우 다음 중 하나를 수행하여 해당 리소스를 완전 관리형 AWS RAM 리소스로 승격할 수 있습니다.

- PromoteResourceShareCreatedFromPolicy API 작업을 사용합니다.
- API 작업과 동등한 작업을 사용합니다. 즉, AWS Command Line Interface(AWS CLI) promote-resource-share-created-from-policy 명령을 사용합니다.

리소스 공유 작동 방식

소유 계정의 리소스를 다른 AWS 계정인 소비 계정과 공유하면 소비 계정의 보안 주체에게 공유 리소스에 대한 액세스 권한이 부여됩니다. 소비 계정의 역할 및 사용자에게 적용되는 모든 정책 및 권한이 공유 리소스에도 적용됩니다. 공유 리소스는 공유하고 있는 AWS 계정의 기본 리소스처럼 보입니다.

글로벌 리소스와 리전 리소스를 모두 공유할 수 있습니다. 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.

리소스 공유

AWS RAM을 사용하면 리소스 공유를 생성하여 소유한 리소스를 공유할 수 있습니다. 리소스 공유를 생성하려면 다음을 지정합니다.

- 리소스 공유를 생성할 AWS 리전. 콘솔의 오른쪽 상단 모서리에 있는 리전 드롭다운 메뉴에서 리전을 선택합니다. AWS CLI에서는 `--region` 파라미터를 사용합니다.
  - 리소스 공유에는 리소스 공유와 동일한 AWS 리전에 있는 리전 리소스만 포함될 수 있습니다.
  - 리소스 공유가 글로벌 리소스의 지정된 홈 리전인 미국 동부(버지니아 북부), `us-east-1`에 있는 경우에만 리소스 공유에 글로벌 리소스가 포함될 수 있습니다.
- 리소스 공유의 이름
- 이 리소스 공유의 일부로 액세스 권한을 부여하려는 리소스 목록
- 리소스 공유에 대한 액세스 권한을 부여할 보안 주체. 주체는 개별 AWS 계정, AWS Organizations에 있는 조직 또는 OU(조직 구성 단위)의 계정, 개별 AWS Identity and Access Management(IAM) 역할 또는 사용자일 수 있습니다.

> **Note**
>
> 모든 리소스 유형을 IAM 역할 및 사용자와 공유할 수 있는 것은 아닙니다. 이러한 보안 주체와 공유할 수 있는 리소스에 대한 자세한 내용은 공유 가능한 리소스 AWS 섹션을 참조하세요.

- 리소스 공유에 포함된 각 리소스 유형과 연결할 관리형 권한. 관리형 권한에 따라 다른 계정의 주체가 리소스 공유에 있는 리소스로 수행할 수 있는 작업이 결정됩니다.

  권한의 동작은 보안 주체 유형에 따라 다릅니다.

  - 보안 주체가 리소스를 소유한 계정과 다른 계정에 있는 경우 리소스 공유에 연결된 권한이 해당 계정의 역할 및 사용자에게 부여할 수 있는 최대 권한입니다. 그런 다음 해당 계정의 관리자는 IAM 자격 증명 기반 정책을 사용하여 공유 리소스에 대한 액세스 권한을 개별 역할 및 사용자에게 부여해야 합니다. 이러한 정책에서 부여되는 권한은 리소스 공유에 연결된 권한에 정의된 권한을 초과할 수 없습니다.

리소스 소유 계정은 공유하는 리소스에 대한 전체 소유권을 보유합니다.

공유 리소스 사용

리소스 소유자가 내 계정과 리소스를 공유하면 내 계정이 리소스를 소유한 것처럼 공유 리소스에 액세스할 수 있습니다. 관련 서비스의 콘솔, AWS CLI 명령, API 작업을 사용하여 리소스에 액세스할 수 있습니다. 계정의 보안 주체가 수행할 수 있는 API 작업은 리소스 유형에 따라 다르며, 리소스 공유에 연결된 AWS RAM 권한으로 지정됩니다. 계정에 구성된 모든 IAM 정책 및 서비스 제어 정책도 계속 적용되므로 보안 및 거버넌스 제어에 대한 기존 투자를 활용할 수 있습니다.

해당 리소스의 서비스를 사용하여 공유 리소스에 액세스하면 리소스를 소유한 AWS 계정과 동일한 권한 및 제한 사항이 적용됩니다.

- 리전 리소스인 경우, 소유 계정의 리소스가 있는 AWS 리전에서만 액세스할 수 있습니다.
- 글로벌 리소스인 경우, 리소스의 서비스 콘솔 및 도구가 지원하는 모든 AWS 리전에서 리소스에 액세스할 수 있습니다. 리소스 공유 및 글로벌 리소스는 지정된 홈 리전인 미국 동부(버지니아 북부), `us-east-1`에서만 AWS RAM 콘솔 및 도구에서 보고 관리할 수 있습니다.

AWS RAM 액세스

다음 방법 중 하나를 사용하여 AWS RAM에서 작업할 수 있습니다.

AWS RAM 콘솔

AWS RAM는 웹 기반 사용자 인터페이스인 AWS RAM 콘솔을 제공합니다. AWS 계정에 가입한 고객은 AWS Management Console에 로그인한 후 콘솔 홈 페이지에서 AWS RAM을 선택하면 AWS RAM 콘솔에 액세스할 수 있습니다.

브라우저에서 직접 AWS RAM 콘솔로 이동할 수도 있습니다. 아직 로그인하지 않은 경우 콘솔이 표시되기 전에 로그인하라는 메시지가 표시됩니다.

AWS CLI 및 Windows PowerShell용 도구

AWS CLI 및 AWS Tools for PowerShell는 AWS RAM 퍼블릭 API 작업에 대한 직접 액세스를 제공합니다. AWS는 Windows, macOS, Linux에서 이러한 도구를 지원합니다. 시작하기에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서 또는 AWS Tools for Windows PowerShell 사용 설명서를 참조하세요. AWS RAM 명령에 대한 자세한 내용은 AWS CLI 명령 참조 또는 AWS Tools for Windows PowerShell Cmdlet 참조를 참조하세요.

AWS SDK

AWS는 광범위한 프로그래밍 언어 세트에 대한 API 명령을 제공합니다. 시작하기에 대한 자세한 내용은 AWS SDK 및 도구 참조 안내서를 참조하세요.

Query API

지원되는 프로그래밍 언어 중 하나를 사용하지 않는 경우 AWS RAM HTTPS Query API를 사용하여 AWS RAM 및 AWS에 프로그래밍 방식으로 액세스할 수 있습니다. AWS RAM API를 사용하면 서비스에 직접 HTTPS 요청을 발행할 수 있습니다. AWS RAM API를 사용할 때는 자격 증명을 사용하여 요청에 디지털 방식으로 서명하는 코드를 포함해야 합니다. 자세한 내용은 AWS RAM API 참조를 참조하세요.

AWS RAM 요금

AWS RAM을 사용하거나 리소스 공유를 생성하고 계정 간에 리소스를 공유하는 데는 추가 요금이 부과되지 않습니다. 리소스 사용 요금은 리소스 유형에 따라 다릅니다. AWS에서 공유 가능한 리소스에 요금을 청구하는 방법에 대한 자세한 내용은 리소스 소유 서비스의 설명서를 참조하세요.

규정 준수 및 국제 표준

PCI DSS

AWS RAM에서는 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 참조하세요.

FedRAMP

미국 동부(버지니아 북부), 미국 동부(오하이오), 미국 서부(캘리포니아 북부), 미국 서부(오레곤) AWS 리전에서는 AWS RAM이 FedRAMP Moderate로 승인되었습니다.

AWS GovCloud(미국 서부) 및AWS GovCloud (미국 동부) AWS 리전에서는 AWS RAM이 FedRAMP High로 승인되었습니다.

연방정부 위험 및 권한 부여 관리 프로그램(FedRAMP)은 클라우드 제품 및 서비스의 보안 평가, 권한 부여 및 지속적인 모니터링에 대한 표준 접근 방식을 제공하는 정부 차원의 프로그램입니다.

FedRAMP 규정 준수에 대한 자세한 내용은 FedRAMP을 참조하세요.

SOC 및 ISO

AWS RAM은 SOC(Service Organization Controls) 규정 준수 및 ISO(International Organization for Standardization)의 ISO 9001, ISO 27001, ISO 27017, ISO 27018, ISO 27701 표준의 적용을 받는 워크로드에 사용할 수 있습니다. 금융, 의료 및 기타 규제 대상 부문의 고객은 고객 데이터를 보호하는 보안 프로세스 및 제어에 대한 인사이트를 얻을 수 있으며, 이 인사이트는 SOC 보고서와 AWS ISO 및 CSA STAR 인증서를 통해 AWS Artifact에서 확인할 수 있습니다.

SOC 규정 준수에 대한 자세한 내용은 SOC 섹션을 참조하세요.

ISO 규정 준수에 대한 자세한 내용은 ISO 9001, ISO 27001, ISO 27017, ISO 27018, ISO 27701을 참조하세요.

AWS RAM 시작하기

AWS Resource Access Manager를 사용하면 소유한 리소스를 개별 AWS 계정과 공유할 수 있습니다. 계정을 AWS Organizations에서 관리하는 경우 조직의 다른 계정과 리소스를 공유할 수도 있습니다. 다른 AWS 계정으로부터 공유 받은 리소스를 사용할 수도 있습니다.

AWS Organizations과의 공유를 활성화하지 않은 경우 조직 또는 조직의 조직 단위(OU)와 리소스를 공유할 수 없습니다. 하지만 조직의 개별 AWS 계정과는 계속 리소스를 공유할 수 있습니다. 지원되는 리소스 유형의 경우 조직의 개별 AWS Identity and Access Management(IAM) 역할 또는 사용자와 리소스를 공유할 수도 있습니다. 이 경우 이러한 보안 주체는 조직의 일부가 아닌 외부 계정처럼 취급됩니다. 리소스 공유에 참여하라는 초대를 받게 되고 초대를 수락해야 공유 리소스에 액세스할 수 있습니다.

목차

AWS RAM 용어 및 개념

다음 개념은 AWS Resource Access Manager(AWS RAM)를 사용하여 리소스를 공유하는 방법을 설명하는 데 도움이 됩니다.

리소스 공유

AWS RAM을 사용하여 리소스를 공유하려면 리소스 공유를 생성해야 합니다. 리소스 공유의 세 가지 요소는 다음과 같습니다.

- 공유할 하나 이상의 AWS 리소스 목록
- 리소스 액세스 권한이 부여된 하나 이상의 보안 주체 목록
- 공유에 포함될 각 리소스 유형에 대한 관리형 권한. 각 관리형 권한은 해당 리소스 공유에 있는 해당 유형의 모든 리소스에 적용됩니다.

AWS RAM을 사용하여 리소스 공유를 생성한 후에는 리소스 공유에 지정된 보안 주체에게 공유 리소스에 대한 액세스 권한을 부여할 수 있습니다.

- AWS RAM과 AWS Organizations와의 공유가 활성화되어 있고 공유 대상 보안 주체가 공유 계정과 같은 조직에 속해 있는 경우 계정 관리자가 AWS Identity and Access Management(IAM) 권한 정책을 사용하여 리소스 사용 권한을 부여하는 즉시 해당 보안 주체는 액세스 권한을 부여받을 수 있습니다.
- AWS RAM과 Organizations와의 공유를 활성화하지 않은 경우에도 조직 내 개별 AWS 계정과는 리소스를 공유할 수 있습니다. 소비 계정의 관리자는 리소스 공유에 참여하라는 초대를 받게 되며, 초대를 수락해야 리소스 공유에 지정된 주체가 공유 리소스에 액세스할 수 있습니다.
- 리소스 유형에서 지원하는 경우 조직 외부 계정과 공유할 수도 있습니다. 소비 계정의 관리자는 리소스 공유에 참여하라는 초대를 받게 되며, 초대를 수락해야 리소스 공유에 지정된 주체가 공유 리소스에 액세스할 수 있습니다. 이 유형의 공유를 지원하는 리소스 유형에 대한 자세한 내용은 공유 가능한 리소스 AWS에서 조직 외부 계정과 공유 가능 열을 참조하세요.

공유 계정

공유 계정은 공유되는 리소스를 포함하고 있으며, AWS RAM 관리자가 AWS RAM을 사용하여 AWS 리소스 공유를 생성할 때 사용됩니다.

AWS RAM 관리자는 AWS 계정에서 리소스 공유를 생성하고 구성할 권한이 있는 IAM 보안 주체입니다. AWS RAM은 리소스 기반 정책을 리소스 공유의 리소스에 연결하는 방식으로 작동하므로 AWS RAM 관리자는 리소스 공유에 포함된 각 리소스 유형에 대해 AWS 서비스의 `PutResourcePolicy` 작업을 호출할 수 있는 권한도 갖고 있어야 합니다.

소비 보안 주체

소비 계정은 리소스가 공유되는 AWS 계정입니다. 리소스 공유에는 계정 전체를 보안 주체로 지정하거나, 일부 리소스 유형의 경우 계정의 개별 역할 또는 사용자를 주체로 지정할 수 있습니다. 이 유형의 공유를 지원하는 리소스 유형에 대한 자세한 내용은 공유 가능한 리소스 AWS에서 IAM 역할 및 사용자와 공유 가능 열을 참조하세요.

AWS RAM은 또한 리소스 공유의 소비자로 서비스 보안 주체도 지원합니다. 이 유형의 공유를 지원하는 리소스 유형에 대한 자세한 내용은 공유 가능한 리소스 AWS에서 서비스 보안 주체와 공유 가능 열을 참조하세요.

소비 계정의 보안 주체는 다음 권한이 모두 허용하는 작업만 수행할 수 있습니다.

- 리소스 공유에 연결된 관리형 권한. 이 권한은 소비 계정의 보안 주체에게 부여할 수 있는 최대 권한을 지정합니다.

- 소비 계정의 IAM 관리자가 개별 역할 또는 사용자에게 연결하는 IAM 자격 증명 기반 정책. 이 정책은 공유 계정 내 리소스의 Amazon 리소스 이름(ARN)및 지정된 작업에 대한 `Allow` 액세스 권한을 부여해야 합니다.

AWS RAM은 다음과 같은 IAM 보안 주체 유형을 리소스 공유의 소비자로 지원합니다.

- 다른 AWS 계정 - 리소스 공유를 통해 공유 계정에 포함된 리소스를 소비 계정에서 사용할 수 있습니다.
- 개별 IAM 역할 또는 다른 계정의 사용자 - 일부 리소스 유형의 경우 개별 IAM 역할 또는 사용자와 직접 공유하는 것을 지원합니다. 이 보안 주체 유형은 해당 ARN으로 지정합니다.
  - IAM 역할 – `arn:aws:iam::123456789012:role/rolename`
  - IAM 사용자 – `arn:aws:iam::123456789012:user/username`
- 서비스 보안 주체 - AWS 서비스와 리소스를 공유하여 서비스에 리소스 공유에 대한 액세스 권한을 부여합니다. 서비스 보안 주체 공유를 사용하면 AWS 서비스가 사용자를 대신해 작업을 수행하여 운영 부담을 덜어줍니다.

  서비스 보안 주체와 공유하려면 누구에게나 공유를 허용하도록 선택한 다음 보안 주체 유형 선택에서 드롭다운 목록에서 서비스 보안 주체를 선택합니다. 서비스 보안 주체의 이름은 다음 형식으로 지정합니다.

  - *`service-id`*`.amazonaws.com`

  혼동된 대리인 위험을 줄이기 위해 리소스 정책은 `aws:SourceAccount` 조건 키에 리소스 소유자의 계정 ID를 표시합니다.
- 조직 내 계정 - 공유 계정을 AWS Organizations에서 관리하는 경우 리소스 공유에는 조직의 모든 계정과 공유할 조직의 ID를 지정할 수 있습니다. 리소스 공유에는 해당 조직 단위(OU)의 모든 계정과 공유할 OU ID를 지정할 수도 있습니다. 공유 계정은 자체 조직 또는 자체 조직 내의 OU ID와만 공유할 수 있습니다. 조직 내 계정은 조직 또는 OU의 ARN으로 지정합니다.
  - 조직의 모든 계정 - 다음은 AWS Organizations 조직의 ARN 예시입니다.

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>
    ```
  - 조직 단위의 모든 계정 - 다음은 OU ID의 ARN 예시입니다.

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>/ou-<rootid>-<ouid>
    ```

> **Important**
>
> 조직 또는 OU와 공유할 때 해당 범위에 리소스 공유를 소유한 계정이 포함되어 있으면 공유 계정의 모든 주체가 자동으로 공유의 리소스에 대한 액세스 권한을 얻게 됩니다. 부여된 액세스 권한은 공유와 연결된 관리형 권한에 의해 정의됩니다. 이는 AWS RAM에서 공유의 각 리소스에 연결한 리소스 기반 정책이 `"Principal": "*"`을 사용하기 때문입니다. 자세한 내용은 리소스 기반 정책에서 "Principal": "*" 사용 시 유의 사항 섹션을 참조하세요.
> 다른 소비 계정의 보안 주체는 공유 리소스에 즉시 액세스할 수 없습니다. 다른 계정의 관리자가 먼저 자격 증명 기반 권한 정책을 해당 보안 주체에 연결해야 합니다. 이러한 정책은 리소스 공유에 있는 개별 리소스의 ARN에 `Allow` 액세스 권한을 부여해야 합니다. 이러한 정책의 권한은 리소스 공유와 연결된 관리형 권한에 지정된 권한을 초과할 수 없습니다.

리소스 기반 정책

리소스 기반 정책은 IAM 정책 언어를 구현하는 JSON 텍스트 문서입니다. IAM 역할 또는 사용자와 같은 보안 주체에 연결하는 자격 증명 기반 정책과 달리 리소스 기반 정책은 리소스에 연결합니다. AWS RAM은 리소스 공유에 대해 사용자가 제공한 정보를 기반으로 사용자를 대신하여 리소스 기반 정책을 작성합니다. 리소스에 액세스할 수 있는 사용자를 결정하는 `Principal` 정책 요소를 지정해야 합니다. 자세한 내용은 IAM 사용 설명서에서 자격 증명 기반 정책 및 리소스 기반 정책을 참조하세요.

AWS RAM에서 생성하는 리소스 기반 정책은 다른 모든 IAM 정책 유형과 함께 평가됩니다. 여기에는 리소스에 액세스하려는 보안 주체에 연결된 모든 IAM 자격 증명 기반 정책과 AWS 계정에 적용할 수 있는AWS Organizations의 서비스 제어 정책(SCP)이 포함됩니다. AWS RAM에서 생성하는 리소스 기반 정책은 다른 모든 IAM 정책과 동일한 정책 평가 로직에 참여합니다. 정책 평가에 대한 자세한 내용과 그에 따른 권한을 결정하는 방법은 IAM 사용 설명서에서 정책 평가 로직을 참조하세요.

AWS RAM은 사용하기 쉬운 추상화 리소스 기반 정책을 제공하여 간단하고 안전한 리소스 공유 환경을 제공합니다.

리소스 기반 정책을 지원하는 리소스 유형의 경우 AWS RAM에서 자동으로 리소스 기반 정책을 구성하고 관리합니다. 지정된 리소스에 대해 AWS RAM은 해당 리소스를 포함하는 모든 리소스 공유의 정보를 결합하여 리소스 기반 정책을 구축합니다. 예를 들어, AWS RAM을 사용하여 공유하는 Amazon SageMaker 파이프라인을 두 개의 서로 다른 리소스 공유에 포함시킨다고 가정해 보겠습니다. 하나의 리소스 공유로 전체 조직에 읽기 전용 액세스 권한을 제공하고, 다른 리소스 공유로 단일 계정에 SageMaker 실행 권한만 부여할 수 있습니다. AWS RAM에서는 이러한 두 개의 권한을 여러 명령문이 있는 단일 리소스 정책으로 자동 결합합니다. 그런 다음 결합된 리소스 기반 정책을 파이프라인 리소스

에 연결합니다. 이 기본 리소스 정책은 GetResourcePolicy 작업을 호출하여 확인할 수 있습니다. 그런 다음 AWS 서비스는 해당 리소스 기반 정책을 사용하여 공유 리소스에 대해 작업을 수행하려는 모든 보안 주체에 권한을 부여합니다.

리소스 기반 정책을 수동으로 생성하고 `PutResourcePolicy`를 호출하여 리소스에 연결할 수도 있지만, 다음과 같은 이점이 있으므로 AWS RAM을 사용하는 것이 좋습니다.

- 공유 소비자를 위한 검색 가능성 - AWS RAM을 사용하여 리소스를 공유할 경우 사용자는 공유 받은 모든 리소스를 리소스 소유 서비스의 콘솔 및 API 작업에서 마치 해당 리소스가 사용자 계정에 직접 있는 것처럼 볼 수 있습니다. 예를 들어 AWS CodeBuild 프로젝트를 다른 계정과 공유하는 경우 소비 계정의 사용자는 CodeBuild 콘솔과 수행된 CodeBuild API 작업의 결과에서 프로젝트를 볼 수 있습니다. 리소스 기반 정책을 직접 연결하여 공유한 리소스는 이런 방식으로 보이지 않습니다. 대신 ARN으로 리소스를 검색하고 명시적으로 참조해야 합니다.
- 공유 소유자를 위한 관리 효율성 - AWS RAM을 사용하여 리소스를 공유할 경우 공유 계정의 리소스 소유자는 자신의 리소스에 액세스할 수 있는 다른 계정을 중앙에서 확인할 수 있습니다. 리소스 기반 정책을 사용하여 리소스를 공유할 경우 관련 서비스 콘솔 또는 API에서 개별 리소스에 대한 정책을 검토해야만 소비 계정을 확인할 수 있습니다.
- 효율성 - AWS RAM을 사용하여 리소스를 공유할 경우 여러 리소스를 공유하고 하나의 단위로 관리할 수 있습니다. 리소스 기반 정책만 사용하여 리소스를 공유하려면 공유하는 모든 리소스에 개별 정책을 연결해야 합니다.
- 단순성 - AWS RAM을 사용할 경우 JSON 기반 IAM 정책 언어를 이해하지 않아도 됩니다. AWS RAM은 즉시 사용 가능한 AWS 관리형 권한을 제공하는데, 이 권한 중에서 선택하여 리소스 공유에 연결할 수 있습니다.

AWS RAM을 사용하면 리소스 기반 정책을 아직 지원하지 않는 일부 리소스 유형을 공유할 수도 있습니다. 이러한 리소스 유형의 경우 AWS RAM에서 실제 권한을 나타내는 리소스 기반 정책을 자동으로 생성합니다. 사용자는 GetResourcePolicy를 호출하여 이 표현을 확인할 수 있습니다. 여기에는 다음과 같은 리소스 유형이 포함됩니다.

- Amazon Aurora – DB 클러스터
- Amazon EC2 – 용량 예약 및 전용 호스트
- AWS License Manager – 라이선스 구성
- AWS Outposts – 로컬 게이트웨이 라우팅 테이블, outposts, 사이트
- Amazon Route 53 – 전달 규칙
- Amazon Virtual Private Cloud - 고객 소유 IPv4 주소, 접두사 목록, 서브넷, 트래픽 미러 대상, 전송 게이트웨이, 전송 게이트웨이 멀티캐스트 도메인

AWS RAM에서 생성한 리소스 기반 정책의 예

EC2 Image Builder 이미지 리소스를 개별 AWS RAM 계정과 공유하는 경우 은 다음 예와 같은 정책을 생성하여 리소스 공유에 포함된 이미지 리소스에 연결합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
        }
    ]
}
```

EC2 Image Builder 이미지 리소스를 다른 AWS 계정의 IAM 역할 또는 사용자와 공유하는 경우, AWS RAM은 다음 예와 같은 정책을 생성하여 리소스 공유에 포함된 이미지 리소스에 연결합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/MySampleRole"
      },
      "Action": [
          "imagebuilder:GetImage",
          "imagebuilder:ListImages",
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
    }
  ]
}
```

EC2 Image Builder 이미지 리소스를 조직의 모든 계정 또는 OU 계정과 공유하는 경우, AWS RAM은 다음 예와 같은 정책을 생성하여 리소스 공유에 포함된 이미지 리소스에 연결합니다.

> **Note**
>
> 이 정책은 `"Principal": "*"`를 사용한 다음 `"Condition"` 요소를 사용하여 지정된 `PrincipalOrgID`와 일치하는 ID로 권한을 제한합니다. 자세한 내용은 리소스 기반 정책에서 "Principal": "*" 사용 시 유의 사항 섹션을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-123456789"
                }
            }
        }
    ]
}
```

리소스 기반 정책에서 "Principal": "*" 사용 시 유의 사항

리소스 기반 정책에 `"Principal": "*"`를 포함시키면 이 정책은 해당 리소스를 포함하는 계정의 모든 IAM 주체에 액세스 권한을 부여합니다. 단, `Condition` 요소가 있는 경우 그에 따른 제한이 적용됩니다. 호출 보안 주체에 적용되는 모든 정책의 명시적 `Deny` 문은 이 정책에서 부여한 권한보다 우선합니다. 그러나 해당 자격 증명 정책, 권한 경계 정책 또는 세션 정책에 암시적 `Deny`(명시적 `Allow`가 없음을 의미함)가 있을 경우 해당 리소스 기반 정책에 따라 작업에 액세스 권한이 부여된 주체에는 `Deny`가 적용되지 않습니다.

이것이 원하는 동작이 아닌 경우 관련 역할 및 사용자에게 영향을 주는 자격 증명 정책, 권한 경계, 또는 세션 정책에 명시적 Deny 문을 추가하여 이 동작을 제한할 수 있습니다.

관리형 권한

관리형 권한은 리소스 공유에서 지원되는 리소스 유형에 대해 관리자가 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 공유를 생성할 때는 리소스 공유에 포함된 각 리소스 유형에 사용할 관리형 권한을 지정해야 합니다. 관리형 권한은 AWS RAM을 사용하여 공유되는 리소스에 대해 보안 주체가 수행할 수 있는 actions 및 조건 세트를 나열합니다.

리소스 공유의 리소스 유형당 하나의 관리형 권한만 연결할 수 있습니다. 특정 유형의 일부 리소스는 하나의 관리형 권한을 사용하고 같은 유형의 다른 리소스는 다른 관리형 권한을 사용하는 리소스 공유는 생성할 수 없습니다. 이렇게 하려면 서로 다른 두 개의 리소스 공유를 생성하고 두 공유에 리소스를 분할하여 각 세트서로 다른 관리형 권한을 부여해야 합니다. 관리형 권한에는 두 가지 유형이 있습니다.

AWS 관리형 권한

AWS 관리형 권한은 AWS에서 생성 및 유지 관리하며 일반적인 고객 시나리오에 대한 권한을 부여합니다. AWS RAM은 지원되는 모든 리소스 유형에 대해 하나 이상의 AWS 관리형 권한을 정의합니다. 일부 리소스 유형의 경우 둘 이상의 AWS 관리형 권한을 지원하며, 이때 하나의 관리형 권한이 AWS 기본값으로 지정됩니다. 달리 지정하지 않는 한 기본 AWS 관리형 권한이 연결됩니다.

고객 관리형 권한

고객 관리형 권한은 AWS RAM을 사용하여 공유되는 리소스에 대해 어떤 조건에서 어떤 작업을 수행할 수 있는지 정확하게 지정하여 작성하고 유지 관리하는 관리형 권한입니다. 예를 들어, 대규모로 IP 주소를 관리하는 데 도움이 되도록 Amazon VPC IP 주소 관리자(IPAM) 풀에 대한 읽기 액세스를 제한하려고 합니다. 개발자가 IP 주소를 할당할 수 있는 고객 관리형 권한을 생성할 수 있지만, 다른 개발자 계정이 할당하는 IP 주소 범위를 볼 수는 없습니다. 최소 권한 모범 사례에 따라 공유 리소스에 대한 작업을 수행하는 데 필요한 권한만 부여할 수 있습니다.

리소스 공유에서 리소스 유형에 대한 자체 권한을 정의하고, 글로벌 컨텍스트 키 및 서비스별 키와 같은 조건을 추가하여 보안 주체가 리소스에 액세스할 수 있는 조건을 지정할 수 있습니다. 이러한 권한은 하나 이상의 AWS RAM 공유에서 사용할 수 있습니다. 고객 관리형 권한은 리전별로 적용됩니다.

AWS RAM은 관리형 권한을 입력으로 사용하여 공유 리소스에 대한 리소스 기반 정책을 작성합니다.

관리형 권한 버전

관리형 권한에 대한 변경 사항은 해당 관리형 권한의 새 버전으로 표시됩니다. 새 버전이 모든 새 리소스 공유의 기본값입니다. 각 관리형 권한에는 항상 하나의 버전이 기본 버전으로 지정됩니다. 사용자 또는 AWS이 관리형 권한 버전을 새로 생성하는 경우 기존 리소스 공유 각각에 대해 관리형 권한을 명시적으로 업데이트해야 합니다. 이 단계에서는 리소스 공유에 변경 사항을 적용하기 전에 변경 사항을 평가할 수 있습니다. 모든 새 리소스 공유는 해당 리소스 유형에 대한 관리 권한의 새 버전을 자동으로 사용합니다.

AWS 관리형 권한 버전

AWS 관리형 권한에 대한 모든 변경 사항은 AWS에서 처리합니다. 이러한 변경으로 새로운 기능이 추가되거나 발견된 단점이 제거됩니다. 기본 관리형 권한 버전은 리소스 공유에만 적용할 수 있습니다.

고객 관리형 권한 버전

고객 관리형 권한에 대한 모든 변경 사항은 사용자가 처리합니다. 새 기본 버전을 생성하거나, 이전 버전을 기본 버전으로 설정하거나, 리소스 공유와 더 이상 연결되지 않는 버전을 삭제할 수 있습니다. 각 고객 관리형 권한의 버전은 최대 5개까지 보유할 수 있습니다.

리소스 공유를 생성하거나 업데이트할 때 지정된 관리형 권한의 기본 버전만 연결할 수 있습니다. 자세한 내용은 AWS 관리형 권한을 최신 버전으로 업데이트 섹션을 참조하세요.

AWS 리소스 공유

AWS RAM을 사용하여 내 소유의 리소스를 공유하려면 다음을 수행합니다.

- AWS Organizations 내에서 리소스 공유 활성화(선택 사항)
- 리소스 공유 생성

> **참고**
>
> - 리소스를 소유한 AWS 계정 외부의 보안 주체와 리소스를 공유해도 리소스를 생성한 계정 내에서 해당 리소스에 적용되는 권한 또는 할당량은 변경되지 않습니다.
> - AWS RAM은 리전 서비스입니다. 나와 리소스를 공유하는 보안 주체는 해당 리소스가 생성된 AWS 리전에서만 리소스 공유에 액세스할 수 있습니다.

- 일부 리소스에는 공유를 위한 특별 고려 사항과 사전 요구 사항이 있습니다. 자세한 내용은 공유 가능한 리소스 AWS 섹션을 참조하세요.

AWS Organizations 내에서 리소스 공유 활성화

AWS Organizations에서 계정을 관리하는 경우 이를 활용하면 리소스를 더 쉽게 공유할 수 있습니다. Organizations 사용 여부와 관계없이, 사용자는 개별 계정과 리소스를 공유할 수 있습니다. 그러나 계정이 조직에 있는 경우 각 계정을 열거할 필요 없이 개별 계정과 공유하거나 조직 또는 OU의 모든 계정과 공유할 수 있습니다.

조직 내에서 리소스를 공유하려면 먼저 AWS RAM 콘솔이나 AWS Command Line Interface(AWS CLI)를 사용하여 AWS Organizations와의 공유를 활성화해야 합니다. 조직의 리소스를 공유하는 경우 AWS RAM에서는 보안 주체에게 초대를 보내지 않습니다. 조직의 보안 주체는 초대를 주고받지 않고도 공유 리소스에 액세스할 수 있습니다.

조직 내에서 리소스 공유를 활성화하면 AWS RAM에서는 **`AWSServiceRoleForResourceAccessManager`**라는 서비스 연결 역할을 생성합니다. 이 역할은 AWS RAM 서비스만 수임할 수 있으며, AWS 관리형 정책 `AWSResourceAccessManagerServiceRolePolicy`를 사용하여 소속된 조직에 대한 정보를 검색할 수 있는 AWS RAM 권한을 부여합니다.

전체 조직 또는 OU와 리소스를 더 이상 공유할 필요가 없는 경우 리소스 공유를 비활성화할 수 있습니다. 자세한 내용은 AWS Organizations와의 리소스 공유 비활성화 섹션을 참조하세요.

최소 권한

아래 절차를 실행하려면 다음 권한이 있는 조직의 관리 계정에 보안 주체로 로그인해야 합니다.

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

요구 사항

- 조직의 관리 계정에 보안 주체로 로그인한 상태에서만 이 단계를 수행할 수 있습니다.

- 조직에서 모든 기능이 활성화되어 있어야 합니다. 자세한 내용은 AWS Organizations 사용 설명서에서 조직 내 모든 기능 활성화를 참조하세요.

> **Important**
>
> AWS RAM 콘솔 또는 enable-sharing-with-aws-organization AWS CLI 명령을 사용하여 AWS Organizations와의 공유를 활성화해야 합니다. 이렇게 하면 `AWSServiceRoleForResourceAccessManager` 서비스 연결 역할이 생성됩니다. AWS Organizations 콘솔 또는 enable-aws-service-access AWS CLI 명령을 사용하여 AWS Organizations에 대한 신뢰할 수 있는 액세스를 활성화하면 `AWSServiceRoleForResourceAccessManager` 서비스 연결 역할이 생성되지 않으며 조직 내에서 리소스를 공유할 수 없습니다.

Console

조직 내 리소스 공유를 활성화하려면

1. AWS RAM 콘솔에서 설정 페이지를 엽니다.
2. AWS Organizations와 공유 활성화를 선택한 다음 설정 저장을 선택합니다.

AWS CLI

조직 내 리소스 공유를 활성화하려면

enable-sharing-with-aws-organization 명령을 사용합니다.

이 명령은 모든 AWS 리전에서 사용할 수 있으며, AWS RAM이 지원되는 모든 리전에서 AWS Organizations와의 공유를 활성화합니다.

