사용자 가이드

AWS 리소스 탐색기

AWS 리소스 탐색기: 사용자 가이드

Table of Contents

AWS 리소스 탐색기란 무엇인가요?

AWS 리소스 탐색기 는 리소스 검색 및 검색 서비스입니다. Resource Explorer를 사용하면 인터넷 검색 엔진과 유사한 환경을 사용하여 Amazon Elastic Compute Cloud 인스턴스, Amazon Kinesis 스트림 또는 Amazon DynamoDB 테이블과 같은 리소스를 탐색할 수 있습니다. 이름, 태그 및 와 같은 리소스 메타데이터를 사용하여 리소스를 검색할 수 있습니다IDs. Resource Explorer는 계정 AWS 리전 에서 작동하여 리전 간 워크로드를 단순화합니다.

Resource Explorer는 AWS 리소스 탐색기 서비스에서 생성 및 유지 관리하는 인덱스를 사용하여 검색 쿼리에 대한 빠른 응답을 제공합니다. Resource Explorer는 다양한 데이터 소스를 사용하여 사용자의 AWS 계정리소스에 대한 정보를 수집합니다. Resource Explorer는 해당 정보를 Resource Explorer가 검색할 인덱스에 저장합니다.

> 이 설명서에 대한 여러분의 의견을 기다립니다
>
> 우리의 목표는 사용자가 Resource Explorer에서 가능한 모든 것을 얻을 수 있도록 돕는 것입니다. 이 안내서가 도움이 된다면 알려주세요. 안내서가 도움이 되지 않는 경우 문제를 해결할 수 있도록 여러분의 의견을 듣고 싶습니다. 모든 페이지의 오른쪽 상단에 있는 Feedback 링크를 사용하세요. 그러면 여러분의 의견이 이 안내서의 작성자에게 직접 전달됩니다. 우리는 모든 제출물을 검토하며 설명서를 개선할 기회를 찾고 있습니다. 도움을 주셔서 미리 감사드립니다!

주제

Resource Explorer를 처음 사용하시나요?

Resource Explorer를 처음 사용하는 경우 먼저 시작하기 섹션에서 다음 주제를 읽어보는 것이 좋습니다.

- Resource Explorer 용어 및 개념
- 빠른 설정을 사용하여 Resource Explorer 설정

Resource Explorer 기능

Resource Explorer는 다음의 기능을 제공합니다.

- 사용자는 에서 AWS 리전 또는 리전 간에 리소스를 검색할 수 있습니다 AWS 계정.
- 사용자는 키워드, 검색 연산자, 태그와 같은 속성을 사용하여 일치하는 리소스로만 검색하도록 검색 결과를 필터링할 수 있습니다.
- 사용자는 검색 결과에서 리소스를 찾으면 즉시 리소스의 기본 콘솔로 이동하여 해당 리소스로 작업할 수 있습니다.
- 관리자는 검색 결과에서 사용할 수 있는 리소스를 정의하는 뷰를 생성할 수 있습니다. 관리자는 작업에 따라 사용자 그룹별로 다른 뷰를 생성하고 필요한 사용자에게만 뷰에 대한 권한을 부여할 수 있습니다.
- Resource Explorer AWS 서비스는 다른 여러 와 마찬가지로 가 획기적으로 일관됩니다. Resource Explorer는 전 세계 Amazon 데이터 센터 내의 여러 서버에 걸쳐 데이터를 복제함으로써 고가용성을 구현합니다. 일부 데이터를 변경하겠다는 요청이 성공하면 변경이 실행되고 그 결과는 안전하게 저장됩니다. 그러나 변경 사항은 Resource Explorer에 두루 복제되어야 하며, 이 작업에는 일정한 시간이 걸립니다. 예를 들어, Resource Explorer가 한 리전의 리소스를 찾아 계정의 애그리게이터 인덱스가 포함된 리전으로 복제하는 작업이 여기에 포함됩니다.

Resource Explorer 지원 리전

리전 이름	지역	엔드포인트	프로토콜	
미국 동부(오하이오)	us-east-2	resource-explorer-2.us-east-2.amazonaws.com resource-explorer-2-fips.us-east-2.amazonaws.com resource-explorer-2-fips.us-east-2.api.aws	HTTPS HTTPS HTTPS	
미국 동부(버지니아 북부)	us-east-1	resource-explorer-2.us-east-1.amazonaws.com resource-explorer-2-fips.us-east-1.amazonaws.com resource-explorer-2-fips.us-east-1.api.aws	HTTPS HTTPS HTTPS	

리전 이름	지역	엔드포인트	프로토콜
미국 서부(캘리포니아 북부)	us-west-1	resource-explorer-2.us-west-1.amazonaws.com resource-explorer-2-fips.us-west-1.amazonaws.com resource-explorer-2-fips.us-west-1.api.aws	HTTPS HTTPS HTTPS
미국 서부(오레곤)	us-west-2	resource-explorer-2.us-west-2.amazonaws.com resource-explorer-2-fips.us-west-2.amazonaws.com resource-explorer-2-fips.us-west-2.api.aws	HTTPS HTTPS HTTPS
아프리카(케이프타운)	af-south-1	resource-explorer-2.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	resource-explorer-2.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	resource-explorer-2.ap-south-2.amazonaws.com	HTTPS
아시아 태평양(자카르타)	ap-southeast-3	resource-explorer-2.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	resource-explorer-2.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	resource-explorer-2.ap-south-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(오사카)	ap-northeast-3	resource-explorer-2.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	resource-explorer-2.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	resource-explorer-2.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	resource-explorer-2.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	resource-explorer-2.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	resource-explorer-2.ca-central-1.amazonaws.com resource-explorer-2-fips.ca-central-1.amazonaws.com resource-explorer-2-fips.ca-central-1.api.aws	HTTPS HTTPS HTTPS
캐나다 서부(캘거리)	ca-west-1	resource-explorer-2.ca-west-1.amazonaws.com resource-explorer-2-fips.ca-west-1.amazonaws.com resource-explorer-2-fips.ca-west-1.api.aws	HTTPS HTTPS HTTPS
유럽(프랑크푸르트)	eu-central-1	resource-explorer-2.eu-central-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜	
유럽(아일랜드)	eu-west-1	resource-explorer-2.eu-west-1.amazonaws.com	HTTPS	
유럽(런던)	eu-west-2	resource-explorer-2.eu-west-2.amazonaws.com	HTTPS	
유럽(밀라노)	eu-south-1	resource-explorer-2.eu-south-1.amazonaws.com	HTTPS	
유럽(파리)	eu-west-3	resource-explorer-2.eu-west-3.amazonaws.com	HTTPS	
유럽(스페인)	eu-south-2	resource-explorer-2.eu-south-2.amazonaws.com	HTTPS	
유럽(스톡홀름)	eu-north-1	resource-explorer-2.eu-north-1.amazonaws.com	HTTPS	
유럽(취리히)	eu-central-2	resource-explorer-2.eu-central-2.amazonaws.com	HTTPS	
이스라엘(텔아비브)	il-central-1	resource-explorer-2.il-central-1.amazonaws.com	HTTPS	
중동(바레인)	me-south-1	resource-explorer-2.me-south-1.amazonaws.com	HTTPS	
중동(UAE)	me-central-1	resource-explorer-2.me-central-1.amazonaws.com	HTTPS	
남아메리카(상파울루)	sa-east-1	resource-explorer-2.sa-east-1.amazonaws.com	HTTPS	

관련 AWS 서비스

다음은 AWS 리소스를 관리하는 데 도움이 되는 다른 AWS 서비스 주요 목적입니다.