```
$ aws ram enable-sharing-with-aws-organization
{
    "returnValue": true
}
```

리소스 공유 생성

내 소유의 리소스를 공유하려면 리소스 공유를 생성합니다. 다음은 이 프로세스를 요약한 것입니다.

1. 공유하려는 리소스를 추가합니다.
2. 공유에 포함할 리소스 유형마다 해당 리소스 유형에 사용할 관리형 권한을 지정합니다.
   - 사용 가능한 AWS 관리형 권한 중 하나 또는 기존 고객 관리형 권한을 선택하거나 고객 관리형 권한을 새로 생성할 수 있습니다.
   - AWS 관리형 권한은 표준 사용 사례를 다루기 위해 AWS에서 생성합니다.
   - 고객 관리형 권한을 사용하면 보안 및 비즈니스 요구 사항에 맞게 관리형 권한을 맞춤 설정할 수 있습니다.

   > **Note**
   >
   > 선택한 관리형 권한에 여러 버전이 있는 경우 AWS RAM에서 자동으로 기본 버전을 연결합니다. 기본 버전으로 지정된 버전만 연결할 수 있습니다.

3. 리소스에 대한 액세스를 허용할 보안 주체를 지정합니다.

고려 사항

- 공유에 포함된 AWS 리소스를 나중에 삭제해야 하는 경우 먼저 해당 리소스가 포함된 리소스 공유에서 리소스를 제거하거나 리소스 공유를 삭제하는 것이 좋습니다.
- 리소스 공유에 포함될 수 있는 리소스 유형은 공유 가능한 리소스 AWS에 나열되어 있습니다.
- 본인이 소유한 리소스만 공유할 수 있습니다. 공유 받은 리소스는 공유할 수 없습니다.
- AWS RAM은 리전 서비스입니다. 리소스를 다른 AWS 계정의 보안 주체와 공유하는 경우 해당 보안 주체는 리소스가 생성된 동일한 AWS 리전에서 각 리소스에 액세스해야 합니다. 지원되는 글로벌 리소스의 경우, 해당 리소스의 서비스 콘솔 및 도구에서 지원하는 모든 AWS 리전에서 액세스할 수 있습니다. 이러한 리소스 공유 및 글로벌 리소스는 지정된 홈 리전인 미국 동부(버지니아 북부), `us-east-1`에서만 AWS RAM 콘솔 및 도구에서 볼 수 있습니다. AWS RAM 및 글로벌 리소스에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
- 공유 중인 계정이 AWS Organizations에 있는 조직에 속해 있고 조직 내 공유가 활성화되어 있으면 초대를 사용하지 않아도 공유하는 조직의 모든 보안 주체에게 리소스 공유에 대한 액세스 권한이 자동으로 부여됩니다. 조직 외부에서 나와 공유하고 있는 계정의 보안 주체는 리소스 공유에 참여하라는 초대를 받게 되며, 초대를 수락해야만 공유 리소스에 대한 액세스 권한이 부여됩니다.
- 서비스 주체와 공유하는 경우 다른 주체를 리소스 공유에 연결할 수 없습니다.
- 조직에 속한 계정 또는 보안 주체 간에 공유하는 경우 조직 멤버십이 변경되면 리소스 공유에 대한 액세스 권한이 동적으로 영향을 받습니다.

- 리소스 공유에 액세스할 수 있는 조직이나 OU에 AWS 계정을 추가하면 새 멤버 계정에 리소스 공유에 대한 액세스 권한이 자동으로 부여됩니다. 그러면 공유한 계정의 관리자가 해당 계정의 개별 보안 주체에게 해당 공유의 리소스에 대한 액세스 권한을 부여할 수 있습니다.
- 리소스 공유에 액세스할 수 있는 조직 또는 OU에서 계정을 제거하면 해당 계정의 모든 보안 주체는 해당 리소스 공유를 통해 액세스한 리소스에 자동으로 액세스할 수 없게 됩니다.
- 멤버 계정 또는 멤버 계정 내의 IAM 역할 또는 사용자와 직접 공유한 다음 조직에서 해당 계정을 제거하면 해당 계정의 모든 보안 주체는 해당 리소스 공유를 통해 액세스한 리소스에 액세스할 수 없게 됩니다.

> **Important**
>
> 조직 또는 OU와 공유할 때 해당 범위에 리소스 공유를 소유한 계정이 포함되어 있으면 공유 계정의 모든 주체가 자동으로 공유의 리소스에 대한 액세스 권한을 얻게 됩니다. 부여된 액세스 권한은 공유와 연결된 관리형 권한에 의해 정의됩니다. 이는 AWS RAM에서 공유의 각 리소스에 연결한 리소스 기반 정책이 `"Principal": "*"`을 사용하기 때문입니다. 자세한 내용은 리소스 기반 정책에서 "Principal": "*" 사용 시 유의 사항 섹션을 참조하세요.
> 다른 소비 계정의 보안 주체는 공유 리소스에 즉시 액세스할 수 없습니다. 다른 계정의 관리자가 먼저 자격 증명 기반 권한 정책을 해당 보안 주체에 연결해야 합니다. 이러한 정책은 리소스 공유에 있는 개별 리소스의 ARN에 `Allow` 액세스 권한을 부여해야 합니다. 이러한 정책의 권한은 리소스 공유와 연결된 관리형 권한에 지정된 권한을 초과할 수 없습니다.

- 계정이 속해 있는 조직과 해당 조직의 OU만 리소스 공유에 추가할 수 있습니다. 내 조직 외부의 OU 또는 조직을 리소스 공유에 보안 주체로 추가할 수 없습니다. 그러나 개별 AWS 계정 또는 조직 외부의 IAM 역할 및 사용자(지원되는 서비스의 경우)는 리소스 공유에 보안 주체로 추가할 수 있습니다.

> **Note**
>
> 모든 리소스 유형을 IAM 역할 및 사용자와 공유할 수 있는 것은 아닙니다. 이러한 보안 주체와 공유할 수 있는 리소스에 대한 자세한 내용은 공유 가능한 리소스 AWS 섹션을 참조하세요.

- 다음 리소스 유형의 경우 7일 이내에 공유 참여 초대를 수락해야 합니다. 만료되기 전에 초대를 수락하지 않으면 초대가 자동으로 거부됩니다.

> **Important**
>
> 다음 목록에 없는 공유 리소스 유형의 경우 12시간 이내에 리소스 공유 참여 초대를 수락해야 합니다. 12시간이 경과하면 초대가 만료되고 리소스 공유의 최종 사용자 보안 주체가 연결 해제됩니다. 최종 사용자는 더 이상 초대를 수락할 수 없습니다.

- Amazon Aurora – DB 클러스터
- Amazon EC2 – 용량 예약 및 전용 호스트
- AWS License Manager – 라이선스 구성
- AWS Outposts – 로컬 게이트웨이 라우팅 테이블, outposts, 사이트
- Amazon Route 53 – 전달 규칙
- Amazon VPC - 고객 소유 IPv4 주소, 접두사 목록, 서브넷, 트래픽 미러 대상, 전송 게이트웨이, 전송 게이트웨이 멀티캐스트 도메인

Console

리소스 공유를 생성하려면

1. AWS RAM 콘솔을 엽니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), `us-east-1`로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요. 리소스 공유에 글로벌 리소스를 포함하려면 지정된 홈 리전인 미국 동부(버지니아 북부), `us-east-1`을 선택해야 합니다.
3. AWS RAM을 처음 사용하는 경우 홈 페이지에서 리소스 공유 생성을 선택합니다. 그렇지 않은 경우 내 공유: 리소스 공유 페이지에서 리소스 공유 생성을 선택합니다.
4. 1단계: 리소스 공유 세부 정보 지정에서 다음을 수행합니다.

   a. 이름에 리소스 공유를 설명하는 이름을 입력합니다.

   b. 리소스에서 다음과 같이 리소스 공유에 추가할 리소스를 선택합니다.

      - 리소스 유형 선택에서 공유할 리소스 유형을 선택합니다. 그러면 공유 가능한 리소스 목록이 선택한 유형의 리소스로만 필터링됩니다.

- 결과 리소스 목록에서 공유하려는 개별 리소스 옆의 확인란을 선택합니다. 선택한 리소스가 선택한 리소스 아래로 이동합니다.

  특정 가용 영역과 연결된 리소스를 공유하는 경우 가용 영역 ID(AZ ID)를 사용하면 여러 계정에서 이러한 리소스의 상대적 위치를 파악할 수 있습니다. 자세한 내용은 AWS 리소스의 가용 영역 ID 섹션을 참조하세요.

c. (선택 사항) 리소스 공유에 태그를 연결하려면 태그 아래에 태그 키와 값을 입력합니다. 새 태그 추가를 선택하여 다른 태그를 추가합니다. 필요에 따라 이 단계를 반복합니다. 이러한 태그는 리소스 공유 자체에만 적용되며 리소스 공유의 리소스에는 적용되지 않습니다.

5. 다음을 선택합니다.

6. 2단계: 각 리소스 유형과 관리형 권한 연결에서 AWS를 통해 생성된 관리형 권한을 리소스 유형과 연결하거나, 기존 고객 관리형 권한을 선택하거나, 지원되는 리소스 유형에 대해 고객 관리형 권한을 직접 생성할 수 있습니다. 자세한 내용은 관리형 권한의 유형 섹션을 참조하세요.

   고객 관리형 권한 생성을 선택하여 공유 사용 사례의 요구 사항을 충족하는 고객 관리형 권한을 구성합니다. 자세한 내용은 고객 관리형 정책 생성 섹션을 참조하세요. 프로세스를 완료한 후

   를 선택한 다음 관리형 권한 드롭다운 목록에서 새 고객 관리형 권한을 선택할 수 있습니다.

   > **Note**
   >
   > 선택한 관리형 권한에 여러 버전이 있는 경우 AWS RAM에서 자동으로 기본 버전을 연결합니다. 기본 버전으로 지정된 버전만 연결할 수 있습니다.

   관리형 권한에서 허용하는 작업을 표시하려면 이 관리형 권한에 대한 정책 템플릿 보기를 확장합니다.

7. 다음을 선택합니다.

8. 3단계: 보안 주체에 액세스 권한 부여에서 다음을 수행합니다.

   a. 기본적으로 누구에게나 공유 허용이 선택되어 있습니다. 즉, 이를 지원하는 리소스 유형의 경우 조직 외부에 있는 AWS 계정과 리소스를 공유할 수 있습니다. 이는 Amazon VPC 서브넷과 같이 조직 내에서만 공유할 수 있는 리소스 유형에는 영향을 주지 않습니다. 지원되는 일부 리소스 유형을 IAM 역할 및 사용자와 공유할 수도 있습니다.

리소스 공유를 조직 내 계정 및 보안 주체로만 제한하려면 조직 내에서만 공유 허용을 선택합니다.

b. 보안 주체에서 다음을 수행합니다.

- 조직, 조직 단위(OU) 또는 조직에 속한 AWS 계정을 추가하려면 조직 구조 표시를 켭니다. 그러면 조직의 트리 보기가 표시됩니다. 그런 다음 추가하려는 각 보안 주체 옆의 확인란을 선택합니다.

> **Important**
>
> 조직 또는 OU와 공유할 때 해당 범위에 리소스 공유를 소유한 계정이 포함되어 있으면 공유 계정의 모든 주체가 자동으로 공유의 리소스에 대한 액세스 권한을 얻게 됩니다. 부여된 액세스 권한은 공유와 연결된 관리형 권한에 의해 정의됩니다. 이는 AWS RAM에서 공유의 각 리소스에 연결한 리소스 기반 정책이 `"Principal": "*"`을 사용하기 때문입니다. 자세한 내용은 리소스 기반 정책에서 "Principal": "*" 사용 시 유의 사항 섹션을 참조하세요.
> 다른 소비 계정의 보안 주체는 공유 리소스에 즉시 액세스할 수 없습니다. 다른 계정의 관리자가 먼저 자격 증명 기반 권한 정책을 해당 보안 주체에 연결해야 합니다. 이러한 정책은 리소스 공유에 있는 개별 리소스의 ARN에 `Allow` 액세스 권한을 부여해야 합니다. 이러한 정책의 권한은 리소스 공유와 연결된 관리형 권한에 지정된 권한을 초과할 수 없습니다.

- 조직(ID가 `o-`로 시작)을 선택하면 조직 내 모든 AWS 계정의 보안 주체가 리소스 공유에 액세스할 수 있습니다.
- OU(ID가 `ou-`로 시작)를 선택하면 해당 OU와 하위 OU에 있는 모든 AWS 계정의 보안 주체가 리소스 공유에 액세스할 수 있습니다.
- 개별 AWS 계정을 선택하면 해당 계정에 있는 보안 주체만 리소스 공유에 액세스할 수 있습니다.

> **Note**
>
> 조직 구조 표시 토글은 AWS Organizations와의 공유가 활성화되어 있고 조직의 관리 계정에 로그인한 경우에만 나타납니다.

이 방법으로는 조직 외부의 AWS 계정이나 IAM 역할 또는 사용자를 지정할 수 없습니다. 대신 조직 구조 표시를 끄고 드롭다운 목록과 텍스트 상자를 사용하여 ID 또는 ARN을 입력해야 합니다.

- 조직 외부의 보안 주체를 포함하여 ID 또는 ARN으로 보안 주체를 지정하려면 각 보안 주체에 대해 보안 주체 유형을 선택합니다. 그런 다음 ID(AWS 계정, 조직 또는 OU의 경우) 또는 ARN(IAM 역할 또는 사용자의 경우)을 입력하고 추가를 선택합니다. 사용 가능한 보안 주체 유형, ID 및 ARN 형식은 다음과 같습니다.
  - AWS 계정 – AWS 계정을 추가하려면 12자리 계정 ID를 입력합니다. 예:

    ```
    123456789012
    ```

  - 조직 - 조직의 모든 AWS 계정을 추가하려면 조직 ID를 입력합니다. 예:

    ```
    o-abcd1234
    ```

  - 조직 단위(OU) - OU를 추가하려면 OU ID를 입력합니다. 예:

    ```
    ou-abcd-1234efgh
    ```

  - IAM 역할 - IAM 역할을 추가하려면 역할의 ARN을 입력합니다. 다음 구문을 사용합니다.

    ```
    arn:partition:iam::account:role/role-name
    ```

    예:

    ```
    arn:aws:iam::123456789012:role/MyS3AccessRole
    ```

    > **Note**
    >
    > IAM 역할의 고유 ARN을 가져오려면 IAM 콘솔에서 역할 목록을 확인하고 get-role AWS CLI 명령 또는 GetRole API 작업을 사용합니다.

  - IAM 사용자 - IAM 사용자를 추가하려면 사용자의 ARN을 입력합니다. 다음 구문을 사용합니다.

    ```
    arn:partition:iam::account:user/user-name
    ```

    예:

    ```
    arn:aws:iam::123456789012:user/bob
    ```

> **Note**
>
> IAM 사용자의 고유 ARN을 가져오려면 IAM 콘솔에서 사용자 목록을 확인하고 get-user AWS CLI 명령 또는 GetUser API 작업을 사용합니다.

- 서비스 보안 주체 - 서비스 보안 주체를 추가하려면 보안 주체 유형 선택 드롭박스에서 서비스 주체를 선택합니다. AWS 서비스 보안 주체의 이름을 입력합니다. 다음 구문을 사용합니다.
  - *service-id*.amazonaws.com

    예:

    pca-connector-ad.amazonaws.com

c. 선택한 보안 주체에서 지정한 보안 주체가 목록에 나타나는지 확인합니다.

9. 다음을 선택합니다.
10. 4단계: 검토 및 생성에서 리소스 공유에 대한 구성 세부 정보를 검토합니다. 단계 구성을 변경하려면 돌아가려는 단계에 해당하는 링크를 선택한 다음 필요한 사항을 변경합니다.
11. 리소스 공유 검토를 완료한 후 리소스 공유 생성을 선택합니다.

    리소스 및 보안 주체 연결이 완료되는 데 몇 분 정도 걸릴 수 있습니다. 이 프로세스가 완료될 때까지 기다렸다가 리소스 공유를 사용해 보세요.
12. 언제든지 리소스와 보안 주체를 추가 및 제거하거나 리소스 공유에 사용자 지정 태그를 적용할 수 있습니다. 기본 관리형 권한 이상을 지원하는 리소스 유형의 경우 리소스 공유에 포함된 리소스 유형의 관리형 권한을 변경할 수 있습니다. 리소스를 더 이상 공유하지 않으려는 경우 리소스 공유를 삭제할 수 있습니다. 자세한 내용은 내 소유의 AWS 리소스 공유 섹션을 참조하세요.

AWS CLI

리소스 공유를 생성하려면

create-resource-share 명령을 사용합니다. 다음 명령은 조직의 모든 AWS 계정과 공유되는 리소스 공유를 생성합니다. 공유에는 AWS License Manager 라이선스 구성이 포함되며 해당 리소스 유형에 대해 기본 관리형 권한이 부여됩니다.

> **Note**
>
> 이 리소스 공유의 리소스 유형과 함께 고객 관리형 권한을 사용하려는 경우 기존 고객 관리형 권한을 사용하거나 새 고객 관리형 권한을 생성할 수 있습니다. 고객 관리형 권한의 ARN을 기록해 둔 다음 리소스 공유를 생성합니다. 자세한 내용은 고객 관리형 정책 생성 섹션을 참조하세요.

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

AWS 공유 리소스 사용

AWS Resource Access Manager를 사용하여 내 계정과 공유된 리소스를 사용하려면 다음 작업을 완료합니다.

작업

- 리소스 공유 초대에 응답
- 공유 받은 리소스 사용

리소스 공유 초대에 응답

리소스 공유에 참여하라는 초대를 받은 경우 초대를 수락해야 공유 리소스에 액세스할 수 있습니다.

다음과 같은 경우에는 초대가 사용되지 않습니다.

- AWS Organizations의 조직에 속해 있고 조직 내 공유가 활성화되어 있는 경우 해당 조직의 보안 주체는 초대 없이 공유 리소스에 자동으로 액세스할 수 있습니다.
- 리소스를 소유하고 있는 AWS 계정과 공유할 경우 해당 계정의 보안 주체는 초대 없이 공유 리소스에 자동으로 액세스할 수 있습니다.

Console

초대에 응답하려면

1. AWS RAM 콘솔에서 나와 공유: 리소스 공유 페이지를 엽니다.

   > **Note**
   >
   > 리소스 공유는 해당 공유가 생성된 AWS 리전에서만 볼 수 있습니다. 예상 리소스 공유가 콘솔에 표시되지 않는 경우 오른쪽 상단의 드롭다운 컨트롤을 사용하여 다른 AWS 리전으로 전환해야 할 수 있습니다.

2. 액세스 권한이 부여된 리소스 공유 목록을 검토합니다.

   상태 열은 리소스 공유에 대한 현재 참여 상태를 나타냅니다. `Pending` 상태는 리소스 공유에 추가되었지만 아직 초대를 수락하거나 거부하지 않았음을 나타냅니다.

3. 리소스 공유 초대에 응답하려면 리소스 공유 ID를 선택하고 리소스 공유 수락을 선택하여 초대를 수락하거나 리소스 공유 거부를 선택하여 초대를 거부합니다. 초대를 거부하면 리소스에 액세스할 수 없습니다. 초대를 수락하면 리소스에 액세스할 수 있습니다.

AWS CLI

먼저 사용 가능한 리소스 공유 초대 목록을 확인합니다. 다음 예제 명령은 `us-west-2` 리전에서 실행되었으며, 한 리소스 공유가 `PENDING` 상태임을 보여줍니다.

```
$ aws ram get-resource-share-invitations
{
    "resourceShareInvitations": [
```

```
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
west-2:111122223333:resource-share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
            "resourceShareName": "MyNewResourceShare",
            "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
            "senderAccountId": "111122223333",
            "receiverAccountId": "444455556666",
            "invitationTimestamp": "2021-09-15T15:00:32.568000-07:00",
            "status": "PENDING"
        }
    ]
}
```

이전 명령에 있는 초대의 Amazon 리소스 이름(ARN)을 다음 명령의 파라미터로 사용하여 해당 초대를 수락할 수 있습니다.

```
$ aws ram accept-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
        "resourceShareName": "MyNewResourceShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
        "senderAccountId": "111122223333",
        "receiverAccountId": "444455556666",
        "invitationTimestamp": "2021-09-15T15:14:12.580000-07:00",
        "status": "ACCEPTED"
    }
}
```

출력에는 `status`가 `ACCEPTED`로 변경되었음을 보여줍니다. 이제 해당 리소스 공유에 포함된 리소스를 수락 계정의 보안 주체가 사용할 수 있습니다.

공유 받은 리소스 사용

리소스 공유 참여 초대를 수락한 후에는 공유 리소스에 대해 특정 작업을 수행할 수 있습니다. 이러한 작업은 리소스 유형에 따라 다릅니다. 자세한 내용은 공유 가능한 리소스 AWS 섹션을 참조하세요. 리

소스는 각 리소스의 서비스 콘솔 및 API/CLI 작업에서 직접 사용할 수 있습니다. 리전 리소스인 경우 서비스 콘솔 또는 API/CLI 명령에서 올바른 AWS 리전을 사용해야 합니다. 글로벌 리소스인 경우 지정된 홈 리전인 미국 동부(버지니아 북부), `us-east-1`를 사용해야 합니다. AWS RAM에서 리소스를 보려면 AWS RAM 콘솔을 리소스 공유가 생성된 AWS 리전에서 열어야 합니다.

AWS 공유 리소스 작업

AWS Resource Access Manager(AWS RAM)를 사용하여 내 소유의 AWS 리소스를 공유하고 공유 받은 AWS 리소스에 액세스할 수 있습니다.

목차

글로벌 리소스와 리전 리소스를 비교하여 공유

이 주제에서는 AWS Resource Access Manager(AWS RAM)에서 리전 리소스와 글로벌 리소스를 사용하는 방법의 차이점에 대해 설명합니다.

리소스는 리전 리소스 또는 글로벌 리소스 중 하나입니다. Amazon 리소스 이름(ARN)의 네 번째 필드에서 리전 리소스 또는 글로벌 리소스인지 식별할 수 있습니다. 리전 리소스는 AWS 리전로 표시됩니다. 비어 있다면 글로벌 리소스입니다.

리전 리소스와 글로벌 리소스의 차이점

리전 리소스

AWS RAM과 공유할 수 있는 대부분의 리소스가 리전 리소스입니다. 리전 리소스를 지정된 AWS 리전에 생성하면 해당 리전에 존재하게 됩니다. 이러한 리소스를 보거나 해당 리소스와 상호 작용하려면 해당 리전으로 작업을 지시해야 합니다. 예를 들어 AWS Management Console을 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 생성하려면 인스턴스를 생성할 AWS 리전을 선택합니다. AWS Command Line Interface(AWS CLI)를 사용하여 인스턴스를 생성하는 경우 `--region` 파라미터를 포함해야 합니다. 각 AWS SDK에는 작업에 사용할 리전을 지정하는 자체 메커니즘이 있습니다.

리전 리소스를 사용하는 데에는 여러 가지 이유가 있습니다. 좋은 이유 중 하나는 리소스와 리소스 액세스에 사용하는 서비스 엔드포인트가 고객과 가능한 한 가까운 곳에 위치하도록 보장하는 것입니다. 그러면 지연 시간이 최소화되어 성능이 향상됩니다. 또 다른 이유는 격리 경계를 제공하기 위해서입니다. 이를 통해 리소스의 독립적인 복사본을 여러 리전에 생성하여 부하를 분산하고 확장성을 개선할 수 있습니다. 동시에 리소스를 서로 분리하여 가용성을 높일 수 있습니다.

콘솔이나 AWS CLI 명령에서 서로 다른 AWS 리전을 지정하면 이전 리전에서 볼 수 있었던 리소스를 더 이상 보거나 해당 리소스와 상호작용할 수 없습니다.

리전 리소스의 Amazon 리소스 이름(ARN)을 보면 해당 리소스가 포함된 리전이 ARN의 네 번째 필드로 지정되어 있습니다. 예를 들어 Amazon EC2 인스턴스는 리전 리소스입니다. 이러한 리소스에는 `us-east-1` 리전에 있는 VPC에 대해 다음 샘플과 유사한 ARN이 있습니다.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

글로벌 리소스

일부 AWS 서비스는 전 세계에서 액세스할 수 있는 리소스를 지원하므로 어디서나 리소스를 사용할 수 있습니다. 글로벌 서비스 콘솔에서는 AWS 리전을 지정하지 않습니다. 글로벌 리소스에 액세스하려면 서비스의 AWS CLI 및 AWS SDK 작업을 사용할 때 `--region` 파라미터를 지정하지 마십시오.

글로벌 리소스는 특정 리소스의 인스턴스가 한 번에 하나만 있어야 하는 경우를 지원합니다. 이러한 경우 서로 다른 리전에 있는 복사본 간 복제 또는 동기화는 바람직하지 않습니다. 단일 글로벌 엔

드포인트에 액세스하는 것은 지연 시간이 늘어날 수는 있지만, 모든 변경 사항을 리소스 소비자에게 즉시 표시할 수 있다는 점에서 허용 가능한 것으로 간주됩니다. 예를 들어 AWS Cloud WAN 코어 네트워크를 글로벌 리소스로 생성하면 모든 사용자에게 일관되게 적용됩니다. 따라서 모든 리전에서 하나의 연속적인 글로벌 네트워크로 나타납니다.

글로벌 리소스의 Amazon 리소스 이름(ARN)에는 리전이 포함되지 않습니다. 이러한 ARN의 네 번째 필드는 Cloud WAN 코어 네트워크에 대한 다음 샘플 ARN과 같이 비어 있습니다.

```
arn:aws:networkmanager::123456789012:core-network/core-network-0514d38fa6f796cea
```

리소스 공유 및 해당 리전

AWS RAM은 리전 서비스이고 리소스 공유도 리전입니다. 따라서 리소스 공유에는 리소스 공유와 동일한 AWS 리전 리전의 리소스와 지원되는 모든 글로벌 리소스가 포함될 수 있습니다. 리소스 공유를 생성할 때의 리전이 리소스 공유의 홈 리전입니다.

> **Important**
>
> 현재는 글로벌 리소스가 포함된 리소스 공유를 지정된 홈 리전에서만 즉, 미국 동부(버지니아 북부) 리전(us-east-1)에서만 생성할 수 있습니다. 리소스 공유는 해당 단일 홈 리전에서만 생성할 수 있지만, 공유된 글로벌 리소스는 해당 서비스의 콘솔이나 CLI 및 SDK 작업에서 볼 때 표준 글로벌 리소스로 표시됩니다. 홈 리전에 대한 제한은 리소스 공유에만 적용되며, 리소스 공유에 포함된 리소스에는 적용되지 않습니다.

us-west-2 리전에서 생성한 리전 리소스를 공유하려면 us-west-2를 사용하도록 AWS RAM 콘솔을 구성하고 해당 리전에 리소스 공유를 생성해야 합니다. 포함된 리전 리소스의 AWS 리전이 서로 다를 경우 리소스 공유를 생성할 수 없습니다. 즉, us-west-2 및 eu-north-1의 리소스를 공유하려면 두 개의 서로 다른 리소스 공유를 생성해야 합니다. 서로 다른 두 리전의 리소스를 단일 리소스 공유로 결합할 수는 없습니다.

AWS RAM 콘솔에서 글로벌 리소스를 공유하려면 지정된 홈 리전인 미국 동부(버지니아 북부) us-east-1를 사용하도록 AWS RAM 콘솔을 구성해야 합니다. 그런 다음 지정된 홈 리전에 리소스 공유를 생성합니다. 리소스 공유의 글로벌 리소스는 us-east-1 리전의 리소스와만 결합할 수 있습니다.

글로벌 리소스는 지정된 홈 리전에서만 AWS RAM 리소스 공유에서 볼 수 있지만, 공유한 후에도 계속 글로벌 리소스입니다. 원래 AWS 계정에서 액세스할 수 있는 어느 리전에서든 공유 AWS 계정에서 액세스할 수 있습니다.

고려 사항

- AWS RAM 콘솔에서 리소스 공유를 생성하려면 공유할 리소스가 있는 리전을 사용해야 합니다. 글로벌 리소스를 포함하려면 지정된 홈 리전을 사용하여 공유를 생성해야 합니다. 예를 들어 AWS Cloud WAN 코어 네트워크를 공유하려면 us-east-1 리전에 리소스 공유를 생성해야 합니다.
- AWS RAM 콘솔에서 리소스 공유를 보거나 수정하려면 리소스 공유가 있는 리전을 사용해야 합니다. 마찬가지로, AWS RAM AWS CLI 및 SDK 작업을 사용하면 작업에 지정한 리전에 있는 리소스 공유와만 상호 작용할 수 있습니다. 전역 리소스가 포함된 리소스 공유를 보거나 수정하려면 지정된 홈 리전인 미국 동부(버지니아 북부), us-east-1를 사용해야 합니다.
- AWS RAM 콘솔에서 리전 리소스를 확인하여 리소스 공유에 포함시키려면 해당 리전 리소스가 있는 리전을 사용해야 합니다.
- AWS RAM 콘솔에서 글로벌 리소스를 확인하여 리소스 공유에 포함시키려면 지정된 홈 리전인 미국 동부(버지니아 북부), us-east-1를 사용해야 합니다.
- 지정된 홈 리전인 미국 동부(버지니아 북부), us-east-1에서만 리전 리소스와 글로벌 리소스가 모두 포함된 리소스 공유를 생성할 수 있습니다.

내 소유의 AWS 리소스 공유

AWS Resource Access Manager(AWS RAM)를 사용하여 내가 지정한 리소스를 지정한 주체와 공유할 수 있습니다. 이 섹션에서는 새 리소스 공유를 생성하고, 기존 리소스 공유를 수정하고, 더 이상 필요하지 않은 리소스 공유를 삭제하는 방법에 대해 설명합니다.

주제

- AWS RAM에서 생성한 리소스 공유 보기
- AWS RAM에서 리소스 공유 생성
- AWS RAM에서 리소스 공유 업데이트
- AWS RAM에서 공유 리소스 보기
- AWS RAM에서 내가 리소스를 공유하고 있는 보안 주체 보기
- AWS RAM에서 리소스 공유 삭제

AWS RAM에서 생성한 리소스 공유 보기

생성한 리소스 공유 목록을 볼 수 있습니다. 공유 중인 리소스와 공유 주체를 확인할 수 있습니다.

Console

리소스 공유를 보려면

1. AWS RAM 콘솔에서 내 공유: 리소스 공유 페이지를 엽니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), `us-east-1`로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 결과에서 리소스 공유가 사용하는 관리형 권한 중 기본값으로 지정된 관리형 권한의 새 버전이 있는 경우 페이지에 경고 배너가 표시됩니다. 페이지 상단에 있는 검토 및 모두 업데이트를 선택하여 모든 관리형 권한 버전을 한 번에 업데이트하도록 선택할 수 있습니다.

   또는 개별 리소스 공유에 새 버전의 관리형 권한이 하나 이상 있는 경우 상태 열에 업데이트 가능이 표시됩니다. 이 링크를 선택하면 업데이트된 관리형 권한 버전을 검토하고 이 버전을 해당 리소스 공유의 관련 리소스 유형에 대한 버전으로 할당할 수 있는 프로세스가 시작됩니다.
4. (선택 사항) 필터를 적용하여 특정 리소스 공유를 찾습니다. 여러 필터를 적용하여 검색 범위를 좁힐 수 있습니다. 리소스 공유 이름의 일부와 같은 키워드를 입력하여 이름에 해당 텍스트가 포함된 리소스 공유만 나열할 수 있습니다. 텍스트 상자를 선택하면 제안된 속성 필드의 드롭다운 목록이 표시됩니다. 하나를 선택한 후 해당 필드에 사용할 수 있는 값 목록에서 선택할 수 있습니다. 원하는 리소스를 찾을 때까지 다른 속성이나 키워드를 추가할 수 있습니다.
5. 검토할 리소스 공유의 이름을 선택합니다. 콘솔에 리소스 공유에 대한 다음 정보가 표시됩니다.

   - 요약 - 리소스 공유 이름, ID, 소유자, Amazon 리소스 이름(ARN), 생성 날짜, 외부 계정과의 공유 허용 여부, 현재 상태가 나열됩니다.
   - 관리형 권한 - 해당 리소스 공유에 연결된 관리형 권한이 나열됩니다. 리소스 공유에 포함된 리소스 유형당 관리 권한은 하나만 있을 수 있습니다. 각 관리형 권한에는 리소스 공유와 연결된 해당 관리형 권한의 버전이 표시됩니다. 기본 버전이 아닌 경우 콘솔에 기본 버전으로 업데이트 링크가 표시됩니다. 해당 링크를 선택하면 기본 버전을 사용하도록 리소스 공유를 업데이트할 수 있습니다.
   - 공유 리소스 - 리소스 공유에 포함된 개별 리소스를 나열합니다. 리소스 ID를 선택하면 기본 서비스 콘솔에서 리소스를 볼 수 있는 새 브라우저 탭이 열립니다.
   - 공유 보안 주체 - 리소스를 공유하는 보안 주체가 나열됩니다.
   - 태그 - 리소스 공유 자체에 연결된 태그 키-값 쌍이 나열됩니다. 이 쌍은 리소스 공유에 포함된 개별 리소스에 연결된 태그가 아닙니다.

AWS CLI

리소스 공유를 보려면

`--resource-owner` 파라미터를 `SELF`로 설정하여 get-resource-shares 명령을 사용하면 AWS 계정에 생성된 리소스 공유의 세부 정보를 표시할 수 있습니다.

다음 예에서는 호출하는 AWS 계정에 대해 현재 AWS 리전(`us-east-1`)에서 공유되는 리소스 공유를 보여줍니다. 다른 리전에 생성된 리소스 공유를 가져오려면 `--region` *<region-code>* 파라미터를 사용합니다. 글로벌 리소스가 포함된 리소스 공유를 포함하려면 미국 동부(버지니아 북부), `us-east-1` 리전을 지정해야 합니다.