AWS Resource Access Manager (AWS RAM)

하나의 리소스를 다른 AWS 계정 와 공유합니다 AWS 계정. 계정이 에서 관리되는 경우 AWS Organizations AWS RAM 를 사용하여 조직 단위의 계정 또는 조직의 모든 계정과 리소스를 공유할 수 있습니다. 공유 리소스는 로컬 계정에서 생성된 경우와 마찬가지로 해당 계정의 사용자에게 작동합니다.

AWS Resource Groups

AWS 리소스에 대한 그룹을 생성합니다. 그러면 모든 리소스를 개별적으로 참조할 필요 없이 각 그룹을 하나의 단위로 사용하고 관리할 수 있습니다. 그룹은 동일한 AWS CloudFormation 스택에 속하거나 동일한 태그로 태그가 지정된 리소스로 구성될 수 있습니다. 일부 리소스 유형은 리소스 그룹에 구성을 적용하여 해당 그룹의 모든 관련 리소스에 영향을 주는 기능도 지원합니다.

태그 편집기 및 AWS Resource Groups Tagging API

태그는 리소스에 연결할 수 있는 고객 정의 메타데이터입니다. 비용 할당 및 속성 기반 액세스 제어와 같은 목적으로 리소스를 분류할 수 있습니다.

요금

뷰 생성 AWS 리소스 탐색기, 리전 켜기 또는 리소스 검색을 포함하여 를 사용하여 리소스를 검색하는 데 드는 비용은 없습니다. 리소스 인벤토리를 구축하는 과정에서 Resource Explorer는 APIs 사용자를 대신하여 를 호출하여 요금이 부과될 수 있습니다. 검색 결과에서 찾은 리소스와 상호 작용하면 리소스 유형 및 에 따라 사용 요금이 달라질 수 있습니다 AWS 서비스. 가 특정 리소스 유형의 일반적인 사용에 대해 AWS 청구하는 방법에 대한 자세한 내용은 해당 리소스 유형의 소유 서비스에 대한 설명서를 참조하세요.

Resource Explorer 시작하기

이 섹션의 항목을 통해 에서 사용되는 개념과 용어에 대한 기본적인 이해를 얻으십시오 AWS 리소스 탐색기. Resource Explorer를 성공적으로 사용하기 위해 충족해야 하는 사전 조건과 AWS 계정에서 Resource Explorer를 활성화하는 방법에 대해 알아봅니다.

Resource Explorer에 액세스

다음과 같은 방식으로 Resource Explorer와 상호 작용할 수 있습니다.

Resource Explorer 콘솔

Resource Explorer는 웹 기반 사용자 인터페이스인 Resource Explorer 콘솔을 제공합니다. 에 가입한 AWS 계정경우 에 AWS Management Console로그인하고 콘솔 홈 페이지에서 리소스 탐색기를 선택하여 리소스 탐색기 콘솔에 액세스할 수 있습니다.

브라우저에서 Resource Explorer 대시보드 페이지 또는 리소스 검색 페이지로 직접 이동할 수도 있습니다. 아직 로그인하지 않은 경우 콘솔이 표시되기 전에 로그인하라는 메시지가 표시됩니다.

> **Note**
>
> 리소스 탐색기 콘솔은 글로벌 콘솔이므로 작업할 콘솔을 선택할 필요가 없습니다. AWS 리전 하지만 Resource Explorer를 사용하여 인덱스나 뷰를 생성할 때는 인덱스나 뷰가 저장되는 리전을 지정해야 합니다. Resource Explorer를 사용하여 검색할 때는 액세스할 수 있는 모든 뷰를 선택할 수 있습니다. 결과는 선택한 뷰와 연결된 리전에서 자동으로 제공됩니다. 애그리게이터 인덱스가 포함된 리전의 뷰인 경우 결과에는 Resource Explorer 인덱스를 생성한 모든 리전의 리소스가 포함됩니다.

AWS Management Console 통합 검색

의 모든 페이지 AWS Management Console상단에는 검색 창이 있습니다. Resource Explorer가 통합 검색에 참여하도록 구성할 수 있습니다. 그러면 사용자는 통합 검색 텍스트 상자에서 Resource Explorer 검색 쿼리 구문을 사용하여 해당 검색 결과에서 일치하는 리소스를 볼 수 있습니다. 이 기능을 켜면 사용자는 먼저 리소스 탐색기 콘솔로 AWS 서비스 전환하지 않고도 모든 콘솔에서 리소스를 검색할 수 있습니다.

> **Important**
>
> 통합 검색은 항상 애그리게이터 AWS 리전 색인이 포함된 의 기본 보기를 사용하여 검색합니다.

Windows용 AWS CLI 및 도구의 리소스 탐색기 명령 PowerShell

AWS CLI 및 도구는 리소스 탐색기 공개 API 작업에 직접 액세스할 수 있도록 합니다. PowerShell 이 도구들은 Windows, macOS, Linux에서 작동합니다. 시작하기에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서 또는 AWS Tools for Windows PowerShell 사용 설명서를 참조하세요. Resource Explorer의 명령에 대한 자세한 내용은 AWS CLI 명령 참조 또는 AWS Tools for Windows PowerShell Cmdlet 참조를 참조하세요.

리소스 탐색기 작업은 AWS SDKs

AWS 광범위한 프로그래밍 언어 세트에 대한 API 명령을 제공합니다. 시작하기에 대한 자세한 내용은 와 AWS 리소스 탐색기 함께 사용 AWS SDK섹션을 참조하세요.

쿼리 API

지원되는 프로그래밍 언어 중 하나를 사용하지 않는 경우 리소스 탐색기 HTTPS 쿼리를 API 사용하면 리소스 탐색기에 프로그래밍 방식으로 액세스할 수 있습니다. 리소스 탐색기를 API 사용하면 서비스에 직접 HTTPS 요청을 보낼 수 있습니다. 리소스 탐색기를 사용할 때는 자격 API 증명을 사용하여 요청에 디지털 서명할 수 있는 코드를 포함해야 합니다. AWS 자세한 내용은 참조를 참조하십시오.AWS 리소스 탐색기 API

Resource Explorer 용어 및 개념

AWS 리소스 탐색기은 리소스 검색 및 발견 서비스입니다. Resource Explorer를 사용하면 인터넷 검색 엔진과 유사한 환경을 사용하여 리소스를 탐색할 수 있습니다. 이름, 태그, ID와 같은 메타데이터를 사용하여 Amazon Elastic Compute Cloud 인스턴스, Amazon Kinesis 스트림 또는 Amazon DynamoDB 테이블과 같은 리소스를 검색할 수 있습니다. Resource Explorer는 계정의 AWS 리전 전반에 걸쳐 작동하여 리전 간 워크로드를 단순화합니다.

Resource Explorer는 AWS 리소스 탐색기 서비스에서 생성 및 유지 관리되는 인덱스를 사용하여 검색 쿼리에 빠르게 응답합니다. Resource Explorer는 다양한 데이터 소스를 사용하여 사용자의 AWS 계정 리소스에 대한 정보를 수집합니다. Resource Explorer는 해당 정보를 Resource Explorer가 검색할 인덱스에 저장합니다.

사용자를 위해 AWS 리소스 탐색기을 성공적으로 관리하고 구성하려면 다음 개념을 이해해야 합니다.