```
$  aws ram get-resource-shares \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "name": "MyLicenseConfigShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

AWS RAM에서 리소스 공유 생성

내 소유의 리소스를 공유하려면 리소스 공유를 생성합니다. 다음은 이 프로세스를 요약한 것입니다.

1. 공유하려는 리소스를 추가합니다.
2. 공유에 포함할 리소스 유형마다 해당 리소스 유형에 사용할 관리형 권한을 지정합니다.
   - 사용 가능한 AWS 관리형 권한 중 하나 또는 기존 고객 관리형 권한을 선택하거나 고객 관리형 권한을 새로 생성할 수 있습니다.
   - AWS 관리형 권한은 표준 사용 사례를 다루기 위해 AWS에서 생성합니다.
   - 고객 관리형 권한을 사용하면 보안 및 비즈니스 요구 사항에 맞게 관리형 권한을 맞춤 설정할 수 있습니다.

   > **Note**
   >
   > 선택한 관리형 권한에 여러 버전이 있는 경우 AWS RAM에서 자동으로 기본 버전을 연결합니다. 기본 버전으로 지정된 버전만 연결할 수 있습니다.

3. 리소스에 대한 액세스를 허용할 보안 주체를 지정합니다.

고려 사항

- 공유에 포함된 AWS 리소스를 나중에 삭제해야 하는 경우 먼저 해당 리소스가 포함된 리소스 공유에서 리소스를 제거하거나 리소스 공유를 삭제하는 것이 좋습니다.
- 리소스 공유에 포함될 수 있는 리소스 유형은 공유 가능한 리소스 AWS에 나열되어 있습니다.
- 본인이 소유한 리소스만 공유할 수 있습니다. 공유 받은 리소스는 공유할 수 없습니다.
- AWS RAM은 리전 서비스입니다. 리소스를 다른 AWS 계정의 보안 주체와 공유하는 경우 해당 보안 주체는 리소스가 생성된 동일한 AWS 리전에서 각 리소스에 액세스해야 합니다. 지원되는 글로벌 리소스의 경우, 해당 리소스의 서비스 콘솔 및 도구에서 지원하는 모든 AWS 리전에서 액세스할 수 있습니다. 이러한 리소스 공유 및 글로벌 리소스는 지정된 홈 리전인 미국 동부(버지니아 북부), `us-east-1`에서만 AWS RAM 콘솔 및 도구에서 볼 수 있습니다. AWS RAM 및 글로벌 리소스에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
- 공유 중인 계정이 AWS Organizations에 있는 조직에 속해 있고 조직 내 공유가 활성화되어 있으면 초대를 사용하지 않아도 공유하는 조직의 모든 보안 주체에게 리소스 공유에 대한 액세스 권한이 자동으로 부여됩니다. 조직 외부에서 나와 공유하고 있는 계정의 보안 주체는 리소스 공유에 참여하라는 초대를 받게 되며, 초대를 수락해야만 공유 리소스에 대한 액세스 권한이 부여됩니다.
- 서비스 주체와 공유하는 경우 다른 주체를 리소스 공유에 연결할 수 없습니다.

- 조직에 속한 계정 또는 보안 주체 간에 공유하는 경우 조직 멤버십이 변경되면 리소스 공유에 대한 액세스 권한이 동적으로 영향을 받습니다.
  - 리소스 공유에 액세스할 수 있는 조직이나 OU에 AWS 계정을 추가하면 새 멤버 계정에 리소스 공유에 대한 액세스 권한이 자동으로 부여됩니다. 그러면 공유한 계정의 관리자가 해당 계정의 개별 보안 주체에게 해당 공유의 리소스에 대한 액세스 권한을 부여할 수 있습니다.
  - 리소스 공유에 액세스할 수 있는 조직 또는 OU에서 계정을 제거하면 해당 계정의 모든 보안 주체는 해당 리소스 공유를 통해 액세스한 리소스에 자동으로 액세스할 수 없게 됩니다.
  - 멤버 계정 또는 멤버 계정 내의 IAM 역할 또는 사용자와 직접 공유한 다음 조직에서 해당 계정을 제거하면 해당 계정의 모든 보안 주체는 해당 리소스 공유를 통해 액세스한 리소스에 액세스할 수 없게 됩니다.

> **Important**
>
> 조직 또는 OU와 공유할 때 해당 범위에 리소스 공유를 소유한 계정이 포함되어 있으면 공유 계정의 모든 주체가 자동으로 공유의 리소스에 대한 액세스 권한을 얻게 됩니다. 부여된 액세스 권한은 공유와 연결된 관리형 권한에 의해 정의됩니다. 이는 AWS RAM에서 공유의 각 리소스에 연결한 리소스 기반 정책이 `"Principal": "*"`을 사용하기 때문입니다. 자세한 내용은 리소스 기반 정책에서 "Principal": "*" 사용 시 유의 사항 섹션을 참조하세요.
> 다른 소비 계정의 보안 주체는 공유 리소스에 즉시 액세스할 수 없습니다. 다른 계정의 관리자가 먼저 자격 증명 기반 권한 정책을 해당 보안 주체에 연결해야 합니다. 이러한 정책은 리소스 공유에 있는 개별 리소스의 ARN에 `Allow` 액세스 권한을 부여해야 합니다. 이러한 정책의 권한은 리소스 공유와 연결된 관리형 권한에 지정된 권한을 초과할 수 없습니다.

- 계정이 속해 있는 조직과 해당 조직의 OU만 리소스 공유에 추가할 수 있습니다. 내 조직 외부의 OU 또는 조직을 리소스 공유에 보안 주체로 추가할 수 없습니다. 그러나 개별 AWS 계정 또는 조직 외부의 IAM 역할 및 사용자(지원되는 서비스의 경우)는 리소스 공유에 보안 주체로 추가할 수 있습니다.

> **Note**
>
> 모든 리소스 유형을 IAM 역할 및 사용자와 공유할 수 있는 것은 아닙니다. 이러한 보안 주체와 공유할 수 있는 리소스에 대한 자세한 내용은 공유 가능한 리소스 AWS 섹션을 참조하세요.

- 다음 리소스 유형의 경우 7일 이내에 공유 참여 초대를 수락해야 합니다. 만료되기 전에 초대를 수락하지 않으면 초대가 자동으로 거부됩니다.

> **Important**
>
> 다음 목록에 없는 공유 리소스 유형의 경우 12시간 이내에 리소스 공유 참여 초대를 수락해야 합니다. 12시간이 경과하면 초대가 만료되고 리소스 공유의 최종 사용자 보안 주체가 연결 해제됩니다. 최종 사용자는 더 이상 초대를 수락할 수 없습니다.

- Amazon Aurora – DB 클러스터
- Amazon EC2 – 용량 예약 및 전용 호스트
- AWS License Manager – 라이선스 구성
- AWS Outposts – 로컬 게이트웨이 라우팅 테이블, outposts, 사이트
- Amazon Route 53 – 전달 규칙
- Amazon VPC - 고객 소유 IPv4 주소, 접두사 목록, 서브넷, 트래픽 미러 대상, 전송 게이트웨이, 전송 게이트웨이 멀티캐스트 도메인

Console

리소스 공유를 생성하려면

1. AWS RAM 콘솔을 엽니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), `us-east-1`로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요. 리소스 공유에 글로벌 리소스를 포함하려면 지정된 홈 리전인 미국 동부(버지니아 북부), `us-east-1`을 선택해야 합니다.
3. AWS RAM을 처음 사용하는 경우 홈 페이지에서 리소스 공유 생성을 선택합니다. 그렇지 않은 경우 내 공유: 리소스 공유 페이지에서 리소스 공유 생성을 선택합니다.
4. 1단계: 리소스 공유 세부 정보 지정에서 다음을 수행합니다.

   a. 이름에 리소스 공유를 설명하는 이름을 입력합니다.

   b. 리소스에서 다음과 같이 리소스 공유에 추가할 리소스를 선택합니다.

      - 리소스 유형 선택에서 공유할 리소스 유형을 선택합니다. 그러면 공유 가능한 리소스 목록이 선택한 유형의 리소스로만 필터링됩니다.

- 결과 리소스 목록에서 공유하려는 개별 리소스 옆의 확인란을 선택합니다. 선택한 리소스가 선택한 리소스 아래로 이동합니다.

  특정 가용 영역과 연결된 리소스를 공유하는 경우 가용 영역 ID(AZ ID)를 사용하면 여러 계정에서 이러한 리소스의 상대적 위치를 파악할 수 있습니다. 자세한 내용은 AWS 리소스의 가용 영역 ID 섹션을 참조하세요.

c. (선택 사항) 리소스 공유에 태그를 연결하려면 태그 아래에 태그 키와 값을 입력합니다. 새 태그 추가를 선택하여 다른 태그를 추가합니다. 필요에 따라 이 단계를 반복합니다. 이러한 태그는 리소스 공유 자체에만 적용되며 리소스 공유의 리소스에는 적용되지 않습니다.

5. 다음을 선택합니다.

6. 2단계: 각 리소스 유형과 관리형 권한 연결에서 AWS를 통해 생성된 관리형 권한을 리소스 유형과 연결하거나, 기존 고객 관리형 권한을 선택하거나, 지원되는 리소스 유형에 대해 고객 관리형 권한을 직접 생성할 수 있습니다. 자세한 내용은 관리형 권한의 유형 섹션을 참조하세요.

   고객 관리형 권한 생성을 선택하여 공유 사용 사례의 요구 사항을 충족하는 고객 관리형 권한을 구성합니다. 자세한 내용은 고객 관리형 정책 생성 섹션을 참조하세요. 프로세스를 완료한 후

   를 선택한 다음 관리형 권한 드롭다운 목록에서 새 고객 관리형 권한을 선택할 수 있습니다.

   > **Note**
   >
   > 선택한 관리형 권한에 여러 버전이 있는 경우 AWS RAM에서 자동으로 기본 버전을 연결합니다. 기본 버전으로 지정된 버전만 연결할 수 있습니다.

   관리형 권한에서 허용하는 작업을 표시하려면 이 관리형 권한에 대한 정책 템플릿 보기를 확장합니다.

7. 다음을 선택합니다.

8. 3단계: 보안 주체에 액세스 권한 부여에서 다음을 수행합니다.

   a. 기본적으로 누구에게나 공유 허용이 선택되어 있습니다. 즉, 이를 지원하는 리소스 유형의 경우 조직 외부에 있는 AWS 계정과 리소스를 공유할 수 있습니다. 이는 Amazon VPC 서브넷과 같이 조직 내에서만 공유할 수 있는 리소스 유형에는 영향을 주지 않습니다. 지원되는 일부 리소스 유형을 IAM 역할 및 사용자와 공유할 수도 있습니다.

리소스 공유를 조직 내 계정 및 보안 주체로만 제한하려면 조직 내에서만 공유 허용을 선택합니다.

b. 보안 주체에서 다음을 수행합니다.

- 조직, 조직 단위(OU) 또는 조직에 속한 AWS 계정을 추가하려면 조직 구조 표시를 켭니다. 그러면 조직의 트리 보기가 표시됩니다. 그런 다음 추가하려는 각 보안 주체 옆의 확인란을 선택합니다.

> **Important**
>
> 조직 또는 OU와 공유할 때 해당 범위에 리소스 공유를 소유한 계정이 포함되어 있으면 공유 계정의 모든 주체가 자동으로 공유의 리소스에 대한 액세스 권한을 얻게 됩니다. 부여된 액세스 권한은 공유와 연결된 관리형 권한에 의해 정의됩니다. 이는 AWS RAM에서 공유의 각 리소스에 연결한 리소스 기반 정책이 `"Principal": "*"`을 사용하기 때문입니다. 자세한 내용은 리소스 기반 정책에서 "Principal": "*" 사용 시 유의 사항 섹션을 참조하세요.
> 다른 소비 계정의 보안 주체는 공유 리소스에 즉시 액세스할 수 없습니다. 다른 계정의 관리자가 먼저 자격 증명 기반 권한 정책을 해당 보안 주체에 연결해야 합니다. 이러한 정책은 리소스 공유에 있는 개별 리소스의 ARN에 `Allow` 액세스 권한을 부여해야 합니다. 이러한 정책의 권한은 리소스 공유와 연결된 관리형 권한에 지정된 권한을 초과할 수 없습니다.

- 조직(ID가 `o-`로 시작)을 선택하면 조직 내 모든 AWS 계정의 보안 주체가 리소스 공유에 액세스할 수 있습니다.
- OU(ID가 `ou-`로 시작)를 선택하면 해당 OU와 하위 OU에 있는 모든 AWS 계정의 보안 주체가 리소스 공유에 액세스할 수 있습니다.
- 개별 AWS 계정을 선택하면 해당 계정에 있는 보안 주체만 리소스 공유에 액세스할 수 있습니다.

> **Note**
>
> 조직 구조 표시 토글은 AWS Organizations와의 공유가 활성화되어 있고 조직의 관리 계정에 로그인한 경우에만 나타납니다.

이 방법으로는 조직 외부의 AWS 계정이나 IAM 역할 또는 사용자를 지정할 수 없습니다. 대신 조직 구조 표시를 끄고 드롭다운 목록과 텍스트 상자를 사용하여 ID 또는 ARN을 입력해야 합니다.

- 조직 외부의 보안 주체를 포함하여 ID 또는 ARN으로 보안 주체를 지정하려면 각 보안 주체에 대해 보안 주체 유형을 선택합니다. 그런 다음 ID(AWS 계정, 조직 또는 OU의 경우) 또는 ARN(IAM 역할 또는 사용자의 경우)을 입력하고 추가를 선택합니다. 사용 가능한 보안 주체 유형, ID 및 ARN 형식은 다음과 같습니다.
  - AWS 계정 – AWS 계정을 추가하려면 12자리 계정 ID를 입력합니다. 예:

    ```
    123456789012
    ```

  - 조직 - 조직의 모든 AWS 계정을 추가하려면 조직 ID를 입력합니다. 예:

    ```
    o-abcd1234
    ```

  - 조직 단위(OU) - OU를 추가하려면 OU ID를 입력합니다. 예:

    ```
    ou-abcd-1234efgh
    ```

  - IAM 역할 - IAM 역할을 추가하려면 역할의 ARN을 입력합니다. 다음 구문을 사용합니다.

    ```
    arn:partition:iam::account:role/role-name
    ```

    예:

    ```
    arn:aws:iam::123456789012:role/MyS3AccessRole
    ```

    > **Note**
    >
    > IAM 역할의 고유 ARN을 가져오려면 IAM 콘솔에서 역할 목록을 확인하고 get-role AWS CLI 명령 또는 GetRole API 작업을 사용합니다.

  - IAM 사용자 - IAM 사용자를 추가하려면 사용자의 ARN을 입력합니다. 다음 구문을 사용합니다.

    ```
    arn:partition:iam::account:user/user-name
    ```

    예:

    ```
    arn:aws:iam::123456789012:user/bob
    ```

> **Note**
>
> IAM 사용자의 고유 ARN을 가져오려면 IAM 콘솔에서 사용자 목록을 확인하고 get-user AWS CLI 명령 또는 GetUser API 작업을 사용합니다.

- 서비스 보안 주체 - 서비스 보안 주체를 추가하려면 보안 주체 유형 선택 드롭박스에서 서비스 주체를 선택합니다. AWS 서비스 보안 주체의 이름을 입력합니다. 다음 구문을 사용합니다.
  - *service-id*.amazonaws.com

    예:

    pca-connector-ad.amazonaws.com

c. 선택한 보안 주체에서 지정한 보안 주체가 목록에 나타나는지 확인합니다.

9. 다음을 선택합니다.
10. 4단계: 검토 및 생성에서 리소스 공유에 대한 구성 세부 정보를 검토합니다. 단계 구성을 변경하려면 돌아가려는 단계에 해당하는 링크를 선택한 다음 필요한 사항을 변경합니다.
11. 리소스 공유 검토를 완료한 후 리소스 공유 생성을 선택합니다.

    리소스 및 보안 주체 연결이 완료되는 데 몇 분 정도 걸릴 수 있습니다. 이 프로세스가 완료될 때까지 기다렸다가 리소스 공유를 사용해 보세요.
12. 언제든지 리소스와 보안 주체를 추가 및 제거하거나 리소스 공유에 사용자 지정 태그를 적용할 수 있습니다. 기본 관리형 권한 이상을 지원하는 리소스 유형의 경우 리소스 공유에 포함된 리소스 유형의 관리형 권한을 변경할 수 있습니다. 리소스를 더 이상 공유하지 않으려는 경우 리소스 공유를 삭제할 수 있습니다. 자세한 내용은 내 소유의 AWS 리소스 공유 섹션을 참조하세요.

AWS CLI

리소스 공유를 생성하려면

create-resource-share 명령을 사용합니다. 다음 명령은 조직의 모든 AWS 계정과 공유되는 리소스 공유를 생성합니다. 공유에는 AWS License Manager 라이선스 구성이 포함되며 해당 리소스 유형에 대해 기본 관리형 권한이 부여됩니다.

> **Note**
>
> 이 리소스 공유의 리소스 유형과 함께 고객 관리형 권한을 사용하려는 경우 기존 고객 관리형 권한을 사용하거나 새 고객 관리형 권한을 생성할 수 있습니다. 고객 관리형 권한의 ARN을 기록해 둔 다음 리소스 공유를 생성합니다. 자세한 내용은 고객 관리형 정책 생성 섹션을 참조하세요.

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

AWS RAM에서 리소스 공유 업데이트

리소스 공유는 AWS RAM에서 언제든지 다음과 같은 방법으로 업데이트할 수 있습니다.

- 생성한 리소스 공유에 보안 주체, 리소스 또는 태그를 추가할 수 있습니다.
- 기본 AWS 관리형 권한 이상을 지원하는 리소스 유형의 경우 각 유형의 리소스에 적용할 관리형 권한을 선택할 수 있습니다.
- 리소스 공유에 연결된 관리형 권한에 새 기본 버전이 있는 경우 새 버전을 사용하도록 관리형 권한을 업데이트할 수 있습니다.

- 리소스 공유에서 보안 주체 또는 리소스를 제거하여 공유 리소스에 대한 액세스 권한을 취소할 수 있습니다. 액세스 권한을 취소하면 보안 주체가 더 이상 공유 리소스에 액세스할 수 없게 됩니다.

> **Note**
>
> 공유가 비어 있거나 리소스 공유 나가기를 지원하는 리소스 유형만 포함된 경우 리소스를 공유하는 보안 주체는 리소스 공유에서 나갈 수 있습니다. 리소스 공유에 나가기를 지원하지 않는 리소스 유형이 포함된 경우 공유 소유자에게 문의해야 한다는 메시지가 보안 주체에게 표시됩니다. 이 경우 리소스 공유의 소유자는 리소스 공유에서 보안 주체를 제거해야 합니다. 이 작업을 지원하지 않는 리소스 유형 목록은 리소스 공유에서 나가기 위한 사전 조건 섹션을 참조하세요.

Console

리소스 공유를 업데이트하려면

1. AWS RAM 콘솔에서 내 공유: 리소스 공유 페이지로 이동합니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), `us-east-1`로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 리소스 공유를 선택한 다음 수정을 선택합니다.
4. 1단계: 리소스 공유 세부 정보 지정에서 리소스 공유 세부 정보를 검토하고, 필요한 경우 다음 중 하나를 업데이트합니다.

   a. (선택 사항) 리소스 공유의 이름을 변경하려면 이름을 편집합니다.

   b. (선택 사항) 리소스 공유에 리소스를 추가하려면 리소스에서 리소스 유형을 선택한 다음 리소스 옆의 확인란을 선택하여 리소스 공유에 추가합니다. 글로벌 리소스는 AWS Management Console에서 리전을 미국 동부(버지니아 북부)(`us-east-1`)로 설정한 경우에만 나타납니다.

   c. (선택 사항) 리소스 공유에서 리소스를 제거하려면 선택한 리소스에서 리소스를 찾은 다음 리소스 ID 옆의 X를 선택합니다.

   d. (선택 사항) 리소스 공유에 태그를 추가하려면 태그 아래의 빈 텍스트 상자에 태그 키와 값을 입력합니다. 태그 키와 값 쌍을 두 개 이상 추가하려면 새 태그 추가를 선택합니다. 최대 50개의 태그를 추가할 수 있습니다.

e. 리소스 공유에서 태그를 제거하려면 태그에서 태그를 찾은 다음 옆에 있는 제거를 선택합니다.

5. 다음을 선택합니다.

6. (선택 사항) 2단계: 각 리소스 유형과 관리형 권한 연결에서 AWS를 통해 생성된 관리형 권한을 리소스 유형과 연결하거나, 기존 고객 관리형 권한을 선택하거나, 고객 관리형 권한을 직접 생성할 수 있습니다. 자세한 내용은 관리형 권한의 유형 섹션을 참조하세요.

   또한 고객 관리형 권한 생성을 선택하여 공유 사용 사례의 요구 사항을 충족하는 고객 관리형 권한을 구성할 수도 있습니다. 자세한 내용은 고객 관리형 정책 생성 섹션을 참조하세요. 프로세스를 완료한 후

   를 선택한 다음 관리형 권한 드롭다운 목록에서 새 고객 관리형 권한을 선택할 수 있습니다.

   관리형 권한에서 허용하는 작업을 표시하려면 이 관리형 권한에 대한 정책 템플릿 보기를 확장합니다.

7. 리소스 공유에 현재 할당된 관리형 권한 버전이 현재 기본 버전이 아닌 경우 기본 버전으로 업데이트를 선택하여 기본 버전으로 업데이트할 수 있습니다.

   > **Note**
   >
   > 마지막 단계 후 리소스 공유에 대한 변경 사항을 저장하기 전까지는 이전 버전으로 되돌리기를 선택하여 버전 업데이트를 취소할 수 있습니다. 하지만 AWS 관리형 권한의 경우 리소스 공유를 저장하면 변경 사항이 최종적으로 적용되므로 더 이상 이전 버전으로 되돌릴 수 없습니다.

8. 다음을 선택합니다.

9. 3단계: 액세스할 수 있는 보안 주체 선택에서 선택한 보안 주체를 검토하고, 필요한 경우 다음 중 하나를 업데이트합니다.

   a. (선택 사항) 조직 내부 또는 외부의 보안 주체와의 공유 사용 여부를 변경하려면 다음 옵션 중 하나를 선택합니다.

      - 조직 외부에 있는 AWS 계정 또는 개별 IAM 역할 또는 사용자와 리소스를 공유하려면 외부 보안 주체와의 공유 허용을 선택합니다.
      - AWS Organizations의 조직 내 보안 주체만 리소스를 공유하도록 제한하려면 조직 내의 보안 주체와만 공유 허용을 선택합니다.

b. 보안 주체에서 다음을 수행합니다.

- (선택 사항) 조직, 조직 단위(OU) 또는 멤버 AWS 계정을 조직 내에 추가하려면 조직 구조 표시를 켜서 조직의 트리 보기를 표시합니다. 그런 다음 추가하려는 각 보안 주체 옆의 확인란을 선택합니다.

> **Important**
>
> 조직 또는 OU와 공유할 때 해당 범위에 리소스 공유를 소유한 계정이 포함되어 있으면 공유 계정의 모든 주체가 자동으로 공유의 리소스에 대한 액세스 권한을 얻게 됩니다. 부여된 액세스 권한은 공유와 연결된 관리형 권한에 의해 정의됩니다. 이는 AWS RAM에서 공유의 각 리소스에 연결한 리소스 기반 정책이 `"Principal": "*"`을 사용하기 때문입니다. 자세한 내용은 리소스 기반 정책에서 "Principal": "*" 사용 시 유의 사항 섹션을 참조하세요.
> 다른 소비 계정의 보안 주체는 공유 리소스에 즉시 액세스할 수 없습니다. 다른 계정의 관리자가 먼저 자격 증명 기반 권한 정책을 해당 보안 주체에 연결해야 합니다. 이러한 정책은 리소스 공유에 있는 개별 리소스의 ARN에 `Allow` 액세스 권한을 부여해야 합니다. 이러한 정책의 권한은 리소스 공유와 연결된 관리형 권한에 지정된 권한을 초과할 수 없습니다.

> **Note**
>
> 조직 구조 표시 토글은 AWS Organizations와의 공유가 활성화되어 있고 조직의 관리 계정에 보안 주체로 로그인한 경우에만 나타납니다.
> 이 방법으로는 조직 외부의 AWS 계정이나 IAM 역할 또는 사용자를 지정할 수 없습니다. 대신 조직 구조 표시 스위치 아래의 텍스트 상자에 표시된 식별자를 입력하여 해당 보안 주체를 추가해야 합니다. 다음 항목을 참조하세요.

- (선택 사항) 식별자를 기준으로 보안 주체를 추가하려면 드롭다운 목록에서 보안 주체 유형을 선택한 다음 보안 주체의 ID 또는 ARN을 입력합니다. 마지막으로 추가를 선택합니다.

  개별 AWS 계정을 선택하면 해당 계정만 리소스 공유에 액세스할 수 있습니다. 다음 옵션 중 하나를 선택할 수 있습니다.

  - 다른 AWS 계정(리소스 소유자 제외) - 다른 계정에서 리소스를 사용할 수 있습니다. 해당 계정의 관리자는 자격 증명 기반 권한 정책을 사용하여 공유 리소스에 대한 액세

스 권한을 개별 역할 및 사용자에게 부여하여 프로세스를 완료해야 합니다. 이러한 권한은 리소스 공유에 연결된 관리형 권한에 정의된 권한을 초과할 수 없습니다.

- 이 AWS 계정(리소스 소유자) - 리소스 소유 계정의 모든 역할과 사용자는 리소스 공유에 연결된 관리형 권한으로 정의된 액세스 권한을 자동으로 받게 됩니다.

- 추가된 내용은 선택한 보안 주체 목록에 즉시 표시됩니다.

  그런 다음 이 단계를 반복하여 계정, OU 또는 조직을 추가할 수 있습니다.

- (선택 사항) 보안 주체를 제거하려면 선택한 보안 주체 아래에서 보안 주체를 찾아 해당 확인란을 선택한 다음 선택 취소를 선택합니다.

10. 다음을 선택합니다.
11. 4단계: 검토 및 업데이트에서 리소스 공유에 대한 구성 세부 정보를 검토합니다.
12. 단계 구성을 변경하려면 돌아가려는 단계에 해당하는 링크를 선택한 다음 필요한 사항을 변경합니다.

    관리형 권한이 여전히 기본 버전이 아닌 다른 버전을 사용하고 있는 경우에는 기본 버전으로 업데이트를 선택하여 이 문제를 해결할 수 있습니다.
13. 변경을 마치면 리소스 공유 업데이트를 선택합니다.

AWS CLI

리소스 공유를 업데이트하려면

다음 AWS CLI 명령을 사용하여 리소스 공유를 수정할 수 있습니다.

- 리소스 공유의 이름을 바꾸거나 외부 보안 주체의 허용 여부를 변경하려면 update-resource-share 명령을 사용합니다. 다음 예에서는 지정된 리소스 공유의 이름을 바꾸고 해당 조직의 보안 주체만 허용하도록 설정합니다. 리소스 공유가 포함된 AWS 리전에 대한 서비스 엔드포인트를 사용해야 합니다.

```
$ aws ram update-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --name "my-renamed-resource-share" \
    --no-allow-external-principals
{
    "resourceShare": {
```

```
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "name": "my-renamed-resource-share",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": false,
        "status": "ACTIVE",
        "creationTime": 1565295733.282,
        "lastUpdatedTime": 1565303080.023
    }
}
```

- 리소스 공유에 리소스를 추가하려면 associate-resource-share 명령을 사용합니다. 다음 예에서는 지정된 리소스 공유에 서브넷을 추가합니다.

```
$ aws ram associate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "ASSOCIATING",
        "external": false
    ]
}
```

- 리소스 공유에 리소스 유형에 대한 관리형 권한을 추가하거나 바꾸려면 list-permissions 및 associate-resource-share-permission 명령을 사용합니다. 리소스 공유의 리소스 유형당 하나의 관리형 권한만 할당할 수 있습니다. 이미 관리형 권한이 있는 리소스 유형에 관리형 권한을 추가하려는 경우 `--replace` 옵션을 포함해야 합니다. 그렇지 않으면 명령이 오류와 함께 실패합니다.

  다음 예제 명령은 Amazon Elastic Compute Cloud(Amazon EC2) 서브넷에 사용할 수 있는 관리형 권한에 대한 ARN을 나열한 다음 해당 ARN 중 하나를 사용하여 지정된 리소스 공유의 해당 리소스 유형에 대해 현재 할당된 AWS 관리형 권한을 대체합니다.

```
$ aws ram list-permissions \
    --resource-type ec2:Subnet
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMDefaultPermissionSubnet",
            "resourceType": "ec2:Subnet",
            "creationTime": "2020-02-27T11:38:26.727000-08:00",
            "lastUpdatedTime": "2020-02-27T11:38:26.727000-08:00"
        }
    ]
}
$ aws ram associate-resource-share-permission \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --permission-arn arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet
{
    "returnValue": true
}
```

- 리소스 공유에서 리소스를 제거하려면 disassociate-resource-share 명령을 사용합니다. 다음 예에서는 지정된 ARN을 사용하는 Amazon EC2 서브넷을 지정된 리소스 공유에서 제거합니다.

```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:ubnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "DISASSOCIATING",
        "external": false
```

```
    ]
}
```

- 리소스 공유에 연결된 태그를 수정하려면 tag-resource 및 untag-resource 명령을 사용합니다. 다음 예에서는 지정된 리소스 공유에 `project=lima` 태그를 추가합니다.

```
$ aws ram tag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tags key=project,value=lima
```

다음 예에서는 지정된 리소스 공유에서 키가 `project`인 태그를 제거합니다.

```
$ aws ram untag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tag-keys=project
```

태그 지정 명령은 성공해도 출력을 생성하지 않습니다.

AWS RAM에서 공유 리소스 보기

모든 리소스 공유에서 공유한 개별 리소스 목록을 볼 수 있습니다. 이 목록에서는 현재 공유 중인 리소스, 해당 리소스가 포함된 리소스 공유 수, 해당 리소스에 액세스할 수 있는 보안 주체 수를 확인할 수 있습니다.

Console

현재 공유 중인 리소스를 보려면

1. AWS RAM 콘솔에서 내 공유: 공유 리소스 페이지를 엽니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), `us-east-1`로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 각 공유 리소스에 대해 제공되는 정보는 다음과 같습니다.

- 리소스 ID – 리소스 ID입니다. 리소스 ID를 선택하면 기본 서비스 콘솔에서 리소스를 볼 수 있는 새 브라우저 탭이 열립니다.
- 리소스 유형 - 리소스의 유형입니다.
- 마지막 공유 날짜 - 리소스를 마지막으로 공유한 날짜입니다.
- 리소스 공유 - 리소스가 포함된 리소스 공유 수입니다. 리소스 공유 목록을 보려면 번호를 선택합니다.
- 보안 주체 - 리소스에 액세스할 수 있는 보안 주체 수입니다. 값을 선택하면 보안 주체를 확인할 수 있습니다.

AWS CLI

현재 공유 중인 리소스를 보려면

`--resource-owner` 파라미터를 SELF로 설정하여 list-resources 명령을 사용하면 현재 공유하고 있는 리소스에 대한 세부 정보를 표시할 수 있습니다.

다음 예에서는 호출 AWS 계정에 대해 AWS 리전(us-east-1)의 리소스 공유에 포함된 리소스를 보여줍니다. 다른 리전에서 공유하는 리소스를 가져오려면 `--region` *<region-code>* 파라미터를 사용합니다.

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner SELF
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:41.081000-07:00"
        },
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
```

```
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-07-22T11:48:11.104000-07:00",
            "lastUpdatedTime": "2021-07-22T11:48:11.971000-07:00"
        }
    ]
}
```

AWS RAM에서 내가 리소스를 공유하고 있는 보안 주체 보기

모든 리소스 공유에서 내가 리소스를 공유하고 있는 보안 주체를 확인할 수 있습니다. 보안 주체 목록을 확인하면 공유 리소스에 액세스할 수 있는 사람을 결정하는 데 도움이 됩니다.

Console

나와 리소스를 공유하고 있는 보안 주체를 보려면

1. AWS RAM 콘솔에서 내 공유: 보안 주체 페이지로 이동합니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), us-east-1로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 필터를 적용하여 특정 보안 주체를 찾습니다. 여러 필터를 적용하여 검색 범위를 좁힐 수 있습니다. 텍스트 상자를 선택하면 제안된 속성 필드의 드롭다운 목록이 표시됩니다. 하나를 선택한 후 해당 필드에 사용할 수 있는 값 목록에서 선택할 수 있습니다. 원하는 리소스를 찾을 때까지 다른 속성이나 키워드를 추가할 수 있습니다.
4. 목록에 있는 각 보안 주체에 대해 콘솔에 다음 정보가 표시됩니다.

   - 주체 ID - 보안 주체의 ID입니다. 소스 ID를 선택하면 기본 콘솔에서 보안 주체를 볼 수 있는 새 브라우저 탭이 열립니다.
   - 리소스 공유 - 지정된 보안 주체와 공유한 리소스 공유 수입니다. 숫자를 선택하면 리소스 공유 목록을 볼 수 있습니다.
   - 리소스 - 보안 주체와 공유한 리소스 수입니다. 숫자를 선택하면 공유 리소스 목록을 볼 수 있습니다.

AWS CLI

나와 리소스를 공유하고 있는 보안 주체를 보려면

list-principals 명령을 사용하면 호출 계정에 대해 현재 AWS 리전에 생성한 리소스 공유에서 참조하는 보안 주체 목록을 가져올 수 있습니다.

다음 예에서는 호출 계정의 기본 리전에 생성된 공유에 액세스할 수 있는 보안 주체를 나열합니다. 이 예에서 보안 주체는 호출 계정의 조직이며 서로 다른 두 리소스 공유의 일부인 별도의 AWS 계정입니다. 리소스 공유가 포함된 AWS 리전에 대한 서비스 엔드포인트를 사용해야 합니다.

```
$ aws ram list-principals \
    --region us-east-1 \
    --resource-owner SELF
{
    "principals": [
        {
            "id": "arn:aws:organizations::123456789012:organization/o-a1b2c3dr",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-09-14T20:40:58.532000-07:00",
            "lastUpdatedTime": "2021-09-14T20:40:59.610000-07:00",
            "external": false
        },
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/6405fa7c-0786-4e15-8c9f-8aec02802f18",
            "creationTime": "2021-09-15T15:00:31.601000-07:00",
            "lastUpdatedTime": "2021-09-15T15:14:13.618000-07:00",
            "external": true
        }
    ]
}
```

AWS RAM에서 리소스 공유 삭제

리소스 공유는 언제든지 삭제할 수 있습니다. 리소스 공유를 삭제하면 리소스 공유와 연결된 모든 보안 주체가 공유 리소스에 액세스할 수 없게 됩니다. 리소스 공유를 삭제해도 공유된 리소스는 삭제되지 않습니다.

> **AWS 리소스를 삭제하려면**
>
> 리소스 공유에 포함된 AWS 리소스를 삭제해야 하는 경우 AWS에서는 먼저 해당 리소스가 포함된 리소스 공유에서 리소스를 제거하거나 리소스 공유를 삭제할 것을 권장합니다.

삭제된 리소스 공유는 삭제 후 AWS RAM 콘솔에 잠시 동안 계속 표시되지만 상태가 `Deleted`로 변경됩니다.

Console

리소스 공유를 삭제하려면

1. AWS RAM 콘솔에서 내 공유: 리소스 공유 페이지를 엽니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), `us-east-1`로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 삭제할 리소스 공유를 선택합니다.

   > **Warning**
   >
   > 올바른 리소스 공유를 선택해야 합니다. 리소스 공유를 삭제한 후에는 복구할 수 없습니다.

4. 삭제를 선택한 다음 확인 창에서 삭제를 선택합니다.
5. 삭제된 리소스 공유는 2시간 후에 사라집니다. 그때까지 콘솔에 삭제됨 상태로 표시됩니다.

AWS CLI

리소스 공유를 삭제하려면

delete-resource-share 명령을 사용하여 더 이상 필요하지 않은 리소스 공유를 삭제할 수 있습니다.

다음 예에서는 먼저 get-resource-shares 명령을 사용하여 삭제하려는 리소스 공유의 Amazon 리소스 이름(ARN) 을 가져옵니다. 그런 다음 delete-resource-share를 사용하여 지정된 리소스 공유를 삭제합니다.

```
$ aws ram get-resource-shares \
```

```
    --region us-east-1 \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
$ aws ram delete-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425
{
    "returnValue": true
}
```

나와 공유된 AWS 리소스에 액세스

AWS Resource Access Manager (AWS RAM) 를 사용하면 추가한 리소스 공유, 액세스할 수 있는 공유 리소스, 공유 리소스가 AWS 계정 있는 리소스를 볼 수 있습니다. 공유 리소스에 더 이상 액세스할 필요가 없는 경우 리소스 공유에서 나갈 수도 있습니다.

내용

리소스 공유 초대 수락 및 거부

공유 리소스에 액세스하려면 리소스 공유 소유자가 사용자를 보안 주체로 추가해야 합니다. 소유자는 다음 중 하나를 리소스 공유에 보안 주체로 추가할 수 있습니다.

- 사용자 계정이 속한 조직
- 사용자 계정이 포함된 조직 단위(OU)
- 개별 계정
- 지원되는 리소스 유형의 경우, 특정 IAM 역할 또는 사용자

내 기관의 구성원을 통해 리소스 공유에 추가되고 기관 내 공유가 활성화된 경우 초대를 수락하지 않고도 공유 리소스에 자동으로 접근할 수 있습니다. AWS 계정 AWS Organizations 또한 서비스 주체는 초대를 수락하지 않고도 공유 리소스에 자동으로 액세스할 수 있습니다. 액세스 권한을 받을 때 사용한 계정이 나중에 조직에서 제거되면 해당 계정의 모든 보안 주체는 해당 리소스 공유를 통해 액세스한 리소스에 자동으로 액세스할 수 없게 됩니다.

다음 방법 중 하나를 통해 리소스 공유에 추가된 사용자에게는 리소스 공유에 참여하라는 초대가 발송됩니다.

- 조직 외부의 계정 AWS Organizations
- 조직 내 계정 (공유 시) 이 AWS Organizations 활성화되지 않은 경우

리소스 공유에 참여하라는 초대를 받은 경우 초대를 수락해야 공유 리소스에 액세스할 수 있습니다. 초대를 거부하면 공유 리소스에 액세스할 수 없습니다.

다음 리소스 유형의 경우 7일 이내에 공유 참여 초대를 수락해야 합니다. 만료되기 전에 초대를 수락하지 않으면 초대가 자동으로 거부됩니다.

> **Important**
>
> 다음 목록에 없는 공유 리소스 유형의 경우 12시간 이내에 리소스 공유 참여 초대를 수락해야 합니다. 12시간이 경과하면 초대가 만료되고 리소스 공유의 최종 사용자 보안 주체가 연결 해제됩니다. 최종 사용자는 더 이상 초대를 수락할 수 없습니다.

- Amazon Aurora – DB 클러스터

- Amazon EC2 – 용량 예약 및 전용 호스트
- AWS License Manager — 라이선스 구성
- AWS Outposts — 로컬 게이트웨이 라우팅 테이블, 아웃포스트, 사이트
- Amazon Route 53 – 전달 규칙
- Amazon VPC - 고객 소유 IPv4 주소, 접두사 목록, 서브넷, 트래픽 미러 대상, 전송 게이트웨이, 전송 게이트웨이 멀티캐스트 도메인

Console

리소스 공유 초대에 응답하려면

1. AWS RAM 콘솔의 Shared with me: 리소스 공유 페이지로 이동합니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전 영역에 존재하므로 콘솔 오른쪽 상단의 드롭다운 AWS 리전 목록에서 적절한 것을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 를 미국 동부 (버지니아 북부), () AWS 리전 로 설정해야 합니다. `us-east-1` 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 추가한 리소스 공유 목록을 검토합니다.

   상태 열은 리소스 공유에 대한 현재 참여 상태를 나타냅니다. `Pending` 상태는 리소스 공유에 추가되었지만 아직 초대를 수락하거나 거부하지 않았음을 나타냅니다.
4. 리소스 공유 초대에 응답하려면 리소스 공유 ID를 선택하고 리소스 공유 수락을 선택하여 초대를 수락하거나 리소스 공유 거부를 선택하여 초대를 거부합니다. 초대를 거부하면 리소스에 액세스할 수 없습니다. 초대를 수락하면 리소스에 액세스할 수 있습니다.

AWS CLI

리소스 공유 초대에 응답하려면

다음 명령을 사용하여 리소스 공유에 대한 초대를 수락하거나 거부할 수 있습니다.

- get-resource-share-invitations
- accept-resource-share-invitation
- reject-resource-share-invitation

1. 다음 예제는 get-resource-share-invitations명령을 사용하여 사용자가 사용할 수 있는 모든 초대 목록을 검색하는 것으로 시작합니다. AWS 계정 이 AWS CLI `query` 매개 변수를 사용하면 출

력을 로 설정된 초대장으로만 제한할 수 있습니다. `status` `PENDING` 이 예에서는 지정된 AWS 리전의 현재 계정 123456789012에 대해 111111111111 계정에서 보낸 한 개의 초대가 현재 `PENDING` 상태임을 보여줍니다.

```
$ aws ram get-resource-share-invitations \
    --region us-east-1 \
    --query 'resourceShareInvitations[?status==`PENDING`]'
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
            "resourceShareName": "Test TrngAcct Resource Share",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/c4506c70-df75-4e6c-ac30-42ca03295a37",
            "senderAccountId": "111111111111",
            "receiverAccountId": "123456789012",
            "invitationTimestamp": "2021-09-21T08:56:24.977000-07:00",
            "status": "PENDING"
        }
    ]
}
```

2. 수락하려는 초대를 찾은 후에는 다음 명령에서 초대를 수락할 때 사용할 수 있도록 출력의 `resourceShareInvitationArn`을 기록해 둡니다.

```
$ aws ram accept-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "ACCEPTED"
```

```
    }
}
```

성공하면 응답에서 `status`가 `PENDING`에서 `ACCEPTED`로 변경되었음을 알 수 있습니다.

대신 초대를 거부하려면 동일한 매개 변수를 reject-resource-share-invitation사용하여 명령을 실행하십시오.

```
$ aws ram reject-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111111111111:resource-share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "REJECTED"
    }
}
```

공유 받은 리소스 공유 보기

액세스 권한이 있는 리소스 공유를 볼 수 있습니다. 어떤 보안 주체가 나와 리소스를 공유하고 있으며, 어떤 리소스를 공유하고 있는지 확인할 수 있습니다.

Console

리소스 공유를 보려면

1. AWS RAM 콘솔에서 나와 공유: 리소스 공유 페이지로 이동합니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS

리전을 미국 동부(버지니아 북부), us-east-1로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.

3. (선택 사항) 필터를 적용하여 특정 리소스 공유를 찾습니다. 여러 필터를 적용하여 검색 범위를 좁힐 수 있습니다. 리소스 공유 이름의 일부와 같은 키워드를 입력하여 이름에 해당 텍스트가 포함된 리소스 공유만 나열할 수 있습니다. 텍스트 상자를 선택하면 제안된 속성 필드의 드롭다운 목록이 표시됩니다. 하나를 선택한 후 해당 필드에 사용할 수 있는 값 목록에서 선택할 수 있습니다. 원하는 리소스를 찾을 때까지 다른 속성이나 키워드를 추가할 수 있습니다.
4. AWS RAM 콘솔에 다음과 같은 정보가 표시됩니다.

   - 이름 – 리소스 공유의 이름입니다.
   - ID – 리소스 공유 ID입니다. ID를 선택하면 리소스 공유에 대한 세부 정보 페이지를 볼 수 있습니다.
   - 소유자 - 리소스 공유를 AWS 계정의 ID입니다.
   - 상태 - 리소스 공유의 현재 상태입니다. 가능한 값은 다음과 같습니다.
     - Active – 리소스 공유가 활성화되어 사용 가능합니다.
     - Deleted – 리소스 공유가 삭제되어 더 이상 사용할 수 없습니다.
     - Pending 중 - 리소스 공유를 수락하라는 초대가 응답을 기다리고 있습니다.

AWS CLI

리소스 공유를 보려면

--resource-owner 파라미터를 OTHER-ACCOUNTS로 설정한 상태에서 get-resource-shares 명령을 사용합니다.

다음 예에서는 다른 AWS 계정을 통해 호출 계정과 지정된 AWS 리전에서 공유되는 리소스 공유 목록을 보여줍니다.

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Env Shared Licenses",
            "owningAccountId": "111111111111",
```

```
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:222222222222:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
            "name": "Prod Env Shared Subnets",
            "owningAccountId": "222222222222",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:56:24.737000-07:00",
            "lastUpdatedTime": "2021-09-21T08:56:24.737000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```


공유 받은 리소스 보기

액세스 가능한 공유 리소스를 볼 수 있습니다. 어떤 보안 주체가 나와 리소스를 공유하고 있으며, 어떤 리소스 공유에 해당 리소스가 포함되어 있는지 확인할 수 있습니다.

Console

공유 받은 리소스를 보려면

1. AWS RAM 콘솔에서 나와 공유: 공유 리소스 페이지로 이동합니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), us-east-1로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 필터를 적용하여 특정 공유 리소스를 찾습니다. 여러 필터를 적용하여 검색 범위를 좁힐 수 있습니다.
4. 다음 정보를 사용할 수 있습니다.

   - 리소스 ID – 리소스 ID입니다. 리소스 ID를 선택하면 서비스 콘솔에서 볼 수 있습니다.
   - 리소스 유형 - 리소스의 유형입니다.

- 마지막 공유 날짜 - 리소스가 공유된 날짜입니다.
- 리소스 공유 - 리소스가 포함되어 있는 리소스 공유 수입니다. 값을 선택하면 리소스 공유를 볼 수 있습니다.
- 소유자 ID - 리소스를 소유하고 있는 주체의 ID입니다.

AWS CLI

공유 받은 리소스를 보려면

list-resources 명령을 사용하여 공유 받은 리소스를 볼 수 있습니다.

다음 예제 명령은 다른 AWS 계정에서 지정된 AWS 리전에 지정된 리소스 공유를 통해 액세스할 수 있는 리소스에 대한 세부 정보를 표시합니다.

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:111111111111:license-
configuration:lic-36be0485f5ae379cc74cf8e9242ab143",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "status": "AVAILABLE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:42.517000-07:00"
        }
    ]
}
```

나와 공유하고 있는 보안 주체 보기

나와 리소스를 공유하고 있는 모든 보안 주체의 목록을 확인할 수 있습니다. 이들이 공유하고 있는 리소스와 리소스 공유를 확인할 수 있습니다.

Console

나와 리소스를 공유하고 있는 보안 주체를 확인하려면

1. AWS RAM 콘솔(https://console.aws.amazon.com/ram)을 엽니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), us-east-1로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 탐색 창에서 나와 공유, 보안 주체를 선택합니다.
4. (선택 사항) 필터를 적용하여 특정 보안 주체를 찾을 수 있습니다. 여러 필터를 적용하여 검색 범위를 좁힐 수 있습니다.
5. 콘솔에 다음과 같은 정보가 표시됩니다.
   - 보안 주체 ID - 나와 공유하고 있는 보안 주체의 ID입니다.
   - 리소스 공유 - 보안 주체가 나를 추가한 리소스 공유 수입니다. 숫자를 선택하면 리소스 공유 목록을 볼 수 있습니다.
   - 리소스 - 보안 주체가 나와 공유하고 있는 리소스 수입니다. 값을 선택하면 리소스 목록을 볼 수 있습니다.

AWS CLI

나와 리소스를 공유하고 있는 보안 주체를 확인하려면

list-principals 명령을 사용하여 내 AWS 계정과 리소스를 공유하고 있는 보안 주체 목록을 검색할 수 있습니다.

다음 예제 명령은 지정된 AWS 리전에서 작업을 호출하는 데 사용된 계정과 리소스 공유를 공유한 AWS 계정에 대한 세부 정보를 표시합니다.

```
$  aws ram list-principals \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "principals": [
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
```

```
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T09:06:25.545000-07:00",
            "external": true
        }
    ]
}
```

리소스 공유 나가기

공유 받은 리소스에 더 이상 액세스할 필요가 없는 경우 언제든지 리소스 공유에서 나갈 수 있습니다. 리소스 공유에서 나가면 공유 리소스에 액세스할 수 없게 됩니다.

리소스 공유에서 나가기 위한 사전 조건

- 리소스 공유가 조직 컨텍스트가 아닌 개별 AWS 계정로 공유된 경우에만 리소스 공유에서 나갈 수 있습니다. 사용자가 조직 내 AWS 계정을 통해 리소스 공유에 추가되었으며 AWS Organizations와의 공유가 활성화된 경우에는 리소스 공유에서 나갈 수 없습니다. 조직 내 리소스 공유에 대한 액세스는 자동으로 이루어집니다.
- 리소스 공유에서 나가려면 리소스 공유가 비어 있거나 공유 나가기를 지원하는 리소스 유형만 포함되어 있는지 확인합니다.

  다음은 리소스 공유 나가기를 지원하는 리소스 유형입니다.

서비스	리소스 유형
Amazon Aurora	`rds:Cluster`

Amazon EC2	`ec2:CapacityReservation`
	
	`ec2:DedicatedHost`

AWS License Manager	`license-manager:LicenseConfiguration`

AWS Outposts	`ec2:LocalGatewayRouteTable`
	
	`outposts:Outpost`
	
	`outposts:Site`

서비스	리소스 유형
Amazon Route 53	`route53resolver:ResolverRule`

Amazon VPC	`ec2:CoipPool`
	`ec2:PrefixList`
	`ec2:Subnet`
	`ec2:TrafficMirrorTarget`
	`ec2:TransitGateway`
	`ec2:TransitGatewayMulticastDomain`

리소스 공유에서 나가는 방법

Console

리소스 공유에서 나가려면

1. AWS RAM 콘솔에서 나와 공유: 리소스 공유 페이지로 이동합니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), `us-east-1`로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요.
3. 나가려는 리소스 공유를 선택합니다.
4. 리소스 공유 나가기를 선택하고 확인 대화 상자에서 나가기를 선택합니다.

AWS CLI

리소스 공유에서 나가려면

disassociate-resource-share 명령을 사용하면 리소스 공유에서 나갈 수 있습니다.

다음 예제 명령을 실행하면 명령을 호출하는 AWS 계정이 ARN으로 지정된 리소스 공유가 공유하는 리소스에 액세스할 수 없게 됩니다. 나가려는 리소스 공유가 포함된 AWS 리전의 서비스 엔드포인트로 요청을 보내야 합니다.

1. 먼저 리소스 공유 목록을 검색하여 나가려는 리소스 공유의 ARN을 검색합니다.

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Environment Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

2. 그런 다음 명령을 실행하여 해당 리소스 공유에서 나갈 수 있습니다. 또한 111111111111 계정에서 공유하는 지정된 리소스 공유에서 연결을 해제하려면 계정 ID 123456789012를 공유 주체로 지정해야 합니다.

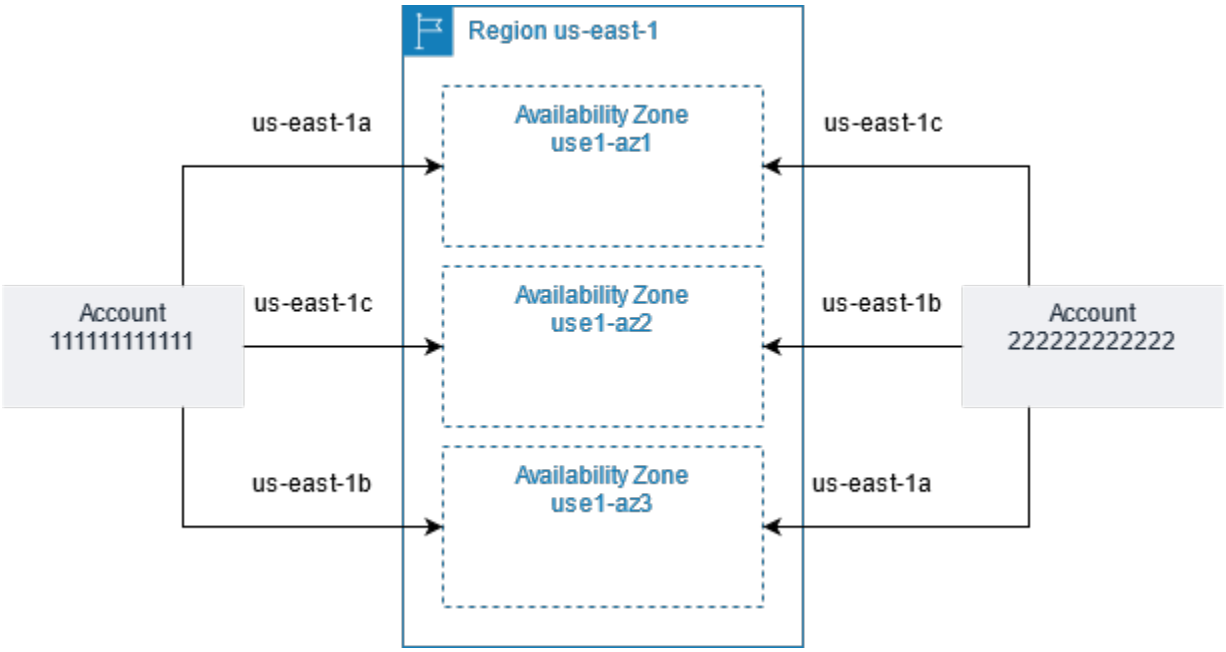
```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
    --principals 123456789012
                        {
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "associatedEntity": "123456789012",
            "associationType": "PRINCIPAL",
            "status": "DISASSOCIATING",
```

```
            "external": false
        }
    ]
}
```

AWS 리소스의 가용 영역 ID

AWS는 물리적 가용 영역을 각 AWS 계정의 가용 영역 이름에 무작위로 매핑합니다. 이 접근 방식을 사용하면 리소스를 각 리전의 가용 영역 "a"에 집중적으로 배치하는 대신 AWS 리전 리전의 가용 영역 전체에 분산시킬 수 있습니다. 따라서 현재 AWS 계정의 가용 영역 `us-east-1a`는 다른 AWS 계정의 `us-east-1a`와 동일한 물리적 위치를 나타내지 않을 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서에서 리전 및 가용 영역을 참조하세요.

다음 그림은 가용 영역 이름은 계정마다 다르게 매핑될 수 있지만 AZ ID는 모든 계정에서 동일하다는 것을 보여줍니다.



일부 리소스의 경우 AWS 리전뿐만 아니라 가용 영역도 식별해야 합니다. Amazon VPC 서브넷을 예로 들 수 있습니다. 단일 계정 내에서 가용 영역을 특정 이름에 매핑하는 것은 중요하지 않습니다. 하지만 AWS RAM을 사용하여 이러한 리소스를 다른 AWS 계정과 공유하는 경우에는 매핑이 중요합니다. 이러한 무작위 매핑은 공유 리소스에 액세스하는 계정이 참조할 가용 영역을 파악하는 것을 복잡하게 만듭니다. 이를 돕기 위해 이러한 리소스의 경우 AZ ID를 사용하여 계정과 관련된 리소스의 실제 위치를 식별할 수도 있습니다. AZ ID는 AWS 계정 전체에서 가용 영역에 대한 고유하고 일관된 식별자입니다.

예를 들어, use1-az1은 us-east-1 리전의 가용 영역 AZ ID이고 모든 AWS 계정에서 동일한 물리적 위치를 나타냅니다.

AZ ID를 사용하면 다른 계정의 리소스를 기준으로 한 계정의 리소스 위치를 확인할 수 있습니다. 예를 들어 AZ ID가 use1-az2인 가용 영역의 서브넷을 다른 계정과 공유하면 이 서브넷은 AZ ID가 use1-az2인 가용 영역의 계정에서 사용할 수 있습니다. 각 서브넷의 AZ ID는 Amazon VPC 콘솔에 표시되며, AWS CLI를 사용하여 쿼리할 수 있습니다.

Console

계정의 가용 영역에 대한 AZ ID를 보려면

1. AWS RAM 콘솔에서 AWS RAM 콘솔 페이지로 이동합니다.
2. AZ ID에서 현재 AWS 리전의 AZ ID를 확인할 수 있습니다.

AWS CLI

계정의 가용 영역에 대한 AZ ID를 보려면

다음 예제 명령은 us-west-2 리전의 가용 영역에 대한 AZ ID와 이 ID가 호출 AWS 계정에 매핑되는 방식을 보여줍니다.

```
$ aws ec2 describe-availability-zones \
    --region us-west-2
{
    "AvailabilityZones": [
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2a",
            "ZoneId": "usw2-az2",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
```

```
            "ZoneName": "us-west-2b",
            "ZoneId": "usw2-az1",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2c",
            "ZoneId": "usw2-az3",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2d",
            "ZoneId": "usw2-az4",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        }
    ]
}
```

공유 가능한 리소스 AWS

AWS Resource Access Manager (AWS RAM) 를 사용하면 다른 사람이 생성하고 관리하는 리소스를 공유할 수 AWS 서비스있습니다. 리소스를 개인과 공유할 수 AWS 계정있습니다. AWS Organizations 내 조직 또는 조직 단위(OU)의 계정과 리소스를 공유할 수도 있습니다. 지원되는 일부 리소스 유형에서는 리소스를 개별 AWS Identity and Access Management (IAM) 역할 및 사용자와 공유할 수도 있습니다.

다음 섹션에는 사용별로 공유할 수 있는 리소스 유형이 그룹별로 AWS 서비스나열되어 있습니다. AWS RAM이 표의 열은 각 리소스 유형이 지원하는 기능을 지정합니다.

IAM 사용자 및 역할과 공유 가능	 예. 계정뿐 아니라 개인 AWS Identity and Access Management (IAM) 역할 및 사용자와도 이 유형의 리소스를 공유할 수 있습니다.  아니요 – 이 유형의 리소스는 계정과만 공유할 수 있습니다.
조직 외부 계정과 공유 가능	 예 – 이 유형의 리소스는 조직 내부 또는 외부의 개별 계정과만 공유할 수 있습니다. 자세한 내용은 고려 사항을 참조하세요.  아니요 – 이 유형의 리소스는 동일한 조직의 멤버인 계정과만 공유할 수 있습니다.

고객 관리형 권한 사용 가능	지원되는 모든 리소스 유형은 AWS 관리 권한을 AWS RAM 지원하지만 이 열에 '예'가 표시되면 고객 관리 권한도 이 리소스 유형에 대해 지원된다는 의미입니다.  예 – 이 유형의 리소스는 고객 관리형 권한 사용을 지원합니다.  아니요 – 이 유형의 리소스는 고객 관리형 권한 사용을 지원하지 않습니다.
서비스 보안 주체와 공유 가능	 예 – 이 유형의 리소스를 AWS 서비스와 공유할 수 있습니다.  아니요 – 이 유형의 리소스를 AWS 서비스와 공유할 수 없습니다.