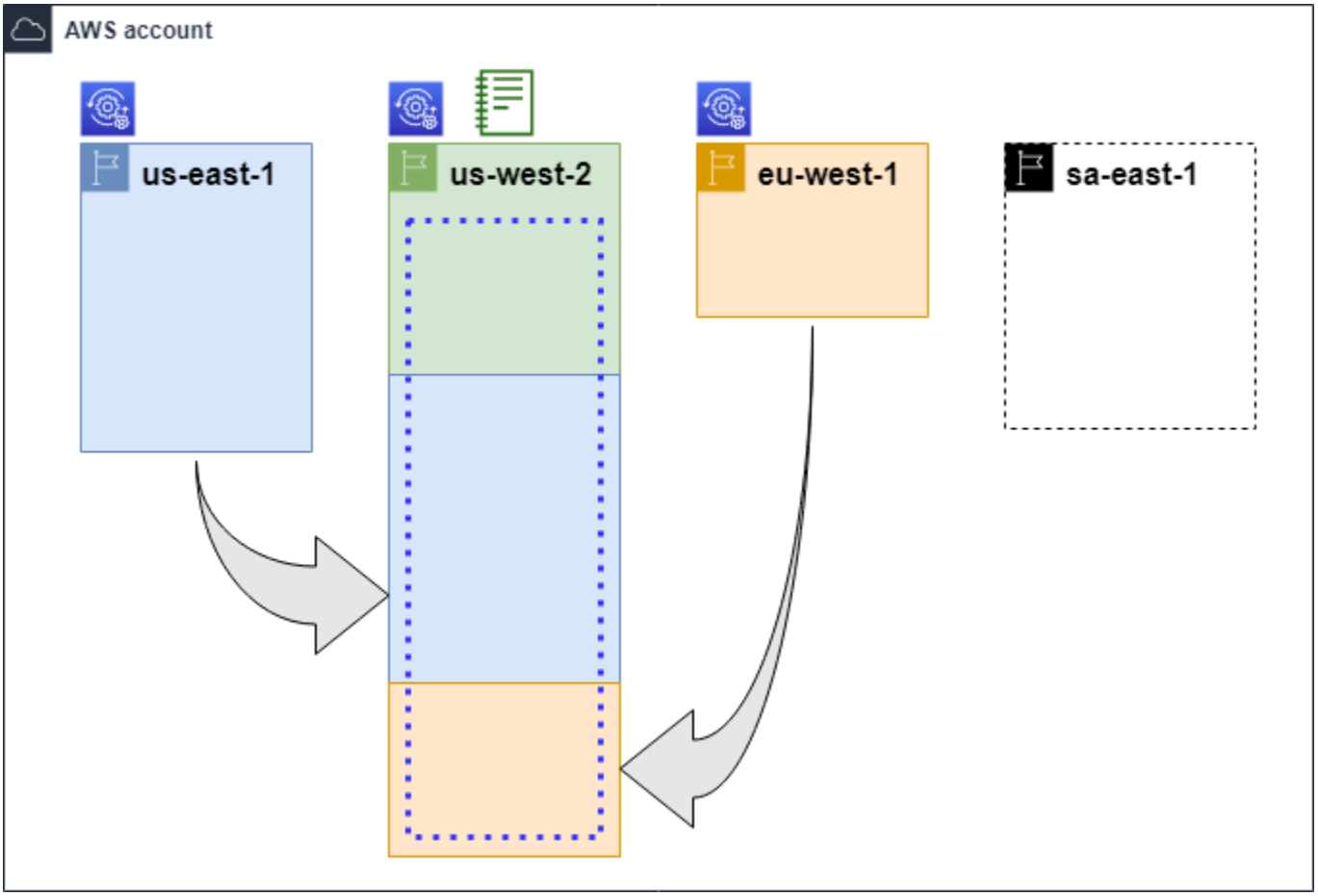
개념

- Resource Explorer 관리자
- Resource Explorer 사용자
- 인덱스
- 뷰
- Resource
- AWS Management Console에서 통합 검색
- 다중 계정 검색

다음 다이어그램은 관리자가 Resource Explorer를 활성화한 세 개의 AWS 리전과 관리자가 활성화하지 않기로 선택한 하나의 리전을 보여줍니다. Resource Explorer가 활성화되어 있지 않은 리전에는 인덱스가 없습니다. 따라서 Resource Explorer 쿼리로 해당 리소스를 검색할 수 없습니다.

이 예제 시나리오에서 관리자는 미국 서부(오레곤) 리전(`us-west-2`)을 계정의 애그리게이터 인덱스를 포함하도록 선택했습니다. 활성화한 모든 리전은 해당 리전의 로컬 인덱스를 애그리게이터 인덱스가 있는 리전에 복제합니다.

Resource Explorer에서 생성된 기본 뷰에는 필터가 없습니다. 따라서 이 뷰로 검색한 결과에는 Resource Explorer가 활성화되어 있는 계정의 모든 리전에 있는 모든 유형의 리소스가 포함될 수 있습니다.



범례	
	이 AWS 리전에서는 Resource Explorer가 활성화되어 있으며 리전의 리소스에 대한 정보가 해당 리전에 있는 로컬 인덱스에 저장됩니다. 모든 리전의 로컬 인덱스는 애그리게이터 인덱스가 포함된 리전에도 복제됩니다(화살표로 표시됨).
	이 AWS 리전에 있는 인덱스는 계정의 애그리게이터 인덱스가 되도록 구성되어 있습니다. Resource Explorer는 Resource Explorer가 활성화된 다른 모든 리전의 로컬 인덱스에서 수집된 리소스 정보를 이 리전에 있는 애그리게이터 인덱스로 복제합니다. 이 리전에서 수행한 검색에는 계정에 있는 모든 리전의 결과가 포함될 수 있습니다.
	빠른 설정에서 생성한 기본 뷰에는 모든 AWS 리전의 모든 리소스가 포함됩니다.

Resource Explorer 관리자

Resource Explorer 관리자는 AWS 계정. Resource Explorer 관리자는 다음 기능을 구성할 수 있습니다.

- 해당 리전에 인덱스를 생성하여 AWS 계정의 개별 AWS 리전에 대한 Resource Explorer를 활성화합니다. 이렇게 하면 Resource Explorer에서 리소스를 검색하고 해당 리소스에 대한 정보로 인덱스를 채워 사용자가 해당 리전의 리소스를 검색할 수 있습니다.
- 한 AWS 리전의 인덱스 유형을 업데이트하여 해당 AWS 계정의 애그리게이터 인덱스로 만듭니다. 이 리전에 있는 애그리게이터 인덱스는 Resource Explorer가 활성화되어 있는 계정의 다른 모든 리전으로부터 리소스 정보의 복제본을 받습니다.
- 사용자가 Resource Explorer에서 검색하고 발견할 수 있는 인덱싱된 정보의 하위 집합을 정의하는 뷰를 생성합니다.
- Resource Explorer 작업에는 포함되지 않지만 Resource Explorer 관리자는 계정의 보안 주체에게 검색 권한을 부여할 수도 있어야 합니다. 관리자는 기존 IAM 권한 정책에 관련 권한을 추가하거나 Resource Explorer 읽기 전용 AWS 관리형 정책을 사용하여 보안 주체에게 이러한 권한을 부여할 수 있습니다.

  액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하십시오:

  - AWS IAM Identity Center의 사용자 및 그룹:

    권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따르세요.

  - ID 공급자를 통해 IAM에서 관리되는 사용자:

    ID 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 사용자(콘솔)에 권한 추가의 지침을 따르세요.

관리자는 일반적으로 인덱스와 뷰를 포함하여 모든 Resource Explorer 리소스에 대한 모든 Resource Explorer 권한(`resource-explorer-2:*`)을 갖습니다. 이러한 권한은 Resource Explorer 전체 액세스 AWS 관리형 정책을 사용하여 부여할 수 있습니다.