AWS App Mesh

를 사용하여 다음 AWS App Mesh 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
메시 appmesh:Mesh	메시를 중앙에서 생성하여 관리하고 다른 AWS 계정 또는 조직과 공유합니다. 공유 메시를 사용하면 서로 다른 리소스에서 만든 리소스가 동일한 메시에서 서로 AWS 계정 통신할 수 있습니다. 자세한 내용은 AWS App Mesh 사용 설명서에서 공유 메시 작업을 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

AWS AppSync GraphQL API

를 사용하여 다음과 같은 AWS AppSync GraphQL API 리소스를 공유할 수 있습니다. AWS RAM

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
GraphyQL API appsync:Apis	AWS AppSync GraphQL API를 중앙에서 관리하고 다른 사람 또는 조직과 공유하세요. AWS 계정 이를 통해 동일한 지역의 여러 계정에 있는 여러 하위 스키마 AWS AppSync API의 데이터에 액세스	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	할 수 있는 통합 AWS AppSync 병합 API를 만드는 과정에서 여러 계정이 API를 공유할 수 있습니다. 자세한 내용은 개발자 안내서의 병합된 API를 참조하십시오. AWS AppSync				

Amazon Aurora

AWS RAM을 사용하여 다음과 같은 Amazon Aurora 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
DB 클러스터 `rds:Cluster`	DB 클러스터를 중앙에서 생성하여 관리하고 다른 AWS 계정 또는 조직과 공유합니다. 이를 통해 중앙 관리형 공유 DB 클러스터를 여러 AWS 계정 에서 복제할 수 있습니다. 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora를 사용한 AWS RAM 계정 간 복제를 참조하십시오.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

AWS Private Certificate Authority

를 사용하여 다음 AWS Private CA 리소스를 공유할 수 있습니다. AWS RAM

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
사설 인증 기관 (CA) `acm-pca:CertificateAuthority`	조직의 내부 PKI (공개 키 인프라) 를 위한 사설 인증 기관 (CA) 을 생성 및 관리하고 이러한 CA를 다른 사람 AWS 계정 또는 조직과 공유하십시오. 이렇게 하면 다른 계정의 AWS Certificate Manager 사용자가 공유 CA에서 서명한 X.509 인증서를 발급할 수 있습니다. 자세한 내용은 AWS Private Certificate Authority 사용 설명서에서 프라이빗 CA에 대한 액세스 제어를 참조하세요.	 예	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 예

아마존 DataZone

를 사용하여 다음 DataZone 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
DataZone 도메인 `datazone:Domain`	도메인을 중앙에서 생성하여 관리하고 다른 AWS 계정 또는 조직과 공유합니다. 이렇게 하면 여러 계정이 Amazon DataZone 도메인을 생성할 수 있습니다. 자세한 내용은 Amazon DataZone 사용 설명서의 DataZone Amazon이란 무엇입니까? 를 참조하십시오.	아니요	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

AWS CodeBuild

를 사용하여 다음 AWS CodeBuild 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
프로젝트 `codebuild:Project`	프로젝트를 생성한 후 이를 사용하여 빌드를 실행합니다. 프로젝트를 다른 사람 AWS 계정 또는 조직과 공유하세요. 이를 통해 여러 AWS 계정 과 사용자가 프로젝트에 대한 정보를 확인하고 빌드를 분석할 수	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	있습니다. 자세한 내용은 AWS CodeBuild 사용 설명서에서 공유 프로젝트 작업을 참조하세요.				
보고서 그룹 codebuild:ReportGroup	보고서 그룹을 생성하고 프로젝트를 빌드할 때 이 그룹을 사용하여 보고서를 생성합니다. 보고서 그룹을 다른 사람 AWS 계정 또는 조직과 공유하세요. 이렇게 하면 여러 AWS 계정 명의 사용자가 보고서 그룹과 해당 보고서, 각 보고서의 테스트 사례 결과를 볼 수 있습니다. 보고서는 생성 후 30일 동안 볼 수 있으며, 그 이후에는 만료되어 더 이상 볼 수 없습니다. 자세한 내용은AWS CodeBuild 사용 설명서에서 공유 프로젝트 작업을 참조하세요.	 여	 여 모든 AWS 계정과 공유할 수 있습니다.	 여	 아니요

Amazon EC2

AWS RAM을 사용하여 다음과 같은 Amazon EC2 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
용량 예약 `ec2:CapacityReservation`	용량 예약을 중앙에서 생성 및 관리하고 예약된 용량을 다른 사람 AWS 계정 또는 조직과 공유할 수 있습니다. 이를 통해 여러 사람이 중앙에서 관리되는 예약 용량으로 Amazon EC2 인스턴스를 AWS 계정 시작할 수 있습니다. 자세한 정보는 Linux 인스턴스용 Amazon EC2 사용 설명서에서 공유 용량 예약 작업을 참조하세요. **Important** 용량 예약 공유를 위한 사전 조건을 모두 충족하지 못하면 공유 작업이 실패할 수 있습니다. 이 경우 사용자가 Amazon EC2 인스턴스를 해당 용량 예약으로 시작하려고 하면 인스턴스가 온디맨드 인스턴스로	아니요	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	시작되어 비용이 더 많이 발생할 수 있습니다. Amazon EC2 콘솔에서 공유 용량 예약을 확인하여 해당 예약에 액세스할 수 있는지 확인하는 것이 좋습니다. 리소스 공유에 실패한 경우를 모니터링하여 사용자가 비용을 높일 수 있는 방식으로 인스턴스를 시작하기 전에 수정 조치를 취할 수 있습니다. 자세한 정보는 예: 리소스 공유 실패에 대한 알림을 참조하세요.				

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
전용 호스트 ec2:DedicatedHost	Amazon EC2 전용 호스트를 중앙에서 할당 및 관리하고 호스트의 인스턴스 용량을 AWS 계정 다른 사람 또는 조직과 공유하십시오. 이를 통해 여러 사람이 중앙에서 관리되는 전용 호스트에서 Amazon EC2 인스턴스를 AWS 계정 시작할 수 있습니다. 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서에서 공유 전용 호스트 작업을 참조하세요.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요
배치 그룹 ec2:PlacementGroup	소유하고 있는 배치 그룹을 조직 내부 및 외부에서 공유할 수 있습니다. AWS 계정공유하는 계정 중 하나에서 공유 배치 그룹으로 Amazon EC2 인스턴스를 시작할 수 있습니다. 자세한 내용을 알아보려면 Linux 인스턴스용 Amazon EC2 사용 설명서에서 배치 그룹 공유를 참조하세요.	 예	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

EC2 Image Builder

AWS RAM을 사용하여 다음과 같은 EC2 Image Builder 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
구성 요소 `imagebuilder:Component`	구성 요소를 중앙에서 생성하여 관리하고 다른 AWS 계정 또는 조직과 공유합니다. 이미지 레시피에서 미리 정의된 빌드 및 테스트 구성 요소를 사용할 수 있는 사용자를 관리합니다. 자세한 내용은 EC2 Image Builder 사용 설명서에서 Share EC2 Image Builder resources를 참조하세요.	 예	 예 모든 AWS 계정과 공유할 수 있습니다.	 예	 아니요
컨테이너 레시피 `imagebuilder:ContainerRecipe`	컨테이너 레시피를 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하세요. 이를 통해 미리 정의된 문서를 사용하여 컨테이너 이미지 빌드를 복제할 수 있는 사용자를 관리할 수 있습니다. 자세한 내용은 EC2 Image Builder 사용 설명서에서 EC2 Image Builder 리소스 공유를 참조하세요.	 예	 예 모든 AWS 계정과 공유할 수 있습니다.	 예	 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
이미지 `imagebuilder:Image`	골든 이미지를 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하세요. 조직 전체에서 EC2 Image Builder로 생성한 이미지를 사용할 수 있는 사용자를 관리합니다. 자세한 내용은 EC2 Image Builder 사용 설명서에서 EC2 Image Builder 리소스 공유를 참조하세요.	 예	 예 모든 AWS 계정과 공유할 수 있습니다.	 예	 아니요
이미지 레시피 `imagebuilder:ImageRecipe`	이미지 레시피를 중앙에서 작성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하세요. 이를 통해 미리 정의된 문서를 사용하여 AMI 빌드를 복제할 수 있는 사용자를 관리할 수 있습니다. 자세한 내용은 EC2 Image Builder 사용 설명서에서 EC2 Image Builder 리소스 공유를 참조하세요.	 예	 예 모든 AWS 계정과 공유할 수 있습니다.	 예	 아니요

Amazon FSx for OpenZFS

AWS RAM을 사용하여 다음과 같은 Amazon FSx for OpenZFS 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
FSx 볼륨 `fsx:Volume`	FSX for OpenZFS 볼륨을 중앙에서 생성 및 관리하고 다른 사용자 또는 조직과 공유하십시오. AWS 계정 이를 통해 여러 계정이 `CreateVolume` FSx API 또는 를 통해 공유 볼륨의 OpenZfs 스냅샷을 사용하여 데이터 복제를 수행할 수 있습니다. `CopySnapshotAndUpdateVolume` 자세한 내용은 Amazon FSx for OpenZFS 사용 설명서의 온디맨드 데이터 복제를 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

AWS Glue

를 사용하여 다음 AWS Glue 리소스를 공유할 수 있습니다. AWS RAM

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
데이터 카탈로그 `glue:Catalog`	중앙 데이터 카탈로그를 관리하고 데이터베이스 및 테이블에 대한 메타데이터를 조직 AWS 계정 또는 조직과 공유하십시오. 이를 통해 사용자는 여러 계정의 데이터에 대해 쿼리를 실행할 수 있습니다. 자세한 내용은AWS Lake Formation 개발자 안내서에서 AWS 계정 간에 데이터 카탈로그 테이블 및 데이터베이스 공유를 참조하세요.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요
데이터베이스 수 `glue:Database`	데이터 카탈로그 데이터베이스를 중앙에서 생성 및 관리하고, 이를 조직 AWS 계정 또는 조직과 공유하세요. 데이터베이스는 데이터 카탈로그 테이블 모음입니다. 이를 통해 사용자는 여러 계정 간에 데이터를 결합하고 쿼리할 수 있는 쿼리 및 추출, 전환, 적재(ETL) 작업을 실행할 수 있습니다. 자세한 내용은AWS Lake Formation 개발자 안내	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	서에서 AWS 계정 간에 데이터 카탈로그 테이블 및 데이터베이스 공유를 참조하세요.				
표 glue:Table	데이터 카탈로그 테이블을 중앙에서 생성 및 관리하고, 이를 조직 AWS 계정 또는 조직과 공유하세요. 데이터 카탈로그 테이블에는 Amazon S3, JDBC 데이터 소스, Amazon Redshift, 스트리밍 소스 및 기타 데이터 스토어의 데이터 테이블에 대한 메타데이터가 포함되어 있습니다. 이를 통해 사용자는 여러 계정 간에 데이터를 결합하고 쿼리할 수 있는 쿼리 및 ETL 작업을 실행할 수 있습니다. 자세한 내용은AWS Lake Formation 개발자 안내서에서 AWS 계정 간에 데이터 카탈로그 테이블 및 데이터베이스 공유를 참조하세요.	아니요	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

AWS License Manager

를 사용하여 AWS RAM다음 AWS License Manager 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
라이선스 구성 `license-manager:LicenseConfiguration`	라이선스 구성을 중앙에서 생성 및 관리하고 다른 사용자 AWS 계정 또는 조직과 공유할 수 있습니다. 이를 통해 여러 AWS 계정의 기업 계약 조건을 기반으로 하는 중앙 관리형 라이선스 규칙을 적용할 수 있습니다. 자세한 내용은 License Manager 사용 설명서에서 License Manager의 라이선스 구성을 참조하세요.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

AWS Marketplace

를 사용하여 AWS RAM다음 AWS Marketplace 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Marketplace Catalog 개체 `aws-marketplace:Entity`	에서 조직 전체 AWS 계정 또는 조직 내에서 엔티티를 만들고, 관리하고, 공유할 수 AWS Marketplace있습니다. 자세한 내용은AWS Marketplace Catalog API 참조의 AWS RAM에서 리소스 공유를 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

AWS Migration Hub Refactor Spaces

를 사용하여 다음 AWS Migration Hub Refactor Spaces 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Refactor Spaces 환경 `refactor-spaces:Environment`	Refactor Spaces 환경을 생성하고 이를 사용하여 Refactor Spaces 애플리케이션을 포함시킵니다. 다른 AWS 계정 또는 조직 내 모든 계정과 환경을 공유합니다. 이를 통해 여러 명의 사용자가 환경 AWS 계정 및 해당 환경 내 애플리케이션에 대한 정보를 볼 수	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	있습니다. 자세한 내용은 AWS Migration Hub Refactor Spaces 사용 설명서에서 AWS RAM을 사용하여 Refactor Spaces 환경 공유를 참조하세요.				

AWS Network Firewall

를 사용하여 다음 AWS Network Firewall 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
방화벽 정책 network-firewall:FirewallPolicy	방화벽 정책을 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유할 수 있습니다. 이를 통해 조직 내 여러 계정에서 공통의 네트워크 모니터링, 보호 및 필터링 동작을 공유할 수 있습니다. 자세한 내용은AWS Network Firewall 개발자 안내서에서 방화벽 정책 및 규칙 그룹 공유를 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능

규칙 그룹
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	스테이트리스 및 스테이트풀 규칙 그룹을 중앙에서 생성 및 관리하고 다른 AWS 계정 사람이나 조직과 공유하세요. 이를 통해 조직의 여러 계정이 네트워크 트래픽을 검사하고 AWS Organizations 처리하기 위한 일련의 기준을 공유할 수 있습니다. 자세한 내용은AWS Network Firewall 개발자 안내서에서 방화벽 정책 및 규칙 그룹 공유를 참조하세요.	예	예
			
			모든 AWS 계정과 공유할 수 있습니다.
				아니요	아니요

AWS Outposts

를 사용하여 AWS RAM다음 AWS Outposts 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Outpost `outposts:Outpost`	Outposts를 중앙에서 생성하여 관리하고 조직 내 다른 AWS 계정과 공유합니다. 이를 통해 여러 계정에서 중앙	아니요	아니요	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	관리형 공유 Outposts에 서브넷과 EBS 볼륨을 생성할 수 있습니다. 자세한 내용은 AWS Outposts 사용 설명서의 공유 AWS Outposts 리소스 사용을 참조하십시오.		소속 조직 내 AWS 계정 과만 공유할 수 있습니다.		
로컬 게이트웨이 라우팅 테이블 `ec2:LocalGatewayRouteTable`	로컬 게이트웨이에 대한 VPC 연결을 AWS 계정 중앙에서 생성 및 관리하고 조직 내 다른 사람과 공유합니다. 이를 통해 여러 계정에서 로컬 게이트웨이에 대한 VPC 연결을 생성하고 라우팅 테이블 및 가상 인터페이스 구성을 확인할 수 있습니다. 자세한 내용은 AWS Outposts 사용 설명서에서 공유 가능한 Outpost 리소스를 참조하세요.	 아니요	 아니요 소속 조직 내 AWS 계정 과만 공유할 수 있습니다.	 아니요	 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
사이트 `outposts:Site`	Outpost 사이트를 생성하여 관리하고 조직 내 다른 AWS 계정 과 공유합니다. 이를 통해 여러 계정이 공유 사이트에서 Outposts를 생성하여 관리할 수 있으며 Outpost 리소스와 사이트 간의 분할 제어를 지원합니다. 자세한 내용은 AWS Outposts 사용 설명서의 공유 AWS Outposts 리소스 사용을 참조하십시오.	아니요	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

Outposts에서의 Amazon S3

AWS RAM을 사용하여 다음과 같은 Amazon S3 on Outposts 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
S3 on Outposts `s3-outposts:Outpost`	Outpost에서 Amazon S3 버킷, 액세스 포인트, 엔드포인트를 생성하여 관리합니다. 이를 통해 여러 계정이 공유 사이트에서 Outposts를 생성하여 관리할 수 있으	아니요	아니요 소속 조직 내 AWS	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	며 Outpost 리소스와 사이트 간의 분할 제어를 지원합니다. 자세한 내용은 AWS Outposts 사용 설명서의 공유 AWS Outposts 리소스 사용을 참조하십시오.		계정 과만 공유할 수 있습니다.		

AWS 리소스 탐색기

를 사용하여 AWS RAM다음 AWS 리소스 탐색기 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
보기 `resource-explorer-2:View`	리소스 탐색기 보기를 AWS 계정 중앙에서 만들고 구성한 다음 조직 내 다른 사용자와 공유할 수 있습니다. 이렇게 하면 여러 역할과 사용자가 뷰를 통해 액세스할 수 있는 리소스를 AWS 계정 검색하고 검색할 수 있습니다. 자세한 내용은 AWS 리소스 탐색기 사용 설명서에서 Resource Explorer 뷰 공유를 참조하세요.	 니요	 니요 소속 조직 내 AWS 계정 과만 공유할 수 있습니다.	 니요	 니요

AWS Resource Groups

를 사용하여 다음 AWS Resource Groups 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
리소스 그룹 `resource-groups:Group`	호스트 리소스 그룹을 AWS 계정 중앙에서 생성 및 관리하고 조직 내 다른 사용자와 공유할 수 있습니다. 이를 통해 AWS License Manager를 사용하여 생성된 Amazon EC2 전용 호스트 그룹을 여러 AWS 계정 에서 공유할 수 있습니다. 자세한 정보는 AWS License Manager 사용 설명서에서 AWS License Manager의 호스트 리소스 그룹을 참조하세요.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

Amazon Route 53

AWS RAM을 사용하여 다음과 같은 Amazon Route 53 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Route 53 Resolver DNS Firewall 규칙 그룹 `route53resolver:FirewallRuleGroup`	Route 53 Resolver DNS 방화벽 규칙 그룹을 중앙에서 생성 및 관리하고 다른 AWS 계정 사람 또는 조직과 공유하십시오. 이를 통해 Route 53 Resolver를 통과하는 아웃바운드 DNS 쿼리를 검사 및 처리하기 위한 일련의 기준을 여러 계정에서 공유할 수 있습니다. 자세한 내용은 Amazon Route 53 개발자 안내서에서 AWS 계정간 Route 53 Resolver DNS 방화벽 규칙 그룹 공유를 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요
Route 53 Profiles `route53profiles:Profile`	Route 53을 Profiles 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하십시오. 이렇게 하면 여러 계정이 Route 53에 지정된 DNS 구성을 여러 VPC에 적용할 Profiles 수 있습니다. 자세한 내용은 아마존 Route 53 Profiles 개발자 안내서의 아마존 Route 53을 참조하십시오.	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Resolver 규칙 `route53resolver:ResolverRule`	Resolver 규칙을 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하십시오. 이를 통해 DNS 쿼리를 여러 계정의 Virtual Private Cloud(VPC)에서 중앙 관리형 공유 Resolver 규칙에 정의된 대상 IP 주소로 전달할 수 있습니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 다른 사람과 리졸버 규칙 공유 AWS 계정 및 공유 규칙 사용을 참조하십시오.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
쿼리 로그 route53resolver:ResolverQueryLogConfig	쿼리 로그를 중앙에서 생성하여 관리하고 다른 AWS 계정 또는 조직과 공유합니다. 이를 통해 여러 AWS 계정 의 VPC에서 시작된 DNS 쿼리를 중앙 관리형 쿼리 로그에 기록할 수 있습니다. 자세한 내용은 Amazon Route 53 개발자 안내서에서 Resolver 쿼리 로깅 구성을 다른 AWS 계정과 공유를 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

Amazon Route 53 Application Recovery Controller

AWS RAM을 사용하여 다음과 같은 Amazon Route 53 Application Recovery Controller 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Route 53 ARC 클러스터 route53-recovery-c	Route 53 ARC 클러스터를 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하십시오. 이를 통해 여러 계정이 하나의	예	예 모든 AWS 계정과 공	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
ontrol:Cluster	공유 클러스터에서 제어판과 라우팅 제어를 생성할 수 있으므로 복잡성을 줄이고 조직에 필요한 총 클러스터 수를 줄일 수 있습니다. 자세한 내용은 Amazon Route 53 Application Recovery Controller 개발자 안내서에서 계정 간에 클러스터 공유를 참조하세요.		유할 수 있습니다.		

Amazon Simple Storage Service

를 사용하여 AWS RAM다음 Amazon Simple Storage Service 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Access Grants s3:AccessGrants	S3 Access Grants 인스턴스를 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유할 수 있습니다. 이렇게 하면 여러 계정에서 공유 리소스를 보고 삭제할 수 있습니다. 자세한 내용은	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	예

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	사용 Amazon Simple Storage Service 설명서의 S3 Access Grants 계정 간 액세스를 참조하십시오.				

아마존 SageMaker

를 사용하여 다음 Amazon SageMaker 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
SageMaker 카탈로그 `sagemaker:SagemakerCatalog`	검색 용이성 — 계정 소유자가 카탈로그의 모든 기능 그룹 리소스에 대해 다른 계정에 검색 가능 권한을 부여할 수 있습니다. SageMaker 액세스 권한이 부여되면 해당 계정의 사용자는 카탈로그에서 공유된 특성 그룹을 볼 수 있습니다. 자세한 내용은 Amazon SageMaker 개발자 안내서의 계정 간 기능 그룹 검색 및 액세스를 참조하십시오.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 예	

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	Note 에서 검색 가능성과 액세스는 별도의 권한입니다. SageMaker				
SageMaker 기능 그룹 `sagemaker:FeatureGroup`	액세스 - 계정 소유자가 일부 특성 그룹 리소스에 대한 액세스 권한을 다른 계정에 부여할 수 있습니다. 액세스 권한이 부여되면 해당 계정의 사용자는 공유된 특성 그룹을 사용할 수 있습니다. 자세한 내용은 Amazon SageMaker 개발자 안내서의 계정 간 기능 그룹 검색 및 액세스를 참조하십시오. Note 에서 검색 가능성과 액세스는 별도의 권한입니다. SageMaker	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
계보 그룹 `sagemaker:LineageGroup`	SageMaker Amazon에서는 파이프라인 메타데이터의 계보 그룹을 생성하여 그 역사와 관계를 더 깊이 이해할 수 있도록 합니다. 계보 그룹을 조직의 다른 사람 AWS 계정 또는 계정과 공유하십시오. 이렇게 하면 여러 AWS 계정 사용자가 계보 그룹에 대한 정보를 보고 계보 그룹 내의 추적 엔티티를 쿼리할 수 있습니다. 자세한 내용은 Amazon SageMaker 개발자 안내서의 계정 간 계보 추적을 참조하십시오.	예	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
SageMaker 모델 카드 `sagemaker:ModelCard`	SageMaker Amazon은 간소화된 거버넌스 및 보고를 위해 기계 학습 (ML) 모델에 대한 중요한 세부 정보를 한 곳에 문서화하는 모델 카드를 생성합니다. 모델 카드를 다른 AWS 계정 또는 조직 내 계정과 공유하여 기계 학습 작업을 위한 다중 계정 전략을 수립합니다. AWS 계정 이를 통해 ML 활동에 대한 모델 카드 액세스 권한을 다른 계정과 공유할 수 있습니다. 자세한 내용은 Amazon SageMaker 개발자 안내서의 Amazon SageMaker 모델 카드를 참조하십시오.	 예	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
SageMaker 파이프라인 `sagemaker:Pipeline`	Amazon SageMaker Model Building Pipeline을 사용하면 end-to-end 기계 학습 워크플로를 대규모로 생성, 자동화 및 관리할 수 있습니다. 파이프라인을 조직의 다른 사용자 AWS 계정 또는 계정과 공유하여 기계 학습 작업을 위한 다중 계정 전략을 달성하십시오. 이렇게 하면 여러 사용자가 다른 AWS 계정 계정에서 파이프라인을 시작, 중지, 재시도할 수 있는 선택적 액세스 권한으로 파이프라인 및 해당 실행에 대한 정보를 볼 수 있습니다. 자세한 내용은 Amazon SageMaker 개발자 안내서의 SageMaker 파이프라인에 대한 교차 계정 지원을 참조하십시오.	 예	 예 모든 AWS 계정과 공유할 수 있습니다.	 예	 아니요

AWS Service Catalog AppRegistry

를 사용하여 다음 AWS Service Catalog AppRegistry 리소스를 공유할 수 있습니다. AWS RAM

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
애플리케이션 servicecatalog:Application	애플리케이션을 만들고 이를 사용하여 AWS 환경 전체에서 해당 애플리케이션에 속하는 리소스를 추적할 수 있습니다. 응용 프로그램을 다른 사람 AWS 계정 또는 조직과 공유하십시오. 이렇게 하면 여러 AWS 계정 명의 사용자가 로컬에서 응용 프로그램 및 관련 리소스에 대한 정보를 볼 수 있습니다. 자세한 내용은 Service Catalog 사용 설명서에서 애플리케이션 사용을 참조하세요.	 아니요	 아니요 소속 조직 내 AWS 계정 과만 공유할 수 있습니다.	 예	 아니요
속성 그룹 servicecatalog:AttributeGroup	속성 그룹을 만들고 이를 사용하여 애플리케이션과 관련된 메타데이터를 저장합니다. 속성 그룹을 다른 AWS 계정 또는 조직과 공유합니다. 이를 통해 여러 AWS 계정 및 사용자가 속성 그룹에 대한 정보를 확인할 수 있습니다. 자세한 내용은 Service Catalog 사용 설명서에서 속성	 아니요	 아니요 소속 조직 내 AWS 계정 과만 공유할 수 있습니다.	 예	 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	그룹 생성을 참조하세요.				

AWS Systems Manager Incident Manager

를 사용하여 다음 AWS Systems Manager Incident Manager 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
연락처 `ssm-contacts:Contact`	연락처 및 에스컬레이션 계획을 중앙에서 생성 및 관리하고 연락처 세부 정보를 다른 사람 AWS 계정 또는 조직과 공유하세요. 이를 통해 많은 사람들이 사고 AWS 계정 중에 발생한 작업을 볼 수 있습니다. 자세한 내용은 AWS Systems Manager Incident Manager 사용 설명서에서 공유 연락처 및 대응 계획 작업을 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
대응 계획 `ssm-incidents:ResponsePlan`	중앙에서 대응 계획을 작성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하세요. 이를 통해 Amazon CloudWatch 경보와 Amazon EventBridge 이벤트 규칙을 대응 계획에 AWS 계정 연결하여 사고가 감지되면 자동으로 사고를 생성할 수 있습니다. 또한 이 인시던트는 다른 AWS 계정의 지표에도 액세스할 수 있습니다. 자세한 내용은 AWS Systems Manager Incident Manager 사용 설명서에서 공유 연락처 및 대응 계획 작업을 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

AWS Systems Manager 파라미터 스토어

를 사용하여 다음 AWS Systems Manager 파라미터 스토어 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
파라미터 `ssm:Parameter`	파라미터를 생성하고 이를 사용하여 스크립트, 명령, SSM 문서, 구성 및 자동화 워크플로에서 참조할 수 있는 구성 데이터를 저장합니다. 파라미터를 다른 사람 AWS 계정 또는 조직과 공유하세요. 이렇게 하면 여러 AWS 계정 명의 사용자가 문자열에 대한 정보를 볼 수 있으며 데이터를 코드에서 분리하여 보안을 개선할 수 있습니다. 자세한 내용은 AWS Systems Manager 사용 안내서의 공유 매개변수 작업을 참조하십시오.	예	예 모든 AWS 계정과 공유할 수 있습니다.	예	아니요

Amazon VPC

AWS RAM을 사용하여 다음과 같은 Amazon Virtual Private Cloud(Amazon VPC) 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
고객 소유 IPv4 주소 `ec2:CoipPool`	AWS Outposts 설치 프로세스 중에 온-프레미스 네트워크에 대해 제공하는 정보를 기반으로 고객 소유 IP 주소 풀이라는 주소 풀을 AWS 만듭니다. 고객 소유 IP 주소는 온프레미스 네트워크를 통해 Outposts 서브넷의 리소스에 대한 로컬 또는 외부 연결을 제공합니다. 이러한 주소는 탄력적 IP 주소를 사용하거나 고객 소유 IP 주소를 자동으로 할당하는 서브넷 설정을 사용하여 EC2 인스턴스 등의 Outpost의 리소스에 할당할 수 있습니다. 자세한 내용은AWS Outposts 사용 설명서에서 고객 소유 IP 주소를 참조하세요.	✗ 아니요	✗ 아니요 소속 조직 내 AWS 계정 과만 공유할 수 있습니다.	✗ 아니요	✗ 아니요
IP 주소 관리자 (IPAM) 풀 `ec2:IpamPool`	Amazon VPC IPAM 풀을 다른 AWS 계정 IAM 역할 또는 사용자 또는 전체 조직 또는 조직 단위 (OU) 와 중앙에서 공유할 수 있습니다. AWS	✓ 예	✓ 예 모든 AWS 계정과 공	✓ 예	✗ 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	Organizations이를 통해 해당 보안 주체는 풀의 CIDR을 각 계정의 VPC와 같은 AWS 리소스에 할당할 수 있습니다. 자세한 내용은 Amazon VPC IP 주소 사용 설명서에서 AWS RAM I을 사용하여 IPAM 풀 공유를 참조하세요.		유할 수 있습니다.		
IP 주소 관리자 (IPAM) 리소스 검색 `ec2:IpamResourceDiscovery`	리소스 검색을 다른 사람과 공유하세요. AWS 계정리소스 검색은 IPAM이 소유 계정에 속한 리소스를 관리하고 모니터링할 수 있도록 하는 Amazon VPC IPAM 구성 요소입니다. 자세한 내용은 Amazon VPC IPAM 사용 설명서에서 리소스 검색 작업을 참조하세요.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
접두사 목록 `ec2:PrefixList`	접두사 목록을 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하세요. 이를 통해 여러 AWS 계정이 VPC 보안 그룹 및 서브넷 라우팅 테이블과 같은 리소스에서 접두사 목록을 참조할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서에서 공유 접두사 목록 작업을 참조하세요.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
서브넷 ec2:Subnet	서브넷을 중앙에서 생성하여 관리하고 조직 내 AWS 계정 과 공유합니다. 이를 통해 여러 AWS 계정 에서 애플리케이션 리소스를 중앙에서 관리되는 VPC로 시작할 수 있습니다. 이러한 리소스에는 Amazon EC2 인스턴스, 아마존 관계형 데이터베이스 서비스 (RDS) 데이터베이스, Amazon Redshift 클러스터 및 함수가 포함됩니다. AWS Lambda 자세한 내용은 Amazon VPC 사용 설명서에서 VPC 공유 작업을 참조하세요. **Note** 리소스 공유를 생성할 때 서브넷을 포함하려면 `ram:CreateResourceShare` 외에도 `ec2:DescribeSubnets` 및 `ec2:DescribeVpcs` 권한	아니요	아니요 소속 조직 내 AWS 계정 과만 공유할 수 있습니다.	아니요	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	이 있어야 합니다. 기본 서브넷은 공유할 수 없습니다. 직접 생성한 서브넷만 공유할 수 있습니다.				
트래픽 미러 대상 `ec2:TrafficMirrorTarget`	트래픽 미러 대상을 중앙에서 생성 및 관리하고 다른 사람 또는 조직과 공유하십시오. AWS 계정 이를 통해 여러 AWS 계정 계정이 미러링된 네트워크 트래픽을 계정의 트래픽 미러 소스에서 중앙 관리형 공유 트래픽 미러 대상으로 전송할 수 있습니다. 자세한 내용은 Traffic Mirroring 설명서에서 크로스 계정 트래픽 미러링 대상을 참조하세요.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 아니요	 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Transit Gateway `ec2:TransitGateway`	대중 교통 게이트웨이를 중앙에서 생성 및 관리하고 다른 사람 AWS 계정 또는 조직과 공유하세요. 이를 통해 여러 AWS 계정 에서 중앙 관리형 공유 전송 게이트웨이를 통해 VPC와 온프레미스 네트워크 간에 트래픽을 라우팅할 수 있습니다. 자세한 내용은 Amazon VPC Transit Gateway에서 Transit Gateway 생성을 참조하세요. **Note** 리소스 공유를 생성할 때 전송 게이트웨이를 포함하려면 `ram:CreateResourceShare` 외에도 `ec2:DescribeTransitGateway` 권한이 있어야 합니다.	✗ 아니요	✓ 예 모든 AWS 계정과 공유할 수 있습니다.	✗ 아니요	✗ 아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
전송 게이트웨이 멀티캐스트 도메인 `ec2:TransitGatewayMulticastDomain`	트랜짓 게이트웨이 멀티캐스트 도메인을 중앙에서 생성 및 관리하고 다른 AWS 계정 사람 또는 조직과 공유하세요. 이렇게 하면 멀티캐스트 도메인에서 그룹 구성원 또는 그룹 소스를 여러 명이 AWS 계정 등록 및 등록 취소할 수 있습니다. 자세한 내용은 Transit Gateways 설명서에서 공유 멀티캐스트 도메인 작업을 참조하세요.	아니요	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
AWS Verified Access 그룹 `ec2:VerifiedAccessGroup`	중앙에서 AWS Verified Access 그룹을 만들고 관리한 다음 다른 사람 AWS 계정 또는 조직과 공유하세요. 이를 통해 여러 계정의 애플리케이션이 하나의 공유 AWS Verified Access 엔드포인트 세트를 사용할 수 있습니다. 자세한 내용은 AWS Verified Access 사용 설명서의 AWS Verified Access 그룹 공유를 참조하십시오. AWS Resource Access Manager	예	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

Amazon VPC Lattice

AWS RAM을 사용하여 다음과 같은 Amazon VPC Lattice 리소스를 공유할 수 있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Amazon VPC Lattice 서비스 `vpc-lattice:Service`	Amazon VPC Lattice 서비스를 중앙에서 생성 및 관리하고 개인 AWS 계정 또는 조직과 공유하십시오. 이를 통해 서	아니요	예	예	아니요

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
	비스 소유자는 다중 계정 환경에서 service-to-service 통신을 연결, 보호 및 관찰할 수 있습니다. 자세한 내용은 VPC Lattice 사용 설명서에서 공유 리소스 작업을 참조하세요.		모든 AWS 계정과 공유할 수 있습니다.		
Amazon VPC Lattice 서비스 네트워크 `vpc-lattice:ServiceNetwork`	Amazon VPC Lattice 서비스 네트워크를 중앙에서 생성 및 관리하고 개인 AWS 계정 또는 조직과 공유하십시오. 이를 통해 서비스 네트워크 소유자는 다중 계정 환경에서 service-to-service 통신을 연결, 보호 및 관찰할 수 있습니다. 자세한 내용은 Amazon VPC Lattice 사용 설명서에서 공유 리소스 작업을 참조하세요.	 아니요	 예 모든 AWS 계정과 공유할 수 있습니다.	 예	 아니요

AWS 클라우드 WAN

를 사용하여 다음과 같은 AWS 클라우드 WAN 리소스를 공유할 수 AWS RAM있습니다.