Resource Explorer 사용자

Resource Explorer 사용자는 다음 작업 중 하나 이상을 수행할 권한이 있는 IAM 보안 주체입니다.

- 뷰를 사용하여 Resource Explorer를 쿼리하여 리소스 검색을 수행합니다. Resource Explorer 사용자는 AWS 리소스를 검색하고 찾고자 하며, 일반적으로 Resource Explorer 콘솔이나 AWS SDK 또는 AWS CLI에서 제공하는 Resource Explorer `Search` 작업을 사용합니다.

  역할 또는 사용자는 IAM 획득 권한을 사용하여 다음 두 가지 방법 중 하나로 검색할 수 있습니다.

  - IAM 역할, 그룹 또는 사용자에 대한 Resource Explorer 읽기 전용 AWS 관리형 정책
  - IAM 역할, 그룹 또는 사용자에 대한 다음과 같은 최소 권한을 포함하는 문이 포함된 IAM 권한 정책

    ```
    {
        "Effect": "Allow",
        "Action": [
            "resource-explorer-2:Search",
            "resource-explorer-2:GetView",
        "Resource": "<ARN of the view>"
    }
    ```

- 일반적으로 관리자 작업으로 간주되지만 신뢰할 수 있는 사용자에게 뷰 생성을 정의하는 권한을 위임할 수 있습니다. 이를 위해 관리자는 관련 역할, 그룹 또는 사용자에게 연결된 IAM 권한 정책에서 `resource-explorer-2:CreateView` 작업을 호출할 수 있는 권한을 부여할 수 있습니다. 뷰에 특정 권한이 필요한 경우 관련 사용자에 대한 IAM 정책을 추가하거나 수정하기 위한 조항을 마련해야 합니다.

Resource Explorer를 사용하여 리소스를 검색하는 방법은 리소스 검색에 AWS 리소스 탐색기 사용를 참조하세요.

인덱스

인덱스는 Resource Explorer에서 AWS 계정에 있는 한 AWS 리전의 모든 AWS 리소스에 대해 유지 관리하는 정보를 모아 놓은 것입니다. Resource Explorer는 Resource Explorer를 활성화하는 각 리전에서 인덱스를 유지합니다. Resource Explorer는 AWS 계정에서 리소스를 생성하고 삭제할 때 자동으로 인덱스를 업데이트합니다. 이전 다이어그램에서 AWS 리전 이름 아래의 상자는 각 AWS 리전에서 유지 관리되는 Resource Explorer 인덱스를 나타냅니다. 리전에 있는 인덱스는 해당 리전에서 생성한 모든 뷰에 대한 정보 소스입니다. 사용자는 인덱스를 직접 쿼리할 수 없습니다. 대신 항상 뷰를 사용하여 쿼리해야 합니다.

인덱스에는 두 가지 유형이 있습니다.

로컬 인덱스

Resource Explorer를 활성화하는 모든 AWS 리전마다 로컬 인덱스가 하나씩 있습니다. 로컬 인덱스에는 동일한 리전의 리소스에 대한 정보만 포함됩니다.

애그리게이터 인덱스

Resource Explorer 관리자는 한 AWS 리전에 있는 인덱스를 AWS 계정의 애그리게이터 인덱스로 지정할 수도 있습니다. 애그리게이터 인덱스는 계정에서 Resource Explorer가 활성화되어 있는 다른 모든 리전의 인덱스 복제본을 수신하여 저장합니다. 또한 애그리게이터 인덱스는 자체 리전의 리소스에 대한 정보를 수신하여 저장합니다. 이전 다이어그램에서, 리전 `us-west-2`에는 계정의 애그리게이터 인덱스가 포함되어 있습니다. 계정의 애그리게이터 인덱스를 지정하는 주된 이유는 계정에 있는 모든 리전의 리소스를 포함할 수 있는 뷰를 생성할 수 있기 때문입니다. 한 AWS 계정에는 애그리게이터 인덱스가 하나만 있을 수 있습니다.

Resource Explorer를 활성화하면 애그리게이터 인덱스를 포함할 AWS 리전을 지정할 수 있습니다. 나중에 애그리게이터 인덱스에 사용되는 AWS 리전을 변경할 수도 있습니다. 로컬 인덱스를 승격하여 해당 AWS 계정의 애그리게이터 인덱스로 만드는 방법에 대한 자세한 내용은 애그리게이터 인덱스를 생성하여 리전 간 검색 활성화를 참조하세요.