리소스 유형 및 코드	사용 사례	IAM 사용자 및 역할과 공유 가능	조직 외부 계정과 공유 가능	고객 관리형 권한 사용 가능	서비스 보안 주체와 공유 가능
Cloud WAN 코어 네트워크 `networkmanager:CoreNetwork`	클라우드 WAN 코어 네트워크를 중앙에서 생성 및 관리하고 다른 AWS 계정사람과 공유하십시오. 이를 통해 단일 클라우드 WAN 코어 네트워크에서 여러 호스트에 AWS 계정 액세스하고 호스트를 프로비저닝할 수 있습니다. 자세한 내용은AWS Cloud WAN 사용 설명서에서 코어 네트워크 공유를 참조하세요.	예	예 모든 AWS 계정과 공유할 수 있습니다.	아니요	아니요

AWS RAM에서 권한 관리

AWS RAM에는 AWS 관리형 권한과 고객 관리형 권한이라는 두 가지 유형의 관리형 권한이 있습니다.

관리형 권한은 소비자가 리소스 공유 내의 리소스에 대해 수행할 수 있는 작업을 정의합니다. 리소스 공유를 생성할 때는 리소스 공유에 포함된 각 리소스 유형에 사용할 관리형 권한을 지정해야 합니다. 관리형 권한의 정책 템플릿에는 보안 주체와 리소스를 제외한 리소스 기반 정책에 필요한 모든 것이 포함되어 있습니다. 리소스의 Amazon 리소스 이름(ARN) 및 리소스 공유와 연결된 보안 주체의 ARN이 리소스 기반 정책의 구성 요소입니다. AWS RAM은 해당 리소스 공유의 모든 리소스에 연결되는 리소스 기반 정책을 작성합니다.

각 관리형 권한에는 하나 이상의 버전이 있을 수 있습니다. 한 버전이 해당 관리형 권한의 기본 버전으로 지정됩니다. AWS에서 새 버전을 생성한 후 해당 새 버전을 기본값으로 지정하여 리소스 유형에 대한 AWS 관리형 권한을 업데이트하는 경우도 있습니다. 사용자가 새 버전을 생성하여 고객 관리형 권한을 업데이트할 수도 있습니다. 리소스 공유에 이미 연결된 관리형 권한은 자동으로 업데이트되지 않습니다. AWS RAM 콘솔에서 새 기본 버전이 사용 가능할 경우 알림이 표시되므로, 사용자는 이전 버전과 비교하여 새 기본 버전의 변경 사항을 검토할 수 있습니다.

> **Note**
>
> 가능한 한 빨리 새 버전의 AWS 관리형 권한으로 업데이트하는 것이 좋습니다. 이러한 업데이트에는 일반적으로 AWS RAM을 사용하여 추가 리소스 유형을 공유할 수 있는 신규 또는 업데이트된 AWS 서비스에 대한 지원이 추가되어 있습니다. 새 기본 버전으로 보안 취약성을 해결하고 수정할 수도 있습니다.

> **Important**
>
> 새 리소스 공유에는 관리형 권한의 기본 버전만 연결할 수 있습니다.

사용 가능한 관리형 권한 목록은 언제든지 검색할 수 있습니다. 자세한 내용은 관리형 권한 보기 섹션을 참조하세요.

주제

- 관리형 권한 보기
- AWS RAM에서 고객 관리형 권한 생성 및 사용

- AWS 관리형 권한을 최신 버전으로 업데이트
- AWS RAM에서 고객 관리형 권한을 사용할 때 고려할 사항
- 관리형 권한의 작동 방식
- 관리형 권한의 유형

관리형 권한 보기

리소스 공유의 리소스 유형에 할당할 수 있는 관리형 권한에 대한 세부 정보를 볼 수 있습니다. 리소스 공유에 할당된 관리형 권한을 식별할 수 있습니다. 이러한 세부 정보를 보려면 AWS RAM 콘솔에서 관리형 권한 라이브러리를 사용하세요.

Console

AWS RAM에서 사용 가능한 관리형 권한에 대한 세부 정보를 보려면

1. AWS RAM 콘솔에서 관리형 권한 라이브러리 페이지로 이동합니다.
2. AWS RAM 리소스 공유는 특정 AWS 리전에 존재하므로 콘솔의 오른쪽 상단에 있는 드롭다운 목록에서 해당 AWS 리전을 선택합니다. 글로벌 리소스가 포함된 리소스 공유를 보려면 AWS 리전을 미국 동부(버지니아 북부), `us-east-1`로 설정해야 합니다. 글로벌 리소스 공유에 대한 자세한 내용은 글로벌 리소스와 리전 리소스를 비교하여 공유 섹션을 참조하세요. 모든 리전에서는 사용 가능한 동일한 AWS 관리형 권한을 공유하지만, 이는 Step 5단계에 설명된 각 관리형 권한에 대해 표시되는 관련 리소스 공유 수에 영향을 미칩니다. 고객 관리형 권한은 생성된 리전에서만 사용할 수 있습니다.
3. 관리형 권한 목록에서 세부 정보를 보려는 관리형 권한을 선택합니다. 검색 상자에 이름 또는 리소스 유형의 일부를 입력하거나 드롭다운 목록에서 관리형 권한 유형을 선택하여 관리형 권한 목록을 필터링할 수 있습니다.
4. (선택 사항) 표시 기본 설정을 변경하려면 관리형 권한 패널의 오른쪽 상단에 있는 톱니바퀴 아이콘을 선택합니다. 다음 기본 설정을 변경할 수 있습니다.

   - 페이지 크기 - 각 페이지에 표시되는 리소스 수입니다.
   - 줄 바꿈 - 테이블 행의 줄 바꿈 여부입니다.
   - 열 - 리소스 유형 및 관련 공유에 대한 정보를 표시할지 또는 숨길지 여부입니다.

   표시 기본 설정을 완료한 후 확인을 선택합니다.
5. 각 관리형 권한에 대해 다음 정보가 표시됩니다.

- 관리형 권한 이름 - 관리형 권한의 이름입니다.
- 리소스 유형 - 관리형 권한과 관련된 리소스 유형입니다.
- 관리형 권한 유형 - 관리형 권한이 AWS 관리형 권한인지 고객 관리형 권한인지 여부입니다.
- 연결된 공유 - 관리형 권한과 관련된 리소스 공유 수입니다. 숫자가 나타나면 숫자를 선택하여 다음 정보가 포함된 리소스 공유 테이블을 표시할 수 있습니다.
  - 리소스 공유 이름 - 관리형 권한과 관련된 리소스 공유의 이름입니다.
  - 관리형 권한 버전 - 해당 리소스 공유에 연결된 관리형 권한의 버전입니다.
  - 소유자 - 리소스 공유 소유자의 AWS 계정 번호입니다.
  - 외부 보안 주체 허용 - AWS Organizations에서 리소스 공유를 조직 외부의 주체와 공유할 수 있도록 허용할지 여부입니다.
  - 상태 - 리소스 공유와 관리형 권한 간의 현재 연결 상태입니다.
- 상태 - 관리형 권한이 다음 상태인지 여부를 설명합니다.
  - 연결 가능 - 리소스 공유에 관리형 권한을 연결할 수 있습니다.
  - 연결 불가능 - 리소스 공유에 관리형 권한을 연결할 수 없습니다.
  - 삭제 중 - 관리형 권한은 더 이상 활성화되지 않으며 곧 삭제됩니다.
  - 삭제됨 - 관리형 권한이 삭제되었습니다. 관리형 권한 라이브러리에서 사라지기 전에 2시간 동안 표시된 상태로 유지됩니다.

관리형 권한의 이름을 선택하면 해당 관리형 권한에 대한 자세한 정보가 표시됩니다. 관리형 권한에 대한 세부 정보 페이지에는 다음 정보가 표시됩니다.

- 리소스 유형 - 이 관리형 권한이 적용되는 AWS 리소스의 유형입니다.
- 버전 수 - 각 고객 관리형 권한의 버전은 최대 5개까지 보유할 수 있습니다.
- 기본 버전 - 어떤 버전이 기본 버전인지 지정하며, 이 관리형 권한을 사용하는 모든 새 리소스 공유에 자동으로 할당됩니다. 다른 버전을 사용하는 기존 리소스 공유가 있으면 리소스 공유를 기본 버전으로 업데이트하라는 메시지가 표시됩니다.
- ARN - 관리형 권한의 Amazon 리소스 이름(ARN)입니다. AWS 관리형 권한의 ARN은 다음 형식을 사용합니다.

  ```
  arn:aws:ram::aws:permission/
  AWSRAM[DefaultPermission]ShareableResourceType
  ```

하위 문자열 *[DefaultPermission]*(실제 ARN에서는 대괄호 없음)은 기본값으로 지정된 해당 리소스 유형에 대한 관리형 권한 한 개의 이름에만 표시됩니다.

- 관리형 권한 버전 - 이 드롭다운 목록 아래의 탭에 표시할 버전의 정보를 선택할 수 있습니다.
  - 세부 정보 탭:
    - 생성 시간 - 이 버전의 관리형 권한이 생성된 날짜 및 시간입니다.
    - 마지막 업데이트 시간 - 이 버전의 관리형 권한이 마지막으로 업데이트된 날짜 및 시간입니다.
  - 정책 템플릿 탭 - 이 버전의 관리형 권한을 통해 보안 주체가 관련 리소스 유형에 대해 수행할 수 있는 서비스 작업 및 조건 목록입니다 (해당하는 경우).
  - 연결된 리소스 공유 - 이 버전의 관리형 권한을 사용하는 리소스 공유 목록입니다.

AWS CLI

AWS RAM에서 사용 가능한 관리형 권한에 대한 세부 정보를 보려면

list-permissions 명령을 사용하면 호출 계정의 현재 AWS 리전에 있는 리소스 공유에 사용할 수 있는 관리형 권한 목록을 가져올 수 있습니다.

```
$ aws ram list-permissions
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:31.732000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:31.732000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "version": "1",
```

```
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-11-18T07:05:46.976000-08:00",
            "lastUpdatedTime": "2022-11-18T07:05:46.976000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },

        ... TRUNCATED FOR BREVITY ... RUN COMMAND TO SEE COMPLETE LIST OF
 PERMISSIONS ...

        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "resourceType": "networkmanager:CoreNetwork",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:46.557000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:46.557000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
            "version": "1",
            "defaultVersion": true,
            "name": "My-Test-CMP",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2023-03-08T06:54:10.038000-08:00",
            "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "CUSTOMER_MANAGED"
        }
    ]
}
```

`list-permissions` AWS CLI 명령의 `--query` 파라미터를 사용하여 특정 관리형 권한의 이름으로 ARN을 찾을 수도 있습니다. 다음 예에서는 지정된 이름과 일치하는 `permissions` 배열 결과의

요소만 포함하도록 출력을 필터링합니다. 또한 결과에 ARN 필드만 표시하고 기본 JSON 대신 일반 텍스트 형식으로 표시하도록 지정합니다.

```
$ aws ram list-permissions \
    --query "permissions[?name == 'My-Test-CMP'].arn \
    --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
```

관심 있는 특정 관리형 권한의 ARN을 찾은 후 get-permission 명령을 실행하여 JSON 정책 텍스트를 포함한 세부 정보를 검색할 수 있습니다.

```
$ aws ram get-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
        "version": "1",
        "defaultVersion": true,
        "name": "My-Test-CMP",
        "resourceType": "ec2:IpamPool",
        "permission": "{\n\t\"Effect\": \"Allow\",\n\t\"Action\": [\n
\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\"ec2:GetIpamPoolCidrs\",\n\t
\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\"ec2:AssociateVpcCidrBlock\",\n
\t\t\"ec2:CreateVpc\",\n\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t
\"ec2:ReleaseIpamPoolAllocation\"\n\t]\n}",
        "creationTime": "2023-03-08T06:54:10.038000-08:00",
        "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
        "isResourceTypeDefault": false,
        "permissionType": "CUSTOMER_MANAGED",
        "featureSet": "STANDARD",
        "status": "ATTACHABLE"
    }
}
```

AWS RAM에서 고객 관리형 권한 생성 및 사용

AWS Resource Access Manager(AWS RAM)는 공유 가능한 리소스 유형마다 적어도 하나의 AWS 관리형 권한을 제공합니다. 하지만 이러한 관리형 권한이 공유 사용 사례에 대한 최소 권한 액세스를 제공하지 않을 수도 있습니다. 제공된 AWS 관리형 권한 중 하나가 작동하지 않는 경우 고객 관리형 권한을 직접 생성할 수 있습니다.

고객 관리형 권한은 AWS RAM을 사용하여 공유되는 리소스에 대해 어떤 조건에서 어떤 작업을 수행할 수 있는지 정확하게 지정하여 작성하고 유지 관리하는 관리형 권한입니다. 예를 들어, 대규모로 IP 주소를 관리하는 데 도움이 되도록 Amazon VPC IP 주소 관리자(IPAM) 풀에 대한 읽기 액세스를 제한하려고 합니다. 개발자가 IP 주소를 할당할 수 있는 고객 관리형 권한을 생성할 수 있지만, 다른 개발자 계정이 할당하는 IP 주소 범위를 볼 수는 없습니다. 최소 권한 모범 사례에 따라 공유 리소스에 대한 작업을 수행하는 데 필요한 권한만 부여할 수 있습니다.

또한 필요에 따라 고객 관리형 권한을 업데이트하거나 삭제할 수 있습니다.

주제

고객 관리형 정책 생성

고객 관리형 권한은 AWS 리전에만 적용됩니다. 해당 리전에서 이 고객 관리형 권한을 생성했는지 확인합니다.

Console

고객 관리형 정책을 생성하려면

1. 다음 중 하나를 수행합니다.
   - 관리형 권한 라이브러리로 이동하여 고객 관리형 권한 생성을 선택합니다.
   - 콘솔에서 고객 관리형 권한 생성 페이지로 바로 이동합니다.
2. 고객 관리형 권한 세부 정보에 고객 관리형 권한 이름을 입력합니다.
3. 이 관리형 권한이 적용되는 리소스 유형을 선택합니다.
4. 정책 템플릿에서 해당 리소스 유형에 대해 수행할 수 있는 작업을 정의합니다.
   - 관리형 권한 가져오기를 선택하여 기존 관리형 권한의 작업을 사용할 수 있습니다.
   - 시각적 편집기에서 요구 사항에 맞는 액세스 수준 정보를 선택하거나 선택 취소합니다.
   - JSON 편집기를 사용하여 조건을 추가하거나 수정합니다.

5. (선택 사항) 관리형 권한에 태그를 연결하려면 태그에 태그 키와 값을 입력합니다. 새 태그 추가를 선택하여 태그를 추가합니다. 필요에 따라 이 단계를 반복합니다.
6. 완료했으면 고객 관리형 권한 생성을 선택합니다.

AWS CLI

고객 관리형 정책을 생성하려면

- create-permission 명령을 실행하고 이름, 고객 관리형 권한이 적용될 리소스 유형, 정책 템플릿 본문 텍스트를 지정합니다.

  다음 예제 명령은 `imagebuilder:Component` 리소스 유형에 대한 관리형 권한을 생성합니다.

```
$ aws ram create-permission \
    --name TestCMP \
    --resource-type imagebuilder:Component \
    --policy-template "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}"
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "1",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "resourceType": "imagebuilder:Component",
        "status": "ATTACHABLE",
        "creationTime": 1680033769.401,
        "lastUpdatedTime": 1680033769.401
    }
}
```

고객 관리형 권한의 새 버전 생성

고객 관리형 권한의 사용 사례가 변경된 경우 관리형 권한의 새 버전을 생성할 수 있습니다. 이는 기존 리소스 공유에는 영향을 미치지 않으며, 이 고객 관리형 권한을 사용하는 향후 새 리소스 공유에만 영향을 미칩니다.

각 관리형 권한에는 최대 5개의 버전이 있을 수 있지만 기본 버전만 연결할 수 있습니다.

Console

고객 관리형 권한의 새 버전을 생성하려면

1. 관리형 권한 라이브러리로 이동합니다.
2. 관리형 권한 목록을 고객 관리형으로 필터링하거나 변경하려는 고객 관리형 권한의 이름을 검색합니다.
3. 관리형 권한 세부 정보 페이지의 관리형 권한 버전 섹션에서 버전 생성을 선택합니다.
4. 정책 템플릿의에서 시각적 편집기 또는 JSON 편집기를 사용하여 작업 및 조건을 추가하거나 제거할 수 있습니다.

   관리형 권한 가져오기를 선택하여 기존 정책 템플릿을 사용할 수도 있습니다.
5. 완료했으면 페이지 하단에 있는 버전 생성을 선택합니다.

AWS CLI

고객 관리형 권한의 새 버전을 생성하려면

1. 새 버전을 생성할 관리형 권한의 Amazon 리소스 이름(ARN)을 찾습니다. 이 작업을 수행하려면 고객 관리형 권한만 포함하도록 list-permissions를 `--permission-type CUSTOMER_MANAGED` 파라미터와 함께 호출합니다.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. ARN을 확보한 후에는 create-permission-version 작업을 호출하고 업데이트된 정책 템플릿을 제공할 수 있습니다.

```
$ aws ram create-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --policy-template {"Effect":"Allow","Action":
["imagebuilder:ListComponents"]}
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "2",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "status": "ATTACHABLE",
        "resourceType": "imagebuilder:Component",
        "permission": "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}",
        "creationTime": 1680038973.79,
        "lastUpdatedTime": 1680038973.79
    }
}
```

출력에 새 버전의 버전 번호가 포함됩니다.

다른 버전을 고객 관리형 권한의 기본값으로 선택

다른 고객 관리형 권한 버전을 새 기본 버전으로 설정할 수 있습니다.

Console

고객 관리형 권한의 새 기본 버전을 설정하려면

1. 관리형 권한 라이브러리로 이동합니다.
2. 관리형 권한 목록을 고객 관리형으로 필터링하거나 변경하려는 고객 관리형 권한의 이름을 검색합니다.
3. 고객 관리형 권한 세부 정보 페이지의 관리형 권한 버전 섹션에서 드롭다운 목록을 사용하여 새 기본값으로 설정할 버전을 선택합니다.
4. 기본 버전으로 설정을 선택합니다.

5. 대화 상자가 나타나면 해당 고객 관리형 권한을 사용하는 모든 새 리소스 공유에 대해 이 버전을 기본 버전으로 설정할지 확인합니다. 동의하면 기본 버전으로 설정을 선택합니다.

AWS CLI

고객 관리형 권한의 새 기본 버전을 설정하려면

1. list-permission-versions를 호출하여 기본 버전으로 설정할 버전 번호를 찾습니다.

   다음 예제 명령은 지정된 관리형 권한의 현재 버전을 검색합니다.

```
$ aws ram list-permission-versions \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "1",
            "defaultVersion": false,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "UNATTACHABLE",
            "creationTime": 1680033769.401,
            "lastUpdatedTime": 1680035597.345
        },
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
```

```
}
```

2. 기본값으로 설정할 버전 번호가 있으면 set-default-permision-version 작업을 호출할 수 있습니다.

```
$ aws ram-cmp set-default-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 2
```

   성공해도 이 명령은 출력을 반환하지 않습니다. list-permission-versions를 다시 실행하면 선택한 버전의 `defaultVersion` 필드가 현재 `true`로 설정되어 있는지 확인할 수 있습니다.

고객 관리형 권한 버전 삭제

각 고객 관리형 권한의 버전은 최대 5개까지 보유할 수 있습니다. 더 이상 필요하지 않아 사용하지 않는 버전은 삭제할 수 있습니다. 고객 관리형 권한의 기본 버전은 삭제할 수 없습니다. 삭제된 버전은 완전히 제거되기 전까지 최대 2시간 동안 콘솔에 삭제됨 상태로 표시됩니다.

Console

고객 관리형 권한 버전을 삭제하려면

1. 관리형 권한 라이브러리로 이동합니다.
2. 관리형 권한 목록을 고객 관리형으로 필터링하거나 삭제하려는 버전이 있는 고객 관리형 권한의 이름을 검색합니다.
3. 삭제하려는 버전이 현재 기본 버전이 아닌지 확인합니다.
4. 페이지의 버전 섹션에서 연결된 리소스 공유 탭을 선택하여 이 버전을 사용하는 공유가 있는지 확인합니다.

   연결된 공유가 있는 경우 이 버전을 삭제하기 전에 고객 관리형 권한 버전을 변경해야 합니다.
5. 버전 섹션 오른쪽에 있는 버전 삭제를 선택합니다.
6. 확인 대화 상자에서 삭제를 선택하여 이 버전의 고객 관리형 권한을 삭제할지 확인합니다.

   이 버전의 고객 관리형 권한을 삭제하지 않으려면 취소를 선택합니다.

AWS CLI

고객 관리형 권한의 한 버전을 삭제하려면

1. list-permission-versions 작업을 호출하여 사용 가능한 버전 번호를 검색합니다.
2. 버전 번호를 확인한 후 delete-permission-version에 파라미터로 제공합니다.

```
$ aws ram-cmp delete-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 1
```

성공해도 이 명령은 출력을 반환하지 않습니다. list-permission-versions를 다시 실행하면 해당 버전이 더 이상 출력에 포함되지 않는지 확인할 수 있습니다.

고객 관리형 권한 삭제

더 이상 필요하지 않아 사용하지 않는 고객 관리형 권한은 삭제할 수 있습니다. 리소스 공유와 연결된 고객 관리형 권한은 삭제할 수 없습니다. 삭제된 고객 관리형 권한은 2시간 후에 사라집니다. 그때까지 관리형 권한 라이브러리에 삭제됨 상태로 표시됩니다.

Console

고객 관리형 권한을 삭제하려면

1. 관리형 권한 라이브러리로 이동합니다.
2. 관리형 권한 목록을 고객 관리형으로 필터링하거나 삭제하려는 고객 관리형 권한의 이름을 검색합니다.
3. 고객 관리형 권한을 선택하기 전에 관리형 권한 목록에서 연결된 공유가 0개인지 확인합니다.

   관리되는 권한과 연결된 리소스 공유가 아직 있는 경우, 계속 진행하기 전에 모든 리소스 공유에 다른 관리형 권한을 할당해야 합니다.
4. 고객 관리형 권한 세부 정보 페이지의 오른쪽 상단에 있는 관리형 권한 삭제를 선택합니다.
5. 확인 대화 상자가 나타나면 삭제를 선택하여 관리형 권한을 삭제합니다.

AWS CLI

고객 관리형 권한을 삭제하려면

1. 고객 관리형 권한만 포함하도록 list-permissions를 `--permission-type CUSTOMER_MANAGED` 파라미터와 함께 호출하여 삭제하려는 관리형 권한의 ARN을 찾습니다.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. 삭제할 관리형 권한의 ARN을 확인한 후 delete-permission에 파라미터로 제공합니다.

```
$ aws ram delete-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "returnValue": true,
    "permissionStatus": "DELETING"
}
```

AWS 관리형 권한을 최신 버전으로 업데이트

경우에 따라 AWS에서는 특정 리소스 유형에 대해 리소스 공유에 연결할 수 있는 AWS 관리형 권한을 업데이트합니다. 이 경우 AWS에서 새 버전의 AWS 관리형 권한을 생성합니다. 지정된 리소스 유형을 포함하고 있는 리소스 공유는 최신 버전의 관리형 권한을 사용하도록 자동으로 업데이트되지 않습니

다. 각 리소스 공유의 관리형 권한을 명시적으로 업데이트해야 합니다. 리소스 공유에 변경 사항을 적용하기 전에 변경 사항을 평가하려면 이 추가 단계가 필요합니다.

Console

콘솔에 리소스 공유와 관련된 권한이 나열된 페이지가 표시되고 이러한 권한 중 하나 이상이 해당 권한의 기본 버전이 아닌 다른 버전을 사용하고 있는 경우 콘솔 페이지 상단에 배너가 표시됩니다. 이 배너는 리소스 공유가 기본 버전이 아닌 다른 버전을 사용하고 있음을 나타냅니다.

또한 개별 권한의 버전이 기본 버전이 아닌 경우 현재 버전 번호 옆에 기본 버전으로 업데이트 버튼이 표시될 수 있습니다.

이 버튼을 선택하면 리소스 공유 업데이트 마법사가 시작됩니다. 마법사의 2단계에서 기본 버전이 아닌 권한이 기본 버전을 사용하도록 업데이트할 수 있습니다.

마법사의 마지막 페이지에서 제출을 선택하여 마법사를 완료할 때까지는 변경 사항이 저장되지 않습니다.

> **Note**
>
> 기본 버전만 연결할 수 있고 다른 버전으로 되돌릴 수는 없습니다.
> 고객 관리형 권한의 경우 권한을 기본 버전으로 업데이트한 후에는 먼저 다른 버전을 기본 값으로 설정하지 않는 한 리소스 공유에 다른 버전을 적용할 수 없습니다. 예를 들어 권한을 기본 버전으로 업데이트한 후에 롤백이 필요한 오류가 발견된 경우 이전 버전을 기본 버전으로 지정할 수 있습니다. 또는 다른 새 버전을 생성한 다음 해당 버전을 기본 버전으로 지정할 수도 있습니다. 이러한 옵션 중 하나를 수행한 후에는 현재 기본 버전을 사용하도록 리소스 공유를 업데이트해야 합니다.

AWS CLI

AWS 관리형 권한의 버전을 업데이트하려면

1. get-resource-shares 명령을 `--permission-arn` 파라미터와 함께 실행하여 업데이트하려는 관리형 권한의 Amazon 리소스 이름(ARN)을 지정합니다. 그러면 명령이 해당 관리형 권한을 사용하는 리소스 공유만 반환합니다.

   예를 들어, 다음 샘플 명령은 Amazon EC2 용량 예약의 기본 AWS 관리형 권한을 사용하는 모든 리소스 공유에 대한 세부 정보를 반환합니다.

   ```
   $ aws ram get-resource-shares \
   ```

```
    --resource-owner SELF \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionCapacityReservation
```

출력에는 해당 관리형 권한으로 액세스가 제어되는 리소스가 하나 이상 있는 모든 리소스 공유의 ARN이 포함됩니다.

2. 이전 명령에 지정된 각 리소스 공유에 대해 associate-resource-share-permission 명령을 실행합니다. 업데이트할 리소스 공유를 지정하려면 `--resource-share-arn`을, 업데이트할 AWS 관리형 권한을 지정하려면 `--permission-arn`을, 해당 관리형 권한의 최신 버전을 사용하도록 공유를 업데이트하도록 지정하려면 `--replace` 파라미터를 포함합니다. 기본 버전이 자동으로 사용되므로 버전 번호를 지정할 필요가 없습니다.

```
$ aws ram associate-resource-share-permission \
    --resource-share-arn < ARN of one of the shares from the output of the
 previous command > \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionCapacityReservation \
    --replace
```

3. 1단계의 명령 결과에서 받은 각 `ResourceShareArn`에 대해 이전 단계의 명령을 반복합니다.

AWS RAM에서 고객 관리형 권한을 사용할 때 고려할 사항

고객 관리형 권한은 해당 권한을 생성한 AWS 리전에서만 사용할 수 있습니다. 모든 리소스 유형이 고객 관리형 권한을 지원하는 것은 아닙니다. AWS Resource Access Manager에서 지원되는 리소스 유형 목록은 공유 가능한 리소스 AWS 섹션을 참조하세요.

여러 문이 포함된 고객 관리형 권한은 지원되지 않습니다. 고객 관리 권한에서는 부정 연산자가 아닌 단일 연산자만 사용할 수 있습니다.

고객 관리형 권한에서 다음 조건은 지원되지 않습니다.

- 조직의 보안 주체:
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- 지정된 서비스의 보안 주체:

  - `aws:SourceArn`
  - `aws:SourceAccount`
- 시스템 태그:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

관리형 권한의 작동 방식

간략한 개요를 보려면 관리형 권한을 통해 최소 권한 액세스의 모범 사례를 AWS 리소스에 적용하는 방법을 보여주는 다음 동영상을 시청하세요.

이 동영상에서는 최소 권한 모범 사례에 따라 고객 관리형 권한을 작성하고 연결하는 방법을 보여줍니다. 자세한 내용은 ??? 섹션을 참조하세요.

리소스 공유를 생성할 때 공유하려는 각 리소스 유형에 AWS 관리형 권한을 연결합니다. 관리형 권한의 버전이 두 개 이상인 경우 새 리소스 공유에는 항상 기본 버전으로 지정된 버전이 사용됩니다.

리소스 공유를 생성한 후에는 AWS RAM에서 관리형 권한을 사용하여 각 공유 리소스에 연결된 리소스 기반 정책을 생성합니다.

관리형 권한의 정책 템플릿에서는 다음을 지정합니다.

Effect

공유 리소스에 대한 작업을 수행할 수 있는 보안 주체 권한을 `Allow` 또는 `Deny`할지 여부를 나타냅니다. 관리형 권한의 경우 effect는 항상 `Allow`입니다. 자세한 내용은 IAM 사용 설명서에서 Effect 섹션을 참조하세요.

Action

보안 주체에게 수행 권한이 부여된 작업 목록입니다. AWS Management Console에서는 작업(action)이고, AWS Command Line Interface(AWS CLI) 또는 AWS API에서는 작업(operation)일 수 있습니다. 작업은 AWS 권한을 통해 정의됩니다. 자세한 내용은 IAM 사용 설명서에서 Action 섹션을 참조하세요.

Condition

보안 주체가 리소스 공유의 리소스와 상호 작용할 수 있는 시기와 방법입니다. 조건은 공유 리소스에 보안을 한층 더 강화합니다. 조건을 사용하여 민감한 작업에 대한 액세스를 공유 리소스로 제한할 수 있습니다. 예를 들어, 특정 회사 IP 주소 범위에서 작업을 시작하거나 멀티 팩터 인증으로 인증된 사용자가 작업을 수행하도록 요구하는 조건을 포함시킬 수 있습니다. 조건에 대한 자세한 내용은 IAM 사용 설명서에서 AWS 글로벌 조건 컨텍스트 키를 참조하세요. 서비스별 조건에 대한 자세한 내용은 서비스 승인 참조에서 AWS 서비스서비스에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

> **Note**
>
> 고객 관리형 권한에는 조건을, AWS 관리형 권한에는 지원되는 리소스 유형을 사용할 수 있습니다.
> 고객 관리형 권한 사용에서 제외되는 조건에 대한 자세한 내용은 AWS RAM에서 고객 관리형 권한을 사용할 때 고려할 사항 섹션을 참조하세요.

관리형 권한의 유형

리소스 공유를 생성할 때 리소스 공유에 포함된 각 리소스 유형과 연결할 관리형 권한을 선택하세요. AWS 관리형 권한은 AWS 리소스 소유 서비스에서 정의하고 AWS RAM에서 관리합니다. 고객 관리형 권한은 사용자가 직접 작성하고 유지 관리합니다.

- AWS관리형 권한 - AWS RAM에서 지원하는 모든 리소스 유형에 대해 하나의 기본 관리형 권한을 사용할 수 있습니다. 명시적으로 관리형 권한 중 하나를 추가로 선택하지 않는 한 기본 관리형 권한이 리소스 유형에 사용됩니다. 기본 관리형 권한은 지정된 유형의 리소스를 공유하는 가장 일반적인 고객 시나리오를 지원하기 위한 것입니다. 기본 관리형 권한을 사용하면 해당 리소스 유형에 대해 서비스에서 정의한 특정 작업을 보안 주체가 수행할 수 있습니다. 예를 들어, Amazon VPC `ec2:Subnet` 리소스 유형의 경우 기본 관리형 권한을 통해 보안 주체가 다음 작업을 수행할 수 있습니다.
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  기본 AWS 관리형 권한의 이름은 `AWSRAMDefaultPermission`*`ShareableResourceType`* 형식을 사용합니다. 예를 들어 `ec2:Subnet` 리소스 유형의 경우 기본 AWS 관리형 권한의 이름은 `AWSRAMDefaultPermissionSubnet`입니다.