인덱스는 Amazon 리소스 이름(ARN)을 가진 리소스입니다. 하지만 인덱스와 직접 상호 작용하는 작업에 대한 액세스 권한을 부여하는 권한 정책에서만 이 ARN을 사용할 수 있습니다. 이러한 작업을 통해 뷰를 생성하여 리전의 기본값으로 설정하고, 리전에서 Resource Explorer를 활성화하거나 비활성화하고, 계정의 애그리게이터 인덱스를 생성할 수 있습니다. 인덱스의 ARN은 다음 예제와 유사합니다.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd11111111
```

뷰

뷰는 인덱스에 나열된 리소스를 쿼리하는 데 사용되는 메커니즘입니다. 뷰는 인덱스에서 검색 및 발견 목적으로 표시되고 사용할 수 있는 정보를 정의합니다. 사용자는 Resource Explorer 인덱스를 직접 쿼리하지 않습니다. 대신 쿼리는 항상 뷰를 거쳐야 하므로 뷰 작성자는 사용자가 검색 결과에서 볼 수 있는 리소스를 제한할 수 있습니다.

뷰를 생성할 때 검색 결과에 포함되는 리소스를 제한하는 필터를 지정합니다. 예를 들어 이 뷰에 대한 액세스 권한을 부여하는 사용자가 사용하는 몇 가지 지정된 리소스 유형의 리소스만 포함하도록 선택

할 수 있습니다. 사용자가 뷰를 통해 작성한 쿼리의 결과는 항상 뷰의 기준과 일치하는 리소스만 포함하도록 자동으로 필터링됩니다.

뷰 사용에 대한 액세스를 부여하려면 다음 방법 중 하나를 사용하여 권한 할당을 사용할 수 있습니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하십시오:

- AWS IAM Identity Center의 사용자 및 그룹:

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

  ID 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 사용자(콘솔)에 권한 추가의 지침을 따르세요.

역할, 그룹 또는 사용자가 Amazon 리소스 이름 (ARN)으로 식별되는 뷰에서 `resource-explorer-2:GetView` 및 `resource-explorer-2:Search` 작업을 호출할 수 있도록 권한을 부여합니다. 또는 뷰를 사용하여 검색해야 하는 모든 보안 주체에 대해 Resource Explorer 읽기 전용 AWS 관리형 정책을 사용할 수 있습니다. 필터와 범위가 다른 여러 뷰를 생성하여 리소스 정보의 다른 하위 집합을 반환할 수 있습니다. 그런 다음 해당 뷰의 결과에 포함된 정보를 확인해야 하는 사용자에게 각 뷰에 대한 권한을 부여할 수 있습니다.

Resource Explorer로 검색하려면 각 사용자에게 하나 이상의 뷰를 사용할 수 있는 권한이 있어야 합니다. 뷰를 사용하지 않고는 Resource Explorer에서 검색을 수행할 수 없습니다.

뷰는 리전 단위로 저장됩니다. 뷰는 해당 AWS 리전에 있는 Resource Explorer 인덱스에만 액세스할 수 있습니다. 계정 전체 검색 결과에 액세스하려면 계정의 애그리게이터 인덱스가 포함된 리전의 뷰를 사용해야 합니다. 빠른 설정 옵션은 계정에서 사용하는 모든 AWS 리전의 모든 리소스를 포함하는 필터와 애그리게이터 인덱스가 있는 AWS 리전에 기본 뷰를 생성합니다.

뷰를 생성하는 방법에 대한 자세한 내용은 검색에 대한 액세스를 제공하기 위한 Resource Explorer 뷰 관리를 참조하세요. 쿼리에서 뷰를 사용하는 방법에 대한 자세한 내용은 리소스 검색에 AWS 리소스 탐색기 사용를 참조하세요.

모든 뷰에는 권한 정책에서 참조하여 개별 뷰에 대한 액세스 권한을 부여할 수 있는 Amazon 리소스 이름(ARN)이 있습니다. 뷰와 상호 작용하는 모든 API 또는 AWS CLI 작업에 뷰의 ARN을 파라미터로 전달할 수도 있습니다. 뷰의 ARN은 다음 예제와 유사합니다.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View-
Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> 모든 뷰 ARN에는 마지막에 AWS 생성 UUID가 포함됩니다. 이렇게 하면 삭제된 특정 이름의 뷰에 대한 액세스가 있었던 사용자를 동일한 이름으로 생성된 새로운 뷰에 자동으로 액세스할 수 없도록 할 수 있습니다.

Resource

리소스는 작업할 수 있는 AWS의 엔터티입니다. 리소스는 서비스의 기능을 사용할 때 AWS 서비스에 의해 생성됩니다. 예를 들어 Amazon EC2 인스턴스, Amazon S3 버킷 또는 AWS CloudFormation 스택이 있습니다. 일부 리소스 유형에는 고객 데이터가 포함될 수 있습니다. 모든 리소스 유형에는 리소스를 고유하게 참조하는 데 사용하는 이름, 설명, Amazon 리소스 이름(ARN)을 포함하여 리소스를 설명하는 속성 또는 메타데이터가 있습니다. 대부분의 리소스 유형은 태그도 지원합니다. 태그는 청구 시 비용 할당, 속성 기반 액세스 제어를 사용한 보안 권한 부여, 기타 분류 요구 사항 지원 등 다양한 목적으로 리소스에 연결할 수 있는 사용자 지정 메타데이터입니다.

Resource Explorer의 기본 목적은 AWS 계정에 있는 리소스를 쉽게 찾을 수 있도록 하는 것입니다. Resource Explorer는 다양한 기술을 사용하여 모든 리소스를 검색하고 이에 대한 정보를 인덱스에 배치합니다. 그런 다음 관리자가 제공하는 모든 뷰를 통해 인덱스를 쿼리할 수 있습니다.

> **Important**
>
> Resource Explorer에서는 고객 데이터를 노출시킬 수 있는 리소스 유형을 의도적으로 제외합니다. 다음 리소스 유형은 Resource Explorer에서 인덱싱되지 않으므로 검색 결과에 반환되지 않습니다.
>
> - 버킷 내에 포함된 Amazon S3 객체
> - Amazon DynamoDB 테이블 항목
> - DynamoDB 속성 값

AWS Management Console에서 통합 검색

모든 AWS 서비스의 AWS Management Console 상단에는 다양한 AWS 관련 항목을 검색하는 데 사용할 수 있는 검색 창이 있습니다. 서비스 및 기능을 검색하고 해당 서비스의 콘솔에서 관련 페이지로 직접 연결되는 링크를 얻을 수 있습니다. 검색어와 관련된 설명서 및 블로그 기사를 검색할 수도 있습니다.

Resource Explorer를 활성화하고 애그리게이터 인덱스 및 기본 뷰를 생성한 후 통합 검색을 통해 계정의 리소스를 검색 결과에 포함할 수도 있습니다. 통합 검색은 계정의 애그리게이터 인덱스가 포함된 AWS 리전의 기본 뷰를 자동으로 사용합니다. 이를 통해 Resource Explorer를 먼저 열지 않고도 AWS Management Console의 모든 페이지에서 리소스를 검색할 수 있습니다. 로컬 인덱스를 계정의 애그리게이터 인덱스로 승격하지 않거나 애그리게이터 인덱스 리전에 기본 뷰를 생성하지 않는 경우 통합 검색의 검색 결과에 리소스가 포함되지 않습니다. 또한 검색을 수행하는 모든 보안 주체는 애그리게이터 인덱스가 포함된 리전의 기본 뷰를 사용할 권한이 있어야 합니다. 그렇지 않으면 통합 검색의 검색 결과에 리소스가 포함되지 않습니다.

> **Important**
>
> 통합 검색은 문자열의 첫 번째 키워드 끝에 와일드카드 문자(*) 연산자를 자동으로 삽입합니다. 즉, 통합 검색 결과에는 지정된 키워드로 시작하는 모든 문자열과 일치하는 리소스가 포함됩니다.
>
> Resource Explorer 콘솔의 리소스 검색 페이지에 있는 쿼리 텍스트 상자에서 수행되는 검색에는 와일드카드 문자가 자동으로 추가되지 않습니다. 검색 문자열에서 용어 뒤에 *를 수동으로 삽입할 수 있습니다.

통합 검색 및 Resource Explorer와의 통합에 대한 자세한 내용은 AWS Management Console에서 통합 검색 사용를 참조하세요.

다중 계정 검색

다중 계정 검색을 사용하면 단일 키워드 검색으로 AWS Organizations, AWS 리전에 걸쳐 리소스를 검색하고 찾을 수 있습니다.

다중 계정 검색에 대한 자세한 내용 및 Resource Explorer에서 다중 계정 검색을 활성화하는 방법에 대한 자세한 내용은 다중 계정 검색 활성화를 참조하세요.

Resource Explorer를 사용하기 위한 사전 조건

AWS 리소스 탐색기 를 처음 사용하기 전에 필요에 따라 다음 작업을 완료합니다.

Tasks

- 에 가입 AWS 계정
- 관리자 액세스 권한이 있는 사용자 생성

에 가입 AWS 계정

가 없는 경우 다음 단계를 AWS 계정완료하여 를 생성합니다.

에 가입하려면 AWS 계정

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

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

   에 가입하면 AWS 계정AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/로 이동하여 내 계정 을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 를 AWS 계정보호하고, 를 AWS 계정 루트 사용자활성화하고 AWS IAM Identity Center, 관리 사용자를 생성합니다.

보안 AWS 계정 루트 사용자

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

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하십시오.

2. 루트 사용자에 대해 다중 인증(MFA)을 켭니다.

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

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM Identity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송URL된 로그인을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

Resource Explorer 설정 및 구성

설정하고 AWS 리소스 탐색기구성하기 전에 먼저 사전 요구 사항을 충족하는지 확인하십시오. 그런 다음 다음 절차에 따라 리소스 탐색기 작업을 수행하는 데 필요한 권한을 가진 IAM 역할 또는 사용자로 로그인합니다.

이 설정 및 구성 절차를 사용하여 기존 계정과 조직에 추가된 새 계정에서 리소스 탐색기를 설정할 수 있습니다.

Resource Explorer 설정 방법은 두 가지입니다.

- 빠른 설정
- 고급 설정

> **Important**
>
> "모두 AWS 리전"라고 표시된 옵션을 사용하여 리소스 탐색기를 설정하는 경우 절차를 수행할 AWS 계정때 존재하고 활성화된 AWS 리전 항목만 활성화됩니다. 리소스 탐색기는 향후 AWS 리전 AWS 추가되는 항목을 자동으로 켜지 않습니다. 새 지역이 AWS 도입되면 리소스 탐색기가 리소스 탐색기 콘솔의 설정 페이지에 표시될 때 수동으로 활성화하거나 CreateIndex작업을 호출하여 해당 지역의 리소스 탐색기를 활성화하도록 선택할 수 있습니다.

> **Note**
>
> Resource Explorer를 설정하면 AWS Management Console의 통합 검색 창을 사용하여 리소스를 검색하는 기능을 활성화할 수도 있습니다. 사용자가 통합 검색 결과에서 리소스를 볼 수 있게 하려면 교차 리전 애그리게이터 인덱스와 기본 뷰로 Resource Explorer를 구성해야 합니다. 자세한 내용은 다음 절차를 참조하세요. 또한 검색 중인 사용자에게 애그리게이터 색인이 포함된 기본 보기를 사용할 수 AWS 리전 있는 권한이 있는지 확인해야 합니다. 자세한 내용은 AWS Management Console에서 통합 검색 사용 단원을 참조하십시오.

빠른 설정을 사용하여 Resource Explorer 설정

빠른 설정 옵션을 선택하면 Resource Explorer가 다음을 수행합니다.

- 모든 항목에 색인을 생성합니다 AWS 리전 . AWS 계정
- 계정의 애그리게이터 인덱스로 지정한 리전에 있는 인덱스를 업데이트합니다.
- 애그리게이터 인덱스 리전에 기본 뷰를 생성합니다. 이 뷰에는 필터가 없으므로 인덱스에서 찾은 모든 리소스를 반환합니다.

최소 권한

다음 절차의 단계를 수행하려면 다음 권한이 있어야 합니다.

- 작업: `resource-explorer-2:*`-리소스: 특정 리소스 없음(*)
- 작업: `iam:CreateServiceLinkedRole` - 리소스: 특정 리소스 없음(*)

AWS Management Console

빠른 설정을 사용하여 Resource Explorer를 설정하려면

1. https://console.aws.amazon.com/resource-explorer에서 AWS 리소스 탐색기 콘솔을 엽니다.
2. Resource Explorer 활성화를 선택합니다.
3. Resource Explorer 활성화 페이지에서 빠른 설정을 선택합니다.
4. 애그리게이터 인덱스에 포함할 AWS 리전 항목을 선택합니다. 사용자의 지리적 위치에 적합한 리전을 선택해야 합니다.
5. 페이지 하단에서 Resource Explorer 활성화를 선택합니다.
6. 진행률 페이지에서 Resource Explorer가 인덱스를 생성할 때 각 AWS 리전 을 모니터링할 수 있습니다. 페이지에는 애그리게이터 인덱스 생성 및 기본 뷰 생성 상태가 표시됩니다.

모든 단계가 성공적으로 완료된 것으로 나타나면 사용자는 리소스 검색 페이지로 이동하여 리소스 검색을 시작할 수 있습니다.

> **Note**
>
> 인덱스에 로컬로 태그가 지정된 리소스는 몇 분 내에 검색 결과에 나타납니다. 태그가 지정되지 않은 리소스는 일반적으로 표시되는 데 2시간 미만이 소요되지만 수요가 많을 경우 더 오래 걸릴 수 있습니다. 또한 모든 기존 로컬 인덱스에서 새 애그리게이터 인덱스로의 초기 복제를 완료하는 데 최대 1시간이 걸릴 수 있습니다.

다음 단계: 사용자가 방금 생성한 기본 뷰로 검색할 수 있으려면 먼저 해당 뷰로 검색할 수 있는 권한을 부여해야 합니다. 자세한 내용은 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여 단원을 참조하십시오.

AWS CLI

를 사용하여 리소스 탐색기를 설정하는 AWS CLI 것은 정의상 고급 설치 옵션과 동일합니다. AWS 계정 이는 리소스 탐색기 콘솔처럼 리소스 탐색기 CLI 작업이 자동으로 어떤 단계도 수행하지 않기

때문입니다. 콘솔을 사용하는 것과 동일한 명령을 고급 설정을 사용하여 Resource Explorer 설정 보려면 의 AWS CLI 탭을 참조하십시오.

고급 설정을 사용하여 Resource Explorer 설정

고급 설정 옵션을 선택한 경우 다음을 수행할 수 있습니다.

- 리소스 탐색기를 켤 위치를 선택합니다. AWS 리전
- 애그리게이터 인덱스로 하나의 리전을 구성할지 여부를 선택합니다. 그럴 경우 파일을 AWS 리전 배치할 위치를 지정합니다. 이 인덱스를 사용하면 계정에 있는 모든 리전의 리소스를 포함할 수 있는 뷰를 생성할 수 있습니다. 자세한 내용은 애그리게이터 인덱스를 생성하여 리전 간 검색 활성화를 참조하세요.
- 기본 뷰를 생성할지 여부를 선택합니다. 이 보기에서는 AWS 리소스 탐색기를 켠 지역의 모든 리소스를 자동으로 검색할 수 있습니다. Resource Explorer에서 기본 뷰를 사용하여 검색해야 하는 모든 보안 주체에게 해당 뷰에 대한 권한이 있는지 확인해야 합니다. 자세한 내용은 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여 단원을 참조하십시오.

> **Note**
>
> AWS Management Console의 통합 검색 기능에서 제공하는 검색 결과에 리소스를 포함하도록 Resource Explorer를 구성할 수 있습니다. 이 기능을 활성화하려면 모든 역할 및 사용자가 검색할 수 있는 애그리게이터 인덱스와 기본 뷰로 Resource Explorer를 구성해야 합니다. 빠른 설정 옵션은 애그리게이터 인덱스와 기본 뷰를 모두 생성하며 Resource Explorer를 활성화하는 권장되는 방법입니다.

최소 권한

다음 절차의 단계를 수행하려면 다음 권한이 있어야 합니다.

- 작업: `resource-explorer-2:*`-리소스: 특정 리소스 없음(*)
- 작업: `iam:CreateServiceLinkedRole` - 리소스: 특정 리소스 없음(*)

AWS Management Console

고급 설정을 사용하여 Resource Explorer를 활성화하려면

1. https://console.aws.amazon.com/resource-explorer에서 AWS 리소스 탐색기 콘솔을 엽니다.
2. Resource Explorer 활성화를 선택합니다.
3. Resource Explorer 활성화 페이지에서 고급 설정을 선택합니다.
4. AWS 리전상자의 지역에서 리소스 탐색기를 전체 AWS 리전또는 특정 지역에서만 활성화할지 여부를 선택합니다.

   이 계정의 지정된 AWS 리전 에서만 Resource Explorer 활성화를 선택하는 경우 검색 결과에 리소스를 포함할 각 리전을 선택합니다.
5. 애그리게이터 인덱스의 경우 애그리게이터 인덱스를 생성할지 여부를 선택합니다. 애그리게이터 인덱스를 생성하도록 선택한 경우 다른 모든 인덱스는 해당 인덱스를 이 리전에 AWS 리전 복제합니다. 이렇게 하면 사용자가 에서 선택한 모든 지역의 리소스를 검색할 수 있습니다. AWS 계정애그리게이터 인덱스가 AWS 리전 포함된 항목을 선택하세요. 사용자가 가장 많은 시간을 보내는 리전 또는 최소한 사용자가 대부분의 리소스 검색을 수행할 것으로 예상되는 리전을 지정하는 것이 좋습니다.
6. 기본 뷰 상자의 뷰 생성에서 기본 뷰를 생성할지 여부를 선택합니다. 이 옵션은 애그리게이터 인덱스를 생성하도록 선택한 경우에만 사용할 수 있습니다. 기본 보기를 만들도록 선택하면 Resource Explorer에서 이 보기를 집계자 색인과 AWS 리전 같은 위치에 배치합니다. 이렇게 하면 리소스 탐색기를 등록한 모든 AWS 리전 결과의 결과가 기본 보기에 포함될 수 있습니다. 사용자가 기본 뷰를 사용하여 리전에서 검색을 수행하고 뷰를 명시적으로 지정하지 않을 때마다 검색에 해당 리전의 기본 뷰가 사용됩니다.

   > **Note**
   >
   > 사용자가 뷰를 통해 검색할 수 있으려면 먼저 해당 뷰를 사용할 수 있는 권한을 부여해야 합니다. 자세한 내용은 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여 단원을 참조하십시오.
7. Resource Explorer 활성화를 선택합니다.

   > **Note**
   >
   > 인덱스에 로컬로 태그가 지정된 리소스는 몇 분 내에 검색 결과에 나타납니다. 태그가 지정되지 않은 리소스는 일반적으로 표시되는 데 2시간 미만이 소요되지만 수요가 많

을 경우 더 오래 걸릴 수 있습니다. 또한 모든 기존 로컬 인덱스에서 새 애그리게이터 인덱스로의 초기 복제를 완료하는 데 최대 1시간이 걸릴 수 있습니다.

AWS CLI

고급 설정을 사용하여 Resource Explorer를 설정하려면

리소스 탐색기 콘솔은 사용자의 선택에 따라 사용자를 대신하여 많은 API 작업 호출을 수행합니다. 다음 예제 AWS CLI 명령은 를 사용하여 콘솔 외부에서 동일한 기본 절차를 수행하는 방법을 보여 줍니다. AWS CLI

Example 1단계: 원하는 AWS 리전에 인덱스를 생성하여 Resource Explorer 활성화

리소스 탐색기를 활성화하려는 각 AWS 리전 위치에서 다음 명령을 실행합니다. 다음 예제 명령은 AWS 리전 의 기본값인 AWS CLI에서 Resource Explorer를 활성화합니다.