> **Note**
>
> 기본 관리형 권한은 관리형 권한의 기본 버전과는 다릅니다. 기본 권한이든 일부 리소스 유형에서 지원하는 추가 관리형 권한 중 하나이든 관계없이 모든 관리형 권한은 별도의 완전한 권한으로, 읽기-쓰기 액세스와 읽기 전용 액세스 등 다양한 공유 시나리오를 지원하는 다양한 효과와 작업을 제공합니다. AWS 관리형 권한이든 고객 관리형 권한이든지 간에 모든 관리형 권한에는 여러 버전이 있을 수 있으며, 그 중 하나가 해당 권한의 기본 버전이 됩니다.

예를 들어 전체 액세스(`Read`및`Write`) 관리형 권한과 읽기 전용 관리형 권한을 모두 지원하는 리소스 유형을 공유하는 경우 전체 액세스 관리형 권한을 가진 관리자를 위한 하나의 리소스 공유를 생성할 수 있습니다. 그런 다음 최소 권한 부여 방식에 따라 읽기 전용 관리형 권한을 사용하여 다른 개발자를 위한 별도의 리소스 공유를 생성할 수 있습니다.

> **Note**
>
> AWS RAM과 함께 작동하는 모든 AWS 서비스는 기본 관리형 권한을 적어도 한 개 지원합니다. 각 AWS 서비스에 사용할 수 있는 권한은 관리형 권한 라이브러리 페이지에서 확인할 수 있습니다. 이 페이지에서는 사용 가능한 각 관리형 권한에 대한 세부 정보를 제공합니다. 여기에는 현재 권한과 연결된 리소스 공유, 외부 보안 주체와의 공유 허용 여부(해당하는 경우) 등이 포함됩니다. 자세한 내용은 관리형 권한 보기 섹션을 참조하세요.
>
> 추가 관리형 권한을 지원하지 않는 서비스의 경우 리소스 공유를 생성하면 선택한 리소스 유형에 대해 정의된 기본 권한을 AWS RAM에서 자동으로 적용합니다. 지원되는 경우 관리형 권한 연결 페이지에서 고객 관리형 권한 생성을 선택할 수도 있습니다.

- 고객 관리형 권한 - 고객 관리형 권한은 AWS RAM을 사용하여 공유되는 리소스에 대해 어떤 조건에서 어떤 작업을 수행할 수 있는지 정확하게 지정하여 작성하고 유지 관리하는 관리형 권한입니다. 예를 들어, 대규모로 IP 주소를 관리하는 데 도움이 되도록 Amazon VPC IP 주소 관리자(IPAM) 풀에 대한 읽기 액세스를 제한하려고 합니다. 개발자가 IP 주소를 할당할 수 있는 고객 관리형 권한을 생성할 수 있지만, 다른 개발자 계정이 할당하는 IP 주소 범위를 볼 수는 없습니다. 최소 권한 모범 사례에 따라 공유 리소스에 대한 작업을 수행하는 데 필요한 권한만 부여할 수 있습니다.

AWS RAM의 보안

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

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

- 클라우드의 보안 – AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. 또한, AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. AWS Resource Access Manager(AWS RAM)에 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램 제공 범위 내 AWS 서비스를 참조하십시오.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

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

주제

- AWS RAM의 데이터 보호
- AWS RAM의 I자격 증명 및 액세스 관리
- AWS RAM의 로깅 및 모니터링
- AWS RAM의 복원성
- AWS RAM의 인프라 보안

AWS RAM의 데이터 보호

AWS 공동 책임 모델은 AWS Resource Access Manager의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 이 콘텐츠에는 사용하는 AWS 서비스 서비스의 보안 구성과 관리 작업이 포함돼 있습니다. 데이터 프라이버시에 대한

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

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

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

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

AWS RAM의 I자격 증명 및 액세스 관리

AWS Identity and Access Management(IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 지원하는 AWS 서비스입니다. IAM 관리자는 어떤 사용자가 AWS 리소스를 사용하도록 인증(로그인)되고 권한이 부여(권한 있음)되는지 제어합니다. IAM을 사용하면 AWS 계정에서 역할, 사용자, 그룹과 같은 보안 주체를 생성할 수 있습니다. 이러한 보안 주체가 AWS 리소스를 통해 작업을 수행할 수 있는 권한을 제어합니다. IAM은 추가 요금 없이 사용할 수 있습니다. 사용자 지정 IAM 정책 관리 및 생성에 대한 자세한 내용 IAM 사용 설명서에서 IAM 정책 관리를 참조하세요.

주제

- AWS RAM에서 IAM을 사용하는 방식
- AWS RAM의 AWS 관리형 정책

- AWS RAM에 서비스 연결 역할 사용
- AWS RAM에 대한 예제 IAM 정책
- AWS Organizations 및 AWS RAM에 대한 예제 서비스 제어 정책
- AWS Organizations와의 리소스 공유 비활성화

AWS RAM에서 IAM을 사용하는 방식

기본적으로 IAM 보안 주체는 AWS RAM 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. IAM 보안 주체가 리소스를 생성 또는 수정하고 작업을 수행할 수 있도록 허용하려면 다음 단계 중 하나를 수행합니다. 이러한 작업은 특정 리소스 및 API 작업을 사용할 수 있는 권한을 부여합니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가합니다.

- AWS IAM Identity Center의 사용자 및 그룹:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따르세요.
- 자격 증명 공급자를 통해 IAM에서 관리되는 사용자:

  아이덴티티 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기(연합)의 지침을 따르세요.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 IAM 사용자의 역할 생성의 지침을 따르세요.
  - (권장되지 않음) 정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자에 권한 추가(콘솔)의 지침을 따르세요.

AWS RAM은 많은 사용자의 요구를 해결하는 데 사용할 수 있는 몇 가지 AWS 관리형 정책을 제공합니다. 이에 대한 자세한 내용은 AWS RAM의 AWS 관리형 정책 섹션을 참조하세요.

사용자에게 부여하는 권한을 더 세밀하게 제어해야 하는 경우 IAM 콘솔에서 자체 정책을 구성할 수 있습니다. 정책을 생성하여 IAM 역할 및 사용자에게 연결하는 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서에서 IAM의 정책 및 권한을 참조하세요.

다음 섹션에서는 IAM 권한 정책 구축에 대한 AWS RAM 관련 세부 정보를 제공합니다.

목차

정책 구조

IAM 권한 정책은 Effect, Action, Resource, Condition 문이 포함되어 있는 JSON 문서입니다. IAM 정책의 형식은 일반적으로 다음과 같습니다.

```
{
    "Statement":[{
        "Effect":"<effect>",
        "Action":"<action>",
        "Resource":"<arn>",
        "Condition":{
            "<comparison-operator>":{
                "<key>":"<value>"
            }
        }
    }]
}
```

Effect

Effect 문은 정책에서 보안 주체의 작업 수행 권한을 허용하는지 또는 거부하는지 여부를 나타냅니다. 가능한 값은 `Allow` 및 `Deny`입니다.

Action

Action 문은 정책에서 권한을 허용하거나 거부하는 AWS RAM API 작업을 지정합니다. 허용되는 작업의 전체 목록은 IAM 사용 설명서에서 AWS Resource Access Manager에서 정의한 작업을 참조하세요.

Resource

Resource 문은 정책의 영향을 받는 AWS RAM 리소스를 지정합니다. 문에서 리소스를 지정하려면 고유한 Amazon 리소스 이름(ARN)을 사용해야 합니다. 허용되는 리소스의 전체 목록은 IAM 사용 설명서에서 AWS Resource Access Manager에서 정의한 리소스를 참조하세요.

Condition

Condition 문은 선택 사항으로, 정책 적용 조건을 더욱 세분화하는 데 사용할 수 있습니다. AWS RAM에서 지원되는 조건 키는 다음과 같습니다.

- `aws:RequestTag/${TagKey}` - 서비스 요청에 지정된 태그 키를 가진 태그가 포함되어 있고 지정된 값을 갖는지 테스트합니다.
- `aws:ResourceTag/${TagKey}` - 서비스 요청의 영향을 받는 리소스에 정책에 지정된 태그 키와 일치하는 태그가 연결되어 있는지 테스트합니다.

  다음 예제 조건은 서비스 요청에 참조된 리소스에 키 이름이 "Owner"이고 값이 "Dev Team"인 태그가 연결되어 있는지 확인합니다.

```
"Condition" : {
    "StringEquals" : {
        "aws:ResourceTag/Owner" : "Dev Team"
    }
}
```

- `aws:TagKeys` – 리소스 공유를 생성하거나 태그 지정할 때 사용해야 하는 태그 키를 지정합니다.
- `ram:AllowsExternalPrincipals` - 서비스 요청의 리소스 공유가 외부 보안 주체와의 공유를 허용하는지 테스트합니다. 외부 보안 주체는 AWS Organizations 조직의 외부에 있는 AWS 계정입니다. `False`로 평가되면 이 리소스 공유를 동일한 조직의 계정과만 공유할 수 있습니다.
- `ram:PermissionArn` - 서비스 요청에 지정된 권한 ARN이 정책에 지정된 ARN 문자열과 일치하는지 테스트합니다.
- `ram:PermissionResourceType` - 서비스 요청에 지정된 권한이 정책에 지정된 리소스 유형에 유효한지 테스트합니다. 공유 가능한 리소스 유형 목록에 표시된 형식을 사용하여 리소스 유형을 지정합니다.
- `ram:Principal` - 서비스 요청에 지정된 보안 주체의 ARN이 정책에 지정된 ARN 문자열과 일치하는지 테스트합니다.
- `ram:RequestedAllowsExternalPrincipals` - 서비스 요청에 `allowExternalPrincipals` 파라미터가 포함되어 있는지, 해당 파라미터의 인수가 정책에 지정된 값과 일치하는지 테스트합니다.
- `ram:RequestedResourceType` - 영향을 받는 리소스의 리소스 유형이 정책에 지정된 리소스 유형 문자열과 일치하는지 테스트합니다. 공유 가능한 리소스 유형 목록에 표시된 형식을 사용하여 리소스 유형을 지정합니다.

- `ram:ResourceArn` - 서비스 요청의 영향을 받는 리소스의 ARN이 정책에 지정된 ARN과 일치하는지 테스트합니다.
- `ram:ResourceShareName` - 서비스 요청의 영향을 받는 리소스 공유의 이름이 정책에 지정된 문자열과 일치하는지 테스트합니다.
- `ram:ShareOwnerAccountId` - 서비스 요청의 영향을 받는 리소스 공유의 계정 ID 번호가 정책에 지정된 문자열과 일치하는지 테스트합니다.

AWS RAM의 AWS 관리형 정책

AWS Resource Access Manager은 현재 이 주제에 설명된 여러 AWS RAM 관리형 정책을 제공합니다.

AWS 관리형 정책

- AWS 관리형 정책: AWSResourceAccessManagerReadOnlyAccess
- AWS 관리형 정책: AWSResourceAccessManagerFullAccess
- AWS 관리형 정책: AWSResourceAccessManagerResourceShareParticipantAccess
- AWS 관리형 정책: AWSResourceAccessManagerServiceRolePolicy
- AWS 관리형 정책으로 AWS RAM 업데이트

위 목록에서 처음 세 개의 정책은 IAM 역할, 그룹 및 사용자에 연결하여 권한을 부여할 수 있습니다. 목록의 마지막 정책은 AWS RAM 서비스의 서비스 연결 역할용으로 예약되어 있습니다.

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

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

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

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSResourceAccessManagerReadOnlyAccess

`AWSResourceAccessManagerReadOnlyAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 AWS 계정 소유의 리소스 공유에 대한 읽기 전용 권한을 제공합니다.

이를 위해 `Get*` 또는 `List*` 작업의 실행 권한을 부여합니다. 리소스 공유를 수정할 수 있는 기능은 제공하지 않습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `ram` - 보안 주체가 계정 소유의 리소스 공유에 대한 세부 정보를 볼 수 있도록 허용합니다.

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

AWS 관리형 정책: AWSResourceAccessManagerFullAccess

`AWSResourceAccessManagerFullAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 AWS 계정 소유의 리소스 공유를 보거나 수정할 수 있는 전체 관리 액세스 권한을 제공합니다.

이를 위해 `ram` 작업 실행 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- ram - 보안 주체가 AWS 계정 소유의 리소스 공유에 대한 정보를 보거나 수정할 수 있도록 허용합니다.

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

AWS 관리형 정책: AWSResourceAccessManagerResourceShareParticipantAccess

AWSResourceAccessManagerResourceShareParticipantAccess 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 보안 주체에게 이 AWS 계정과 공유되는 리소스 공유를 수락하거나 거부하고 이러한 리소스 공유에 대한 세부 정보를 볼 수 있는 기능을 제공합니다. 이러한 리소스 공유를 수정할 수 있는 기능은 제공하지 않습니다.

이를 위해 일부 ram 작업의 실행 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- ram - 보안 주체가 리소스 공유 초대를 수락하거나 거부하고 계정과 공유된 리소스 공유에 대한 세부 정보를 볼 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:GetResourcePolicies",
```

```
                "ram:GetResourceShareInvitations",
                "ram:GetResourceShares",
                "ram:ListPendingInvitationResources",
                "ram:ListPrincipals",
                "ram:ListResources",
                "ram:RejectResourceShareInvitation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSResourceAccessManagerServiceRolePolicy

AWS 관리형 정책 `AWSResourceAccessManagerServiceRolePolicy`는 AWS RAM에 대한 서비스 연결 역할에만 사용할 수 있습니다. 이 정책은 연결, 분리, 수정 또는 삭제할 수 없습니다.

이 정책은 조직 구조에 대한 읽기 전용 액세스를 AWS RAM에 제공합니다. AWS RAM과 AWS Organizations 간의 통합을 활성화하면 AWSServiceRoleForResourceAccessManager라는 서비스 연결 역할을 AWS RAM에서 자동으로 생성하는데, AWS RAM 콘솔에서 조직의 구조를 볼 때와 같이 조직 및 조직 계정에 대한 정보를 조회해야 할 때 서비스에서 이 역할을 맡습니다.

이를 위해 조직의 구조 및 계정에 대한 세부 정보를 제공하는 `organizations:Describe` 및 `organizations:List` 작업을 실행할 수 있는 읽기 전용 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `organizations` - 보안 주체가 조직 단위 및 조직에 포함된 AWS 계정을 포함하여 조직의 구조에 대한 정보를 볼 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
```

```
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
            ]
        }
    ]
}
```

AWS 관리형 정책으로 AWS RAM 업데이트

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

변경 사항	설명	날짜
AWS Resource Access Manager에서 변경 사항 추적 시작	AWS RAM에서 기존 관리 정책을 문서화하고 변경 사항을 추적하기 시작했습니다.	2021년 9월 16일

AWS RAM에 서비스 연결 역할 사용

AWS Resource Access Manager은 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 AWS RAM 서비스에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS에서 미리 정의되며 AWS RAM에서 사용자를 대신하여 기타 AWS 서비스를 자동으로 호출하는 데 필요한 모든 권한을 포함하고 있습니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 AWS RAM을 더 쉽게 구성할 수 있습니다. AWS RAM에서 서비스 연결 역할의 권한을 정의하므로, 달리 정의되지 않은 한 AWS RAM에서만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 모두 포함되며, 권한 정책은 다른 IAM 개체에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조해 서비스 연결 역할(Service-Linked Role) 열이 예(Yes)인 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

AWS RAM에 대한 서비스 연결 역할 권한

AWS Organizations과의 공유를 활성화하면 AWS RAM에서 `AWSServiceRoleForResourceAccessManager`라는 서비스 연결 역할을 사용합니다. 이 역할은 멤버 계정 목록, 각 계정이 속한 조직 단위 등의 조직 세부 정보를 볼 수 있는 권한을 AWS RAM 서비스에 부여합니다.

이 서비스 연결 역할은 역할을 위임하기 위해 다음 서비스를 신뢰합니다.

- `ram.amazonaws.com`

AWSResourceAccessManagerServiceRolePolicy라는 역할 권한 정책이 이 서비스 연결 역할에 연결되어 있으며, AWS RAM에서 지정된 리소스에 대해 다음 작업을 수행할 수 있도록 허용합니다.

- 작업: 조직 구조에 대한 세부 정보를 검색하는 읽기 전용 작업입니다. 전체 작업 목록은 IAM 콘솔에서 AWS ResourceAccessManagerServicerPolicy 정책을 확인할 수 있습니다.

보안 주체가 조직 내 AWS RAM 공유를 활성화하려면 해당 보안 주체(사용자, 그룹, 역할 등의 IAM 개체)에게 서비스 연결 역할을 생성할 수 있는 권한이 있어야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

AWS RAM에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console에서 조직 내 AWS RAM 공유를 활성화하거나 AWS CLI 또는 AWS API를 사용하여 계정에서 EnableSharingWithAwsOrganization를 실행하면 AWS RAM에서 서비스 연결 역할을 자동으로 생성합니다.

이 서비스 연결 역할을 삭제하면 조직 구조의 세부 정보를 볼 수 있는 권한이 더 이상 AWS RAM에 없습니다.

AWS RAM에 대한 서비스 연결 역할 편집

AWS RAM은 AWSSSMOpsInsightsServiceRolePolicy 서비스 연결 역할의 편집을 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AWS RAM에 대한 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수 있습니다.

IAM을 사용하여 수동으로 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 `AWSResourceAccessManagerServiceRolePolicy` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

AWS RAM 서비스 연결 역할을 지원하는 리전

AWS RAM에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 Amazon Web Services 일반 참조의 AWS Regions and endpoints를 참조하세요.

AWS RAM에 대한 예제 IAM 정책

이 주제에서는 특정 리소스 및 리소스 유형을 공유하고 공유를 제한하는 방법을 보여주는 AWS RAM에 대한 IAM 정책의 예를 다룹니다.

IAM 정책의 예

- 예 1: 특정 리소스 공유 허용
- 예 2: 특정 리소스 유형 공유 허용
- 예 3: 외부 AWS 계정과의 공유 제한

예 1: 특정 리소스 공유 허용

IAM 권한 정책을 사용하여 보안 주체가 특정 리소스만 리소스 공유와 연결하도록 제한할 수 있습니다.

예를 들어, 다음 정책은 보안 주체가 지정된 Amazon 리소스 이름 (ARN)을 사용하는 해석기 규칙만 공유하도록 제한합니다. 요청에 `ResourceArn` 파라미터가 포함되어 있지 않거나 해당 파라미터가 포함되어 있으며 값이 지정된 ARN과 정확히 일치하는 경우 `StringEqualsIfExists` 연산자는 요청을 허용합니다.

`...IfExists` 연산자를 사용하는 시기와 이유에 대한 자세한 내용은 IAM 사용 설명서에서 ...IfExists 조건 연산자를 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
            }
        }
    }]
}
```

예 2: 특정 리소스 유형 공유 허용

IAM 정책을 사용하여 보안 주체가 특정 리소스 유형만 리소스 공유와 연결하도록 제한할 수 있습니다.

예를 들어, 다음 정책은 보안 주체가 해석기 규칙만 공유하도록 제한합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    }]
}
```

예 3: 외부 AWS 계정과의 공유 제한

IAM 정책을 사용하여 보안 주체가 AWS 조직 외부에 있는 AWS 계정과 리소스를 공유하지 못하도록 할 수 있습니다.

예를 들어, 다음 IAM 정책은 보안 주체가 리소스 공유에 외부 AWS 계정을 추가하지 못하도록 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "ram:CreateResourceShare",
        "Resource": "*",
        "Condition": {
            "Bool": {
                "ram:RequestedAllowsExternalPrincipals": "false"
            }
        }
    }]
}
```

AWS Organizations 및 AWS RAM에 대한 예제 서비스 제어 정책

AWS RAM은 서비스 제어 정책(SCP)을 지원합니다. SCP는 조직 내 구성 요소에 연결하여 해당 조직 내의 권한을 관리하는 정책입니다. SCP는 SCP를 연결하는 요소 아래의 모든 AWS 계정에 적용됩니다. SCP는 조직의 모든 계정에 사용 가능한 최대 권한을 중앙에서 제어합니다. SCP를 사용하면 조직의 액세스 제어 지침에 따라 AWS 계정을 유지할 수 있습니다. 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.

사전 조건

SCP를 사용하려면 먼저 다음 사항을 수행해야 합니다.

- 조직 내에서 모든 기능을 활성화합니다. 자세한 내용은 AWS Organizations 사용 설명서에서 조직 내 모든 기능 활성화를 참조하세요.
- 조직 내에서 사용할 수 있도록 SCP를 활성화합니다. 자세한 내용은 AWS Organizations 사용 설명서에서 정책 유형 활성화 및 비활성화를 참조하세요.
- 필요한 SCP를 생성합니다. SCP를 생성하는 방법에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 SCP 생성 및 업데이트를 참조하세요.

예제 서비스 제어 정책

목차

- 예 2: 사용자가 조직 외부의 외부 계정으로부터 받은 리소스 공유 초대를 수락하지 못하도록 방지
- 예 3: 특정 계정에서 특정 리소스 유형 공유 허용
- 예 4: 전체 조직 또는 조직 단위와의 공유 금지
- 예 5: 특정 보안 주체와만 공유 허용

다음 예에서는 조직에서 리소스 공유의 다양한 측면을 제어할 수 있는 방법을 보여줍니다.

예 1: 외부 공유 금지

다음 SCP는 사용자가 공유 사용자의 조직 외부에 있는 보안 주체와의 공유를 허용하는 리소스 공유를 만들지 못하도록 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

예 2: 사용자가 조직 외부의 외부 계정으로부터 받은 리소스 공유 초대를 수락하지 못하도록 방지

다음 SCP는 해당 계정의 모든 보안 주체가 리소스 공유 사용 초대를 수락하지 못하도록 차단합니다. 공유 계정과 동일한 조직의 다른 계정으로 공유되는 리소스 공유는 초대가 생성되지 않으므로 이 SCP의 영향을 받지 않습니다.

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

```
            "Effect": "Deny",
            "Action": "ram:AcceptResourceShareInvitation",
            "Resource": "*"
        }
    ]
}
```

예 3: 특정 계정에서 특정 리소스 유형 공유 허용

다음 SCP는 111111111111 및 222222222222 계정만 Amazon EC2 접두사 목록을 공유하는 새 리소스 공유를 생성하거나 접두사 목록을 기존 리소스 공유와 연결할 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEqualsIfExists": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

예 4: 전체 조직 또는 조직 단위와의 공유 금지

다음 SCP는 사용자가 전체 조직 또는 조직 단위와 리소스를 공유하는 리소스 공유를 생성하지 못하도록 합니다. 사용자는 조직의 개별 AWS 계정 또는 IAM 역할 또는 사용자와 공유할 수 있습니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

예 5: 특정 보안 주체와만 공유 허용

다음 SCP 예제는 사용자에게 조직 o-12345abcdef,, 조직 단위 ou-98765fedcba, AWS 계정 111111111111과의 리소스 공유만 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
```

```
                    "111111111111"
                ]
            }
        }
    }
]
}
```

AWS Organizations와의 리소스 공유 비활성화

이전에 AWS Organizations와의 공유를 활성화했는데 더 이상 전체 조직 또는 조직 단위(OU)와 리소스를 공유할 필요가 없는 경우 공유를 비활성화할 수 있습니다. AWS Organizations와의 공유를 비활성화하면 생성한 리소스 공유에서 모든 조직 또는 OU가 제거되고 공유 리소스에 액세스할 수 없게 됩니다.

AWS Organizations와의 공유를 비활성화하려면

1. AWS Organizations disable-aws-service-access AWS CLI 명령을 사용하여 AWS Organizations에 대한 신뢰할 수 있는 액세스를 비활성화합니다.

   ```
   $  aws organizations disable-aws-service-access --service-principal
    ram.amazonaws.com
   ```

   > **Important**
   >
   > AWS Organizations에 대한 신뢰할 수 있는 액세스를 비활성화하면 조직 내 보안 주체가 모든 리소스 공유에서 제거되고 해당 공유 리소스에 액세스할 수 없게 됩니다.

2. IAM 콘솔, AWS CLI 또는 IAM API를 사용하여 AWSServiceRoleForResourceAccessManager 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

AWS RAM의 로깅 및 모니터링

모니터링은 AWS RAM와 사용자 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 중요한 역할을 합니다. 다중 지점 실패가 발생할 경우 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분으로부터 모니터링 데이터를 수집해야 합니다. AWS는 AWS RAM 리소스를 모니터링하고 잠재적 인시던트에 대응하기 위한 여러 도구를 제공합니다.

Amazon CloudWatch Events

AWS 리소스의 변경 사항을 설명하는 실시간에 가까운 시스템 이벤트 스트림을 제공합니다. CloudWatch Events는 특정 이벤트를 감시하는 규칙을 작성하고 이러한 이벤트가 발생할 때 다른 AWS 서비스에서 자동화된 작업을 트리거할 수 있으므로 자동화된 이벤트 기반 컴퓨팅이 가능합니다. 자세한 내용은 CloudWatch Events를 사용하여 AWS RAM 모니터링 섹션을 참조하세요.

AWS CloudTrail

직접 수행하거나 AWS 계정을 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지, 어떤 소스 IP 주소에 호출이 이루어졌는지, 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail을 사용하여 AWS RAM API 호출 로깅 섹션을 참조하세요.

CloudWatch Events를 사용하여 AWS RAM 모니터링

Amazon CloudWatch Events를 사용하면 AWS RAM의 특정 이벤트에 대한 자동 알림을 설정할 수 있습니다. AWS RAM에서 발생하는 이벤트는 거의 실시간으로 CloudWatch Events로 전달됩니다. 리소스 공유의 변경을 나타내는 이벤트에 대한 응답으로 이벤트를 모니터링하고 대상을 호출하도록 CloudWatch Events를 구성할 수 있습니다. 리소스 공유를 변경하면 리소스 공유 소유자와 리소스 공유에 대한 액세스 권한이 부여된 보안 주체 모두에게 이벤트가 트리거됩니다.

이벤트 패턴을 생성할 때 소스는 `aws.ram`입니다.

> **Note**
>
> 이러한 이벤트에 의존하는 코드는 주의해서 작성하세요. 이러한 이벤트는 보장되지 않지만 최상의 노력에 따라 발생됩니다. AWS RAM에서 이벤트 발생을 시도할 때 오류가 발생하면 서비스에서 여러 번 더 시도합니다. 하지만 시간이 초과되어 특정 이벤트가 손실될 수 있습니다.

자세한 내용은 Amazon CloudWatch Events 사용 설명서를 참조하세요.

예: 리소스 공유 실패에 대한 알림

Amazon EC2 용량 예약을 조직의 다른 계정과 공유하려는 시나리오를 생각해 보세요. 이렇게 하면 비용을 절감할 수 있습니다.

하지만 용량 예약 공유를 위한 사전 조건을 모두 충족하지 못할 경우 리소스 공유와 관련된 비동기 작업이 자동으로 수행되지 않을 수 있습니다. 공유 작업이 실패하고 다른 계정의 사용자가 해당 용량 예

약 중 하나를 사용하여 인스턴스를 시작하려고 하면 Amazon EC2는 용량 예약이 꽉 찬 것처럼 작동하고 대신 해당 인스턴스를 온디맨드 인스턴스로 시작합니다. 이로 인해 비용이 예상보다 높아질 수 있습니다.

리소스 공유 실패를 모니터링하려면 AWS RAM에서 리소스 공유에 실패할 때마다 알림을 보내도록 Amazon CloudWatch Events 규칙을 설정하세요. 다음 자습서 절차에서는 Amazon Simple Notification Service(SNS) 주제를 사용하여 EventBridge에서 리소스 공유 실패를 발견할 때마다 모든 주제 구독자에게 알립니다. Amazon SNS에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서를 참조하세요.

리소스 공유 실패 시 알려주는 규칙을 만들려면

1. Amazon EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택한 다음 규칙 목록에서 규칙 생성을 선택합니다.
3. 규칙의 이름과 설명(선택 사항)을 입력하고 다음을 선택합니다.
4. 이벤트 패턴 상자까지 아래로 스크롤하여 사용자 지정 패턴(JSON 편집기)을 선택합니다.
5. 다음 이벤트 패턴을 복사하여 붙여넣습니다.

```
{
  "source": ["aws.ram"],
  "detail-type": ["Resource Sharing State Change"],
  "detail": {
    "event": ["Resource Share Association"],
    "status": ["failed"]
  }
}
```

6. 다음을 선택합니다.
7. 대상 1의 대상 선택에서 AWS 서비스를 선택합니다.
8. 대상 선택에서 SNS 주제를 선택합니다.
9. 주제에서 알림을 게시할 SNS 주제를 선택합니다. 이미 있는 주제여야 합니다.
10. 다음을 선택한 후 다음을 다시 선택하여 구성을 검토합니다.
11. 옵션이 만족스러우면 규칙 생성을 선택합니다.
12. 규칙 페이지로 돌아가서 새 규칙이 활성화됨으로 표시되었는지 확인합니다. 필요한 경우 규칙 이름 옆에 있는 라디오 버튼을 선택한 다음 활성화를 선택합니다.

이 규칙이 활성화되어 있는 한, AWS RAM 리소스 공유가 실패할 경우 게시한 주제의 수신자에게 SNS 알림이 생성됩니다.

또한 공유 용량 예약을 공유한 계정에서 공유 용량 예약에 액세스할 수 있는지 확인하려면 해당 계정을 통해 Amazon EC2 콘솔에서 확인을 시도하면 됩니다.

AWS CloudTrail을 사용하여 AWS RAM API 호출 로깅

AWS RAM는 AWS RAM에서 사용자, 역할, 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail와 통합됩니다. CloudTrail은 AWS RAM에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS RAM 콘솔로부터의 호출과 AWS RAM API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 AWS RAM 이벤트를 포함한 CloudTrail 이벤트를 지정한 Amazon S3 버킷에 지속적으로 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 AWS RAM에 대한 요청, 요청 IP 주소, 요청자, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 AWS RAM 정보

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

AWS RAM에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- AWS 계정에 대한 추적 생성
- CloudTrail 로그와 AWS 서비스 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

모든 AWS RAM 작업은 CloudTrail에서 로깅되고 AWS RAM API 참조에 기록됩니다. 예를 들어 `CreateResourceShare`, `AssociateResourceShare` 및

`EnableSharingWithAwsOrganization` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 누가 요청했는지 확인하는 데 도움이 되는 정보가 포함되어 있습니다.

- AWS 계정 루트 자격 증명
- AWS Identity and Access Management(IAM) 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명
- IAM 사용자의 장기 보안 자격 증명.
- 또 다른 AWS 서비스.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

AWS RAM 로그 파일 항목 이해

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

다음 예제는 `CreateResourceShare` 작업에 대한 CloudTrail 로그 항목을 표시합니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "NOPIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "BCDIOSFODNN7EXAMPLE",
        "userName": "admin"
    },
    "eventTime": "2018-11-03T04:23:19Z",
    "eventSource": "ram.amazonaws.com",
    "eventName": "CreateResourceShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.1.0",
    "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
    "requestParameters": {
        "name": "foo"
```

```
    },
    "responseElements": {
        "resourceShare": {
            "allowExternalPrincipals": true,
            "name": "foo",
            "owningAccountId": "111122223333",
            "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
            "status": "ACTIVE"
        }
    },
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


AWS RAM의 복원성

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

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

AWS RAM의 인프라 보안

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

AWS에서 게시한 API 호출을 사용하여 네트워크를 통해 AWS RAM에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.

- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

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

AWS RAM 문제 해결

설명서의 이 섹션에 설명된 정보를 참조하여 AWS Resource Access Manager(AWS RAM)로 작업할 때 발생하는 일반적인 문제를 진단하고 해결할 수 있습니다.

주제

오류: “AWS 조직에 계정 ID가 존재하지 않음”

시나리오

조직의 계정 또는 조직 단위(OU)와 리소스를 공유하려고 할 때 "AWS 조직에 계정 ID가 존재하지 않음"이라는 오류가 발생합니다.

원인

이 오류는 AWS Resource Access Manager 및 AWS Organizations 간의 통합을 활성화할 때 서비스 연결 역할 AWSServiceRoleForResourceAccessManager가 성공적으로 생성되지 않은 경우에 발생할 수 있습니다.

솔루션

필요한 서비스 연결 역할을 다시 생성하려면 다음 단계를 수행하여 통합을 해제한 다음 다시 활성화하세요.

1. IAM 역할 또는 관리 권한이 있는 사용자로 조직의 관리 계정에 로그인합니다.
2. AWS Organizations 콘솔에서 서비스 페이지로 이동합니다.

3. RAM을 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS RAM 콘솔에서 설정 페이지로 이동합니다.
6. 다음 대상과 공유 활성화: AWS Organizations를 선택한 다음 설정 저장을 선택합니다.

이제 AWS RAM을 사용하여 조직의 계정 및 OU와 리소스를 공유할 수 있어야 합니다.

오류: "AccessDeniedException"

시나리오

리소스를 공유하거나 리소스 공유를 보려고 할 때 액세스 거부됨 예외가 발생합니다.

원인

필요한 권한이 없을 때 리소스 공유를 생성하려고 하면 이 오류가 발생할 수 있습니다. 이는 AWS Identity and Access Management(IAM) 보안 주체에 연결된 정책의 권한이 충분하지 않기 때문일 수 있습니다. 또한 AWS 계정에게 영향을 미치는 AWS Organizations 서비스 제어 정책(SCP)의 제한으로 인해 발생할 수도 있습니다.

솔루션

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가합니다.

- AWS IAM Identity Center의 사용자 및 그룹:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따르세요.
- 자격 증명 공급자를 통해 IAM에서 관리되는 사용자:

  아이덴티티 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기(연합)의 지침을 따르세요.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 IAM 사용자의 역할 생성의 지침을 따르세요.
  - (권장되지 않음) 정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자에 권한 추가(콘솔)의 지침을 따르세요.

이 오류를 해결하려면 요청을 하는 보안 주체가 사용하는 권한 정책에서 `Allow` 문으로 권한이 부여되었는지 확인해야 합니다. 또한 조직의 SCP로 권한을 차단해서는 안됩니다.

리소스 공유를 생성하려면 다음 두 가지 권한이 필요합니다.

- `ram:CreateResourceShare`
- `ram:AssociateResourceShare`

리소스 공유를 보려면 다음 권한이 필요합니다.

- `ram:GetResourceShares`

리소스 공유에 권한을 연결하려면 다음 권한이 필요합니다.

- *`resourceOwningService`*`:`*`PutPolicyAction`*

  이것은 자리 표시자입니다. 공유하려는 리소스를 소유하고 있는 서비스의 "'PutPolicy" 권한(또는 이에 동등한 권한)으로 대체해야 합니다. 예를 들어, Route 53 해석기 규칙을 공유하는 경우 필요한 권한은 `route53resolver:PutResolverRulePolicy`입니다. 여러 리소스 유형이 포함된 리소스 공유를 생성하도록 허용하려면 허용하려는 각 리소스 유형에 대한 관련 권한을 포함시켜야 합니다.

다음 예에서는 IAM 권한 정책의 구조를 보여줍니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare",
                "ram:GetResourceShares",
                "resourceOwningService:PutPolicyAction"
            ],
            "Resource": "*"
        }
    ]
}
```

오류: "UnknownResourceException"

시나리오

다음 오류 중 하나가 발생합니다.