```
$ aws resource-explorer-2 create-index
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-27T16:17:12.130000+00:00",
    "State": "CREATING"
}
```

Example 2단계: 계정의 애그리게이터 인덱스가 AWS 리전 되도록 인덱스를 하나로 업데이트합니다.

리소스 탐색기에서 로컬 인덱스를 계정의 애그리게이터 인덱스로 업데이트하도록 하려면 다음 명령을 실행합니다. AWS 리전 다음 예제 명령은 미국 동부(버지니아 북부)(us-east-1)에서 애그리게이터 인덱스를 업데이트합니다.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt": "2022-07-27T16:29:49.231000+00:00",
    "State": "UPDATING",
```

```
    "Type": "AGGREGATOR"
}
```

Example 3단계: 애그리게이터 AWS 리전 인덱스가 포함된 뷰 만들기

애그리게이터 인덱스를 생성할 때 사용한 다음 명령을 실행합니다. AWS 리전 다음 예제 명령은 Resource Explorer 콘솔 설정 프로세스에서 생성된 것과 동일한 뷰를 생성합니다. 이 새로운 뷰에는 인덱싱된 정보의 일부로 리소스에 연결된 태그가 포함되어 있으며 태그 키 또는 값을 기준으로 리소스 검색을 지원합니다.

```
$ aws resource-explorer-2 create-view \
    --view-name My-New-View \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-07-27T16:34:14.960000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222"
    }
}
```

Example 4단계: 새 뷰를 기본 뷰로 설정 AWS 리전

다음 예제에서는 이전 단계에서 생성한 뷰를 리전의 기본값으로 설정합니다. 기본 뷰를 만든 뷰와 동일한 AWS 리전 위치에서 다음 명령을 실행해야 합니다.

```
$ aws resource-explorer-2 associate-default-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
```

```
}
```

사용자가 뷰를 통해 검색할 수 있으려면 먼저 해당 뷰를 사용할 수 있는 권한을 부여해야 합니다. 자세한 내용은 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여 단원을 참조하십시오.

이러한 명령을 실행하면 Resource Explorer가 AWS 계정의 지정된 리전에서 실행됩니다. Resource Explorer는 각 리전에 위치한 리소스의 세부 정보가 포함된 인덱스를 구축하고 유지 관리합니다. Resource Explorer는 각 개별 리전 인덱스를 지정된 리전에 있는 애그리게이터 인덱스에 복제합니다. 또한 이 지역에는 계정의 모든 IAM 역할 또는 사용자가 인덱싱된 모든 지역의 리소스를 검색할 수 있는 보기가 포함되어 있습니다.

> **Note**
>
> 인덱스에 로컬로 태그가 지정된 리소스는 몇 분 내에 검색 결과에 나타납니다. 태그가 지정되지 않은 리소스는 일반적으로 표시되는 데 2시간 미만이 소요되지만 수요가 많을 경우 더 오래 걸릴 수 있습니다. 또한 모든 기존 로컬 인덱스에서 새 애그리게이터 인덱스로의 초기 복제를 완료하는 데 최대 1시간이 걸릴 수 있습니다.

리소스 탐색기가 켜져 있는 AWS 리전 사용자 식별

지역에 Resource Explorer용 색인이 포함되어 있는지 확인하여 어느 AWS 리전 지역이 AWS 리소스 탐색기 활성화되었는지 확인할 수 있습니다. 인덱스가 있는 리전을 보려면 이 페이지의 절차를 사용하세요.

> **Important**
>
> 사용자는 Resource Explorer가 활성화된 리전에서만 리소스를 검색할 수 있습니다. 또한 한 리전에 애그리게이터 인덱스를 생성하여 모든 리전의 리소스 검색을 지원할 수 있습니다. Resource Explorer는 Resource Explorer 인덱스가 포함된 다른 모든 리전으로부터 애그리게이터 인덱스가 있는 리전에 리소스 정보를 복제합니다. 사용자는 Resource Explorer를 사용하여 인덱스가 없는 리전의 리소스를 검색할 수 없습니다.

리전의 Resource Explorer 상태 확인

를 사용하거나, AWS Command Line Interface (AWS CLI) 의 명령을 사용하거나 AWS Management Console, 에서 API 작업을 사용하여 리소스 탐색기용 색인이 있는 지역을 확인할 수 있습니다. AWS SDK

AWS Management Console

Resource Explorer에 대한 인덱스가 있는 리전을 확인하려면

1. Resource Explorer 콘솔에서 설정 페이지를 엽니다.
2. 인덱스 섹션의 목록에는 Resource Explorer 인덱스가 포함된 리전만 포함됩니다. 유형 열의 값은 인덱스가 해당 리전의 로컬 인덱스인지, 아니면 AWS 계정의 애그리게이터 인덱스인지를 나타냅니다.
3. Resource Explorer가 포함되지 않은 리전을 확인하려면 인덱스 생성을 선택합니다. 리전이 없는 경우 해당 리전에는 Resource Explorer가 포함되지 않은 것입니다.

AWS CLI

Resource Explorer에 대한 인덱스가 있는 리전을 확인하려면

다음 명령을 실행하여 리소스 탐색기용 색인이 AWS 리전 있는 항목을 확인합니다.

```
$ aws resource-explorer-2 list-indexes
{
    "Indexes": [
        {
            "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Region": "us-east-1",
            "Type": "AGGREGATOR"
        },
        {
            "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
            "Region":"us-west-2",
            "Type":"LOCAL"
        }
    ]
}
```

에서 리소스 탐색기를 켜서 리소스를 인덱싱합니다. AWS 리전

를 처음 AWS 리소스 탐색기 켜면 서비스에 대한 색인이 하나 이상 AWS 리전생성되었습니다. AWS 계정빠른 설정 옵션을 사용한 경우 Resource Explorer가 AWS 계정에서 활성화된 모든AWS 리전에 인덱스를 자동으로 생성합니다. 또한 Resource Explorer 서비스는 지정된 리전에 있는 인덱스를 계정의 애그리게이터 인덱스로 승격시킵니다. 고급 설정 옵션을 사용한 경우 인덱스를 생성할 리전을 지정합니다.