- "CannotCreateResourceShare: UnknownResourceException: OrganizationalUnit ou-*xxxx*를 찾을 수 없음"
- "CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou-*xxxx*를 찾을 수 없음"

원인

이러한 오류는 AWS RAM 콘솔 대신 Organizations 콘솔 또는 Organizations EnableAwsServiceAccess API를 사용하여 AWS RAM 및 AWS Organizations 간의 통합을 활성화하는 경우에 발생할 수 있습니다. Organizations 콘솔 또는 API를 사용하여 통합을 활성화하면 서비스가 사용자 계정에 `AWSServiceRoleForResourceAccessManager` 역할을 생성하지 않습니다. 이 역할은 조직에 대한 정보에 액세스하는 데 필요합니다. 역할이 생성되지 않았으므로 AWS RAM에서 조직의 계정 또는 조직 단위(OU)에 대한 세부 정보에 액세스할 수 없습니다.

솔루션

이 문제를 해결하려면 AWS RAM 및 AWS Organizations 간의 통합을 해제합니다. 그런 다음 AWS RAM EnableSharingWithAwsOrganization 작업을 호출하거나 AWS Management Console에서 다음 단계를 수행하여 다시 활성화합니다.

1. IAM 역할 또는 관리 권한이 있는 사용자로 조직의 관리 계정에 로그인합니다.
2. AWS Organizations 콘솔에서 서비스 페이지로 이동합니다.
3. RAM을 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS RAM 콘솔에서 설정 페이지로 이동합니다.
6. 다음 대상과 공유 활성화: AWS Organizations를 선택한 다음 설정 저장을 선택합니다.

이제 AWS RAM을 사용하여 조직의 계정 및 OU와 리소스를 공유할 수 있어야 합니다.

조직 외부 계정과 공유하려고 할 때 오류가 발생함

시나리오

조직 외부의 계정과 리소스를 공유하려고 할 때 다음 오류 중 하나가 발생합니다.

- "조직 외부에서는 리소스를 공유할 수 없습니다."
- "공유하려는 리소스는 AWS 조직 내에서만 공유할 수 있습니다."
- "InvalidParameterException: 보안 주체 계정 ID가 AWS 조직에 없습니다." 리소스 공유에 외부 AWS 계정를 추가할 수 있는 권한이 없습니다."
- "OperationNotPermittedException: 공유하려는 리소스는 AWS 조직 내에서만 공유할 수 있습니다."

가능한 원인 및 해결 방법

일부 리소스 유형은 동일한 조직의 계정과만 공유할 수 있음

일부 리소스 유형은 해당 조직의 멤버가 아닌 계정과 공유할 수 없습니다. 이러한 제한이 적용되는 리소스 유형의 예로는 Amazon Elastic Compute Cloud(Amazon EC2)에 속하는 가상 프라이빗 연결(VPC)이 있습니다.

특정 리소스 유형을 조직 외부의 계정 및 보안 주체와 공유할 수 있는지 확인하려면 공유 가능한 AWS 리소스를 참조하세요.

서비스 연결 역할이 성공적으로 생성되지 않음

이 문제는 AWS RAM 및 AWS Organizations 간의 통합을 활성화했을 때 서비스 연결 역할 `AWSServiceRoleForResourceAccessManager`가 성공적으로 생성되지 않은 경우에 발생할 수 있습니다.

조직에 속한 계정과 리소스를 공유하려고 시도할 때 이러한 오류 중 하나가 발생할 경우 다음 단계를 수행하여 서비스 연결 역할을 삭제하고 다시 생성하세요.

1. IAM 역할 또는 관리 권한이 있는 사용자로 조직의 관리 계정에 로그인합니다.
2. AWS Organizations 콘솔에서 서비스 페이지로 이동합니다.
3. RAM을 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.

5. AWS RAM 콘솔에서 설정 페이지로 이동합니다.
6. 다음 대상과 공유 활성화: AWS Organizations를 선택한 다음 설정 저장을 선택합니다.

대상 계정에서 공유 리소스를 볼 수 없음

시나리오

사용자가 AWS 계정에서 공유되었다고 생각하는 리소스를 볼 수 없습니다.

가능한 원인 및 해결 방법

AWS RAM 대신 Organizations를 사용하여AWS Organizations와의 공유가 활성화됨

AWS RAM 대신 Organizations를 사용하여 AWS Organizations가 활성화된 경우 조직 내 공유가 실패합니다. 이것이 문제의 원인인지 확인하려면 AWS RAM 콘솔의 설정 페이지로 이동하여 공유 활성화 AWS Organizations 확인란이 선택되어 있는지 확인하세요.

- 확인란이 선택되어 있다면 원인이 아닙니다.
- 확인란이 선택되어 있지 않다면 원인일 수 있습니다. 아직 확인란을 선택하지 말고 다음 단계를 수행하여 상황을 해결하세요.

1. IAM 역할 또는 관리 권한이 있는 사용자로 조직의 관리 계정에 로그인합니다.
2. AWS Organizations 콘솔에서 서비스 페이지로 이동합니다.
3. RAM을 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS RAM 콘솔에서 설정 페이지로 이동합니다.
6. 다음 대상과 공유 활성화: AWS Organizations를 선택한 다음 설정 저장을 선택합니다.

공유할 조직 내에서 공유를 업데이트하고 계정 또는 조직 단위를 지정해야 할 수 있습니다.

리소스 공유에서 이 계정을 보안 주체로 지정하지 않음

리소스 공유를 생성한 AWS 계정에서 AWS RAM 콘솔을 통해 리소스 공유를 확인합니다. 리소스에 액세스할 수 없는 계정이 보안 주체로 등록되어 있는지 확인합니다. 등록되어 있지 않은 경우 공유를 업데이트하여 계정을 보안 주체로 추가합니다.

계정의 역할 또는 사용자에게는 필요한 최소 권한이 없음

계정 A의 리소스를 다른 계정 B와 공유할 때 계정 B의 역할과 사용자가 공유의 리소스에 대한 액세스 권한을 자동으로 얻지 못합니다. 계정 B의 관리자가 먼저 리소스에 액세스해야 하는 계정 B의 IAM 역할과 사용자에게 권한을 부여해야 합니다. 예를 들어, 다음 정책은 계정 A의 리소스에 대해 계정 B의 역할 및 사용자에게 읽기 전용 액세스 권한을 부여하는 방법을 보여줍니다. 이 정책은 Amazon 리소스 이름(ARN)으로 리소스를 지정합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:<Region-code>:<Account-A-ID>:<resource-id>"
        }
    ]
}
```

리소스가 현재 콘솔 설정과 다른 AWS 리전에 있음

AWS RAM은 리전 서비스입니다. 리소스는 특정 AWS 리전에 존재하므로, 리소스를 확인하려면 해당 리전의 리소스를 볼 수 있도록 AWS Management Console을 구성해야 합니다.

콘솔에서 현재 액세스 중인 AWS 리전은 콘솔의 오른쪽 상단 모서리에 표시됩니다. 변경하려면 현재 리전 이름을 선택하고 드롭다운 메뉴에서 리소스를 보려는 리전을 선택합니다.

오류: 한도 초과

시나리오

리소스를 공유하려고 할 때 "공유할 수 있는 리소스 수 한도에 도달함" 또는 "ResourceShareLimitExceededException"이라는 메시지가 표시됩니다.

원인

이러한 오류는 AWS RAM 서비스 또는 공유하려는 리소스를 생성한 AWS 서비스를 사용하여 공유할 수 있는 최대 리소스 수에 도달할 때 발생합니다. 이 할당량(이전에는 한도라고 함)은 공유 계정이나 리소스를 공유하고 있는 계정 모두에 영향을 미칠 수 있습니다.

솔루션

1. 할당량을 보려면 오류가 표시된 AWS 계정에서 도달한 할당량 유형에 따라 다음 페이지 중 하나로 이동합니다.
   - Service Quotas 콘솔의 AWS RAM 페이지
   - 할당량의 영향을 받는 리소스의 AWS 서비스 페이지
2. 아래로 스크롤하여 관련 할당량을 선택합니다.
3. 이 할당량을 사용할 수 있는 경우 할당량 증가 요청을 선택합니다.
4. 새 할당량 값을 입력한 다음 요청을 선택합니다.
5. 요청은 할당량 요청 기록 페이지에 표시되며, 여기서 요청이 완료될 때까지 요청 상태를 확인할 수 있습니다.

내 조직의 다른 계정이 초대를 받지 못함

시나리오

AWS Organizations에서 관리하는 동일한 조직의 다른 계정과 리소스를 공유하면 해당 계정이 초대를 받지 못합니다.

원인

이는 계정에 AWS 조직 내 공유가 활성화되어 있는 경우 예상되는 동작입니다.

이 옵션을 활성화하고 조직의 다른 계정과 공유하면 초대가 전송되지 않으므로 수락할 필요도 없습니다. 리소스 공유에서 보안 주체로 지정한 모든 조직 계정이 공유의 리소스에 즉시 액세스할 수 있습니다.

계정에서 AWS 조직 내 공유가 활성화되어 있지 않은 경우, 다른 계정과 공유할 때 동일한 AWS 조직에 있더라도 독립 계정으로 취급됩니다. 초대가 전송되고 이를 수락해야 사용자가 공유의 리소스에 액세스할 수 있습니다.

VPC 서브넷을 공유할 수 없음

시나리오

AWS RAM을 사용하여 VPC 서브넷을 다른 계정과 공유하려고 하면 공유 작업이 성공합니다. 그러나 소비 계정의 AWS RAM 콘솔에 해당 리소스가 `LIMIT EXCEEDED`로 표시됩니다.

원인

일부 개별 리소스 유형에는 AWS RAM에서 적용하는 제한과는 별도로 서비스별 제한이 있습니다. 이러한 제한 중 일부는 AWS RAM의 제한 중 하나에 도달하지 않았더라도 실질적으로 공유를 차단할 수 있습니다. 한도는 이러한 제한의 예입니다. Amazon Virtual Private Cloud(VPC)는 다른 개별 계정과 공유할 수 있는 서브넷 수를 제한합니다. 이미 최대 서브넷 수에 도달한 소비 계정과 서브넷을 공유하려고 하면 해당 소비 계정의 콘솔에 해당 리소스가 `LIMIT EXCEEDED`로 표시됩니다. 한도에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서에서 Amazon VPC 할당량 – VPC 공유를 참조하세요.

이 문제를 해결하려면 먼저 해당 계정과 지정된 리소스를 공유하고 있을 수 있는 다른 리소스 공유가 있는지 확인하고 더 이상 필요하지 않을 수 있는 공유를 제거하세요. 조정을 지원하는 한도에 대해 증가를 요청할 수도 있습니다. 한도 증가를 요청하려면 Service Quotas 콘솔을 사용합니다.

> **Note**
>
> AWS RAM은 증가 변경을 자동으로 감지하지 못합니다. RAM이 변경을 감지할 수 있도록 리소스 또는 보안 주체를 리소스 공유에 다시 연결해야 합니다.

AWS RAM의 서비스 할당량

AWS 계정에는 AWS Resource Access Manager(AWS RAM)와 관련하여 다음과 같은 제한이 있습니다. 사용자는 이러한 제한 중 일부를 늘리도록 요청할 수 있습니다. 제한 증가를 요청하려면 AWS Support에 문의하세요.

> **Note**
>
> 아래 할당량의 설명에는 다음 정의가 적용됩니다.
>
> - 리소스 - Amazon S3 버킷 또는 Amazon EC2 인스턴스 등 공유하려는 개별 AWS 서비스 생성 요소입니다. 리소스 공유에서 참조되는 각 리소스는 이 할당량에서 1개로 계산됩니다. 동일한 리소스를 세 개의 서로 다른 리소스 공유에서 공유하면 이 할당량에 대한 개수가 3개 증가합니다.
> - 리소스 공유 - 리소스를 공유하는 데 사용할 수 있는 AWS RAM 생성 컨테이너입니다. 각 리소스 공유는 포함된 리소스 수와 상관없이 할당량에서 1개로 계산됩니다.
> - 공유 보안 주체 - 리소스 공유와 연결된 식별자로, AWS Identity and Access Management(IAM) 역할 또는 사용자, AWS 계정 식별자, 조직 단위 또는 전체 조직일 수 있습니다. 리소스 공유에서 참조하는 각 공유 보안 주체는 할당량 사용량에 하나씩 추가됩니다. ID를 참조하여 전체 조직과 공유하는 경우 이 할당량에서 1개로 계산됩니다.
> - 고객 관리형 권한 - 최소 권한 액세스를 사용하여 특정 사용 사례를 해결하기 위해 사용자가 생성하는 관리 권한으로, 공유 리소스의 사용 방식을 관리합니다.

리소스	기본 한도
AWS 리전당 최대 리소스 공유 수	25,000
리소스 공유당 최대 리소스 연결 수	5,000
리소스 공유당 최대 보안 주체 연결 수	5,000
최대 고객 관리형 권한 수	1,500
리소스 유형당 최대 고객 관리형 권한 수	10
고객 관리형 권한당 최대 버전 수	5

리소스	기본 한도
AWS 리전의 모든 리소스 공유에 대한 최대 리소스 연결 수 **Note** 리소스 공유에 포함된 각 리소스는 이 한도에 따라 계산됩니다. 하나의 리소스가 10개의 서로 다른 리소스 공유에 포함되어 있는 경우 한도에서 10개로 계산됩니다.	25,000
AWS 리전의 모든 리소스 공유에 대한 최대 보안 주체 연결 수 **Note** 리소스 공유에 포함된 각 보안 주체는 이 한도에 따라 계산됩니다. 하나의 보안 주체가 10개의 서로 다른 리소스 공유에 포함되어 있는 경우 한도에서 10개로 계산됩니다.	25,000
공유 계정당 보류 중인 초대의 최대 개수 • 이 할당량은 동일한 AWS Organizations에 속하지 않은 계정과 공유하는 전송 계정에만 적용됩니다. • 수신 계정이 보유할 수 있는 보류 중인 초대 개수를 제한하는 할당량은 없습니다. • 동일한 AWS Organizations에 속해 있는 계정 간에 공유하고 AWS Organizations 내 리소스 공유를 활성화한 경우에는 초대가 사용되지 않습니다.	250

AWS RAM와 AWS SDK 사용

다양한 프로그래밍 언어에 대해 AWS 소프트웨어 개발 키트(SDK)를 사용할 수 있습니다. 각 SDK는 개발자가 선호하는 언어로 애플리케이션을 구축하는 데 도움이 되는 API, 코드 예제 및 설명서를 제공합니다.

SDK 설명서	코드 예제
AWS SDK for C++	AWS SDK for C++ 코드 예제
AWS SDK for Go	AWS SDK for Go 코드 예제
AWS SDK for Java	AWS SDK for Java 코드 예제
AWS SDK for JavaScript	AWS SDK for JavaScript 코드 예제
AWS SDK for .NET	AWS SDK for .NET 코드 예제
AWS SDK for PHP	AWS SDK for PHP 코드 예제
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 코드 예제
AWS SDK for Ruby	AWS SDK for Ruby 코드 예제

가용성 예

필요한 항목을 찾을 수 없습니까? 피드백 링크를 사용하여 코드 예제를 요청하세요.

AWS RAM 사용 설명서의 문서 기록

다음 표에는 설명서에 추가된 중요한 내용이 설명되어 있습니다. AWS Resource Access Manager 사용자로부터 받은 의견을 수렴하기 위해 설명서가 업데이트됩니다.

이러한 업데이트에 대한 알림을 받으려면 AWS RAM RSS 피드를 구독할 수 있습니다.

변경 사항	설명	날짜
공유에 대한 지원이 추가되었습니다. Amazon Route 53 ResolverProfiles	이제 를 AWS RAM 사용하여 조직 AWS 계정 내 다른 Amazon Route 53 Resolver Profiles 사람과 공유할 수 있습니다.	2024년 4월 22일
AWS Systems Manager 파라미터 스토어 리소스 공유를 위한 지원이 추가되었습니다.	이제 조직 전체 AWS 계정 또는 조직 내에서 고급 파라미터를 안전하고 효율적으로 공유할 수 있습니다.	2024년 2월 21일
Amazon FSx for OpenZFS 스냅샷 공유에 대한 지원이 추가되었습니다.	이제 OpenZFS용 Amazon FSX 스냅샷을 조직 내 다른 사람과 공유할 수 있습니다. AWS 계정	2023년 12월 19일
리소스 공유를 위한 지원이 추가되었습니다. Amazon Simple Storage Service	이제 Amazon Simple Storage Service Access Grants 인스턴스를 다른 사람 AWS 계정 또는 조직과 공유할 수 AWS RAM있습니다.	2023년 11월 27일
AWS 리소스 탐색기 뷰 공유에 대한 지원이 추가되었습니다.	이제 조직 AWS 계정 내 다른 사람과 AWS 리소스 탐색기 뷰를 공유할 수 있습니다.	2023년 11월 14일
Amazon Route 53 Application Recovery Controller 리소스를	이제 Amazon Route 53 애플리케이션 복구 컨트롤러 클러스터를 다른 사람 AWS 계정 또는	2023년 10월 18일

공유하기 위한 지원이 추가되었습니다.	조직과 공유할 수 AWS RAM있습니다.	
Amazon DataZone 리소스 공유를 위한 지원이 추가되었습니다.	이제 Amazon DataZone 리소스를 다른 사람 AWS 계정 또는 조직과 공유할 수 있습니다.	2023년 10월 4일
서비스 보안 주체 공유에 대한 지원이 추가되었습니다.	이제 서비스 보안 주체를 리소스 공유에 연결할 수 있습니다. 이를 통해 지정된 서비스가 사용자를 대신해 고객 리소스에 필요한 작업을 관리할 수 있습니다.	2023년 8월 29일
SageMaker Model Card 리소스 공유를 위한 지원이 추가되었습니다.	이제 SageMaker 모델 카드 리소스를 다른 사람 AWS 계정 또는 조직과 공유할 수 있습니다.	2023년 8월 18일
Amazon SageMaker Feature Store 기능 그룹 및 SageMaker 카탈로그에 대한 지원을 공유 가능한 리소스로 추가했습니다.	이제 Amazon SageMaker Feature Store 기능 그룹 및 SageMaker 카탈로그 리소스를 다른 사람 AWS 계정 또는 조직과 공유할 수 있습니다.	2023년 7월 20일
보류 중인 초대에 대한 서비스 할당량 한도 증가	공유 계정당 보류 중인 초대의 최대 개수가 20개에서 250개로 늘어났습니다.	2023년 6월 8일
AWS AppSync GraphQL API에 대한 지원을 공유 가능한 리소스로 추가했습니다.	이제 AWS AppSync GraphQL API를 다른 사용자와 공유할 수 있습니다. AWS 계정 AWS RAM	2023년 5월 24일
AWS Verified Access 그룹에 대한 지원을 공유 가능한 리소스로 추가했습니다.	이제 중앙에서 AWS Verified Access 그룹을 만들고 관리한 다음 다른 사람 AWS 계정 또는 조직과 공유할 수 있습니다.	2023년 4월 27일

AWS RAM 콘솔에 고객 관리 권한에 대한 지원이 추가되었습니다.	이제 지원되는 리소스 유형에 대해 세분화된 리소스 액세스 제어를 안전하게 작성하고 유지 관리할 수 있습니다.	2023년 4월 19일
Amazon VPC Lattice 서비스 및 서비스 네트워크 공유 가능 리소스에 대한 지원이 추가되었습니다.	이제 Amazon VPC Lattice 서비스 및 서비스 네트워크 리소스를 다른 사람과 공유할 수 있습니다. AWS 계정	2023년 3월 31일
AWS Marketplace 카탈로그 엔티티를 공유 가능한 리소스로 지원하는 기능이 추가되었습니다.	이제 AWS 계정 Marketplace에서 다른 사람과 엔티티를 공유할 수 있습니다.	2023년 3월 27일
AWS RAM 콘솔에서 권한 버전을 관리하기 위한 지원이 추가되었습니다.	이제 AWS RAM 콘솔을 사용하여 버전 세부 정보를 보고 권한을 기본값으로 지정된 버전으로 업데이트할 수 있습니다.	2023년 1월 16일
IAM 모범 사례 업데이트	IAM 모범 사례에 따라 가이드가 업데이트되었습니다. 자세한 내용은 IAM의 보안 모범 사례 섹션을 참조하세요.	2023년 1월 3일
Amazon EC2 배치 그룹이 공유 가능한 리소스로 추가되었습니다.	이제 Amazon EC2 배치 그룹을 다른 사람과 AWS 계정 공유하여 해당 인스턴스를 시작할 수 있습니다.	2022년 11월 8일
에 대한 소개 동영상 두 개에 대한 링크를 추가했습니다. AWS RAM	다른 사람과 리소스를 공유하는 방법을 AWS RAM 설명하고 안내하는 개요 비디오가 추가되었습니다. AWS 계정	2022년 8월 29일
Amazon SageMaker 파이프라인에 대한 지원이 추가되었습니다.	이제 SageMaker 파이프라인을 다른 사람과 공유할 수 있습니다. AWS 계정	2022년 8월 2일

AWS Service Catalog AppRegistry 애플리케이션 및 속성 그룹을 공유 가능한 리소스 유형으로 지원하는 기능이 추가되었습니다.	이제 AppRegistry 응용 프로그램 및 속성 그룹을 다른 AWS 계정사람과 공유할 수 있습니다.	2022년 6월 17일
AWS Resource Access Manager SOC 및 ISO 인증을 받았습니다.	AWS RAM 서비스 조직 통제 (SOC) 및 국제 표준화 기구 (ISO) ISO 9001, ISO 27001, ISO 27017, ISO 27018 및 ISO 27701 표준을 준수하는 것으로 검증되었습니다.	2022년 5월 31일
AWS Resource Access Manager FedRAMP 인증을 받았습니다.	AWS RAM 연방 위험 및 권한 관리 프로그램 (FedRAMP) 을 준수하는 것으로 검증되었습니다.	2022년 4월 8일
AWS Resource Access Manager PCI DSS 인증을 받았습니다.	AWS RAM 결제 카드 산업 (PCI) 데이터 보안 표준 (DSS) 을 준수하는 것으로 검증되었습니다.	2022년 2월 27일
Amazon VPC IPAM 리소스 검색이 공유 가능한 리소스로 추가되었습니다. 또한 이제 IPAM 풀을 조직 외부의 계정과 공유할 수 있습니다.	이제 IPAM 리소스 검색을 다른 AWS 계정과 공유할 수 있습니다.	2022년 1월 25일
글로벌 리소스 공유에 대한 지원이 추가되었습니다.	이제 글로벌 리소스를 다른 사람과 공유할 수 있습니다. AWS 계정	2021년 12월 2일
공유 가능한 글로벌 리소스로서 AWS 클라우드 WAN 코어 네트워크에 대한 지원이 추가되었습니다.	이제 클라우드 WAN 코어 네트워크를 다른 AWS 계정사람과 공유할 수 있습니다.	2021년 12월 2일

Amazon VPC IP 주소 관리자 (IPAM) 풀 공유에 대한 지원	를 AWS RAM 사용하여 Amazon VPC IPAM 풀을 공유할 수 있습니다. 자세한 내용은 사용 설명서의 공유 가능한 AWS 리소스를 참조하십시오.AWS RAM	2021년 12월 1일
Amazon SageMaker 리소스 공유 지원	SageMaker 계보 그룹을 공유하는 AWS RAM 데 사용할 수 있습니다. 자세한 내용은AWS RAM 사용 설명서에서 공유 가능한 AWS 리소스를 참조하세요.	2021년 11월 30일
AWS Migration Hub 리팩터링 스페이스 리소스 공유 지원	Migration Hub 환경을 공유하는 AWS RAM 데 사용할 수 있습니다. 자세한 내용은AWS RAM 사용 설명서에서 공유 가능한 AWS 리소스를 참조하세요.	2021년 11월 29일
AWS RAMAWS-managed IAM 권한 정책에 대한 정보가 추가되었습니다.	사용 가능한 AWS관리 권한 정책에 대한 세부 정보가 게시되었으며, IAM 콘솔에서 액세스하여 IAM 보안 주체에 연결할 수 있습니다. AWS 계정	2021년 9월 16일
S3 on Outposts 리소스 공유에 대한 지원이 추가되었습니다.	이제 Outposts의 S3를 다른 사람과 공유하는 AWS RAM 데 사용할 수 있습니다. AWS 계정	2021년 8월 5일
추가 관리형 권한 및 IAM 보안 주체와 리소스 공유에 대한 지원이 추가되었습니다.	지원되는 리소스 유형의 경우 추가 AWS RAM 관리 권한 중에서 선택하여 개별 IAM 역할 및 사용자와 리소스를 공유할 수 있습니다.	2021년 6월 10일

AWS Systems Manager 인시던트 관리자 리소스 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 AWS Systems Manager 인시던트 관리자 연락처 및 대응 계획을 다른 사람과 공유할 수 AWS 계정있습니다.	2021년 5월 10일
Amazon Route 53 리소스 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 Amazon Route 53 리졸버 DNS 방화벽 규칙 그룹을 다른 사람과 공유할 수 있습니다. AWS 계정	2021년 3월 31일
리소스 공유에 대한 지원이 추가되었습니다. AWS Transit Gateway	이제 를 AWS RAM 사용하여 트랜짓 게이트웨이 멀티캐스트 도메인을 다른 AWS 계정도메인과 공유할 수 있습니다.	2020년 12월 10일
리소스 AWS Network Firewall 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 AWS Network Firewall 방화벽 정책 및 규칙 그룹을 다른 사람과 공유할 수 AWS 계정있습니다.	2020년 11월 17일
Outposts 및 로컬 게이트웨이 라우팅 테이블 공유에 대한 지원이 추가되었습니다.	이제 Outposts 및 로컬 게이트웨이 라우팅 테이블을 다른 사람과 공유하는 AWS RAM 데 사용할 수 있습니다. AWS 계정	2020년 10월 15일
Route 53 쿼리 로그 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 Route 53 쿼리 로그를 다른 AWS 계정사람과 공유할 수 있습니다.	2020년 9월 7일
AWS Private Certificate Authority 리소스 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 AWS Private CA 사설 인증 기관 (CA) 을 다른 사람과 공유할 수 AWS 계정있습니다.	2020년 8월 17일

AWS Glue 데이터 카탈로그, 데이터베이스, 테이블 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 AWS Glue 데이터 카탈로그, 데이터베이스 및 테이블을 다른 사람과 공유할 수 있습니다. AWS 계정	2020년 7월 7일
Amazon VPC 접두사 목록 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 접두사 목록을 공유할 수 있습니다.	2020년 6월 29일
AWS Outposts 고객 소유 IPv4 주소 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 AWS Outposts 고객 소유 IPv4 주소를 다른 사람과 공유할 수 있습니다. AWS 계정	2020년 4월 22일
메시 공유에 대한 지원이 추가되었습니다. AWS App Mesh	이제 를 사용하여 다른 사람과 AWS RAM 메시를 공유할 수 있습니다. AWS 계정	2020년 1월 17일
AWS CodeBuild 프로젝트 및 보고서 그룹 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 AWS CodeBuild 프로젝트 및 보고서 그룹을 다른 사람과 공유할 수 AWS 계정있습니다.	2019년 12월 13일
추가 리소스 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 Amazon EC2 전용 호스트, AWS Resource Groups 리소스 그룹, Amazon EC2 Image Builder 구성 요소, 이미지, 이미지 레시피를 다른 사람과 공유할 수 있습니다. AWS 계정	2019년 12월 2일
온디맨드 용량 예약 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 온디맨드 용량 예약을 다른 사람과 공유할 수 있습니다. AWS 계정	2019년 7월 29일

Aurora DB 클러스터 공유에 대한 지원이 추가되었습니다	이제 를 AWS RAM 사용하여 Aurora DB 클러스터를 다른 사람과 공유할 수 있습니다. AWS 계정	2019년 7월 2일
트래픽 미러링 대상 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 트래픽 미러링 대상을 다른 사람과 공유할 수 있습니다. AWS 계정	2019년 6월 25일
라이선스 구성 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 AWS License Manager 라이선스 구성을 다른 사람과 공유할 수 AWS 계정있습니다.	2018년 12월 5일
서브넷 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 Amazon VPC 서브넷을 다른 사람과 공유할 수 있습니다. AWS 계정	2018년 11월 27일
전송 게이트웨이 공유에 대한 지원이 추가되었습니다.	이제 를 AWS RAM 사용하여 Amazon VPC 전송 게이트웨이를 다른 사람과 공유할 수 있습니다. AWS 계정	2018년 11월 26일
Resolver 규칙 공유에 대한 지원이 추가되었습니다.	이제 Route 53 리졸버 규칙을 AWS RAM 사용하여 다른 사람과 공유할 수 있습니다. AWS 계정	2018년 11월 20일

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