주제

- 리전에서 Resource Explorer 인덱스 생성
- AWS 옵트인 지역에 대한 고려사항

에서 리소스 탐색기를 켜면 서비스가 다음 작업을 수행합니다. AWS 리전

- 의 첫 번째 지역에서 리소스 탐색기를 시작하면 리소스 탐색기가 이름이 지정된 계정에 서비스 연결 역할을 만듭니다. AWS 계정`AWSServiceRoleForResourceExplorer` 이 역할은 Resource Explorer가 AWS CloudTrail 및 태그 지정 서비스와 같은 서비스를 사용하여 계정의 리소스를 검색하고 인덱싱할 수 있는 권한을 부여합니다. 서비스 연결 역할은 계정에 첫 AWS 리전 번째 역할을 등록한 경우에만 생성됩니다. Resource Explorer는 나중에 추가하는 모든 추가 리전에 대해 동일한 서비스 연결 역할을 사용합니다.
- Resource Explorer는 지정된 리전에 인덱스를 생성하여 해당 리전의 리소스에 대한 세부 정보를 저장합니다.
- Resource Explorer는 지정된 리전의 리소스를 검색하기 시작하고 리소스에 대해 찾은 정보를 해당 리전의 인덱스에 추가합니다.
- 계정에 이미 다른 리전에 애그리게이터 인덱스가 포함되어 있는 경우, Resource Explorer는 새 리전의 인덱스의 정보를 애그리게이터 인덱스로 복제하기 시작하여 교차 리전 검색을 지원합니다.

이러한 단계가 완료되면 사용자가 리소스에 대한 정보를 검색할 수 있습니다. 사용자는 동일한 리전 또는 애그리게이터 인덱스가 포함된 리전에 정의된 뷰 중 하나를 사용하여 검색할 수 있습니다.

리전에서 Resource Explorer 인덱스 생성

를 사용하거나, AWS Command Line Interface (AWS CLI) 의 명령을 사용하거나 AWS Management Console, 에서 API 작업을 사용하여 추가로 AWS 리전 리소스 탐색기 색인을 만들 수 있습니다. AWS SDK 한 리전에 하나의 인덱스만 생성할 수 있습니다.

최소 권한

다음 절차의 단계를 수행하려면 다음 권한이 있어야 합니다.

- 작업: `resource-explorer-2:*`-리소스: 특정 리소스 없음(*)
- 작업: `iam:CreateServiceLinkedRole` - 리소스: 특정 리소스 없음(*)

AWS Management Console

에서 리소스 탐색기 색인을 만들려면 AWS 리전

1. Resource Explorer 설정 페이지에서
2. 인덱스 섹션에서 인덱스 생성을 선택합니다.
3. 색인 생성 페이지에서 색인을 만들려는 색인 AWS 리전 옆의 확인란을 선택하여 해당 지역의 리소스 검색을 지원합니다. 사용할 수 없는 확인란은 Resource Explorer 인덱스가 이미 포함되어 있는 리전을 나타냅니다.
4. (선택 사항) 태그 섹션에서 인덱스에 대한 태그 키와 값 쌍을 지정할 수 있습니다.
5. 인덱스 생성을 선택합니다.

   Resource Explorer는 페이지 상단에 녹색 배너를 표시하여 성공을 나타내거나, 선택한 리전 중 하나 이상에 인덱스를 생성하는 동안 오류가 발생한 경우 빨간색 배너를 표시합니다.

> **Note**
>
> 인덱스에 로컬로 태그가 지정된 리소스는 몇 분 내에 검색 결과에 나타납니다. 태그가 지정되지 않은 리소스는 일반적으로 표시되는 데 2시간 미만이 소요되지만 수요가 많을 경우 더 오래 걸릴 수 있습니다. 또한 모든 기존 로컬 인덱스에서 새 애그리게이터 인덱스로의 초기 복제를 완료하는 데 최대 1시간이 걸릴 수 있습니다.

다음 단계 - 이미 애그리게이터 인덱스를 생성한 경우 새 리전이 자동으로 해당 인덱스 정보를 애그리게이터 인덱스에 복제하기 시작합니다. 사용자가 여기에서 모든 검색을 수행하는 경우 새 리전의 리소스가 해당 검색 결과에 표시되고 작업이 완료됩니다.

하지만 사용자가 새로 인덱싱된 리전에서만 리소스를 검색할 수 있도록 하려면 해당 리전의 사용자에 대한 뷰도 생성하고 사용자에게 해당 뷰에 대한 권한을 부여해야 합니다. 뷰를 생성하는 방법에 대한 지침은 검색에 대한 액세스를 제공하기 위한 Resource Explorer 뷰 관리를 참조하세요.

AWS CLI

에서 리소스 탐색기 색인을 만들려면 AWS 리전

색인을 만들려는 각 AWS 리전 영역에 대해 다음 명령을 실행하여 해당 지역의 리소스 검색을 지원합니다. 다음 예제 명령은 미국 동부(버지니아 북부)(`us-east-1`)에 Resource Explorer를 등록합니다.

```
$ aws resource-explorer-2 create-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-11-01T20:00:59.149Z",
    "State": "CREATING"
}
```

Resource Explorer를 활성화하려는 각 리전에 대해 이 명령을 반복합니다. 이때 `--region` 파라미터는 해당 리전 코드로 대체합니다.

Resource Explorer는 일부 인덱스 생성을 백그라운드에서 비동기 작업으로 수행하기 때문에 응답이 `CREATING`일 수 있으며, 이는 백그라운드 프로세스가 아직 완료되지 않았음을 나타냅니다.

> **Note**
>
> 인덱스에 로컬로 태그가 지정된 리소스는 몇 분 내에 검색 결과에 나타납니다. 태그가 지정되지 않은 리소스는 일반적으로 표시되는 데 2시간 미만이 소요되지만 수요가 많을 경우 더 오래 걸릴 수 있습니다. 또한 모든 기존 로컬 인덱스에서 새 애그리게이터 인덱스로의 초기 복제를 완료하는 데 최대 1시간이 걸릴 수 있습니다.

다음 명령을 실행하고 `ACTIVE` 상태를 확인하여 최종 완료 여부를 확인할 수 있습니다.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

다음 단계 - 이미 애그리게이터 인덱스를 생성한 경우 새 리전이 자동으로 해당 인덱스 정보를 애그리게이터 인덱스에 복제하기 시작합니다. 사용자가 여기에서 모든 검색을 수행하는 경우 새 리전의 리소스가 해당 검색 결과에 표시되고 작업이 완료됩니다.

하지만 사용자가 새로 인덱싱된 리전에서만 리소스를 검색할 수 있도록 하려면 해당 리전의 사용자에 대한 뷰도 생성하고 사용자에게 해당 뷰에 대한 권한을 부여해야 합니다. 뷰를 생성하는 방법에 대한 지침은 검색에 대한 액세스를 제공하기 위한 Resource Explorer 뷰 관리를 참조하세요.

AWS 옵트인 지역에 대한 고려사항

옵트인 지역은 옵트인 지역의 계정을 통한 IAM 데이터 공유와 관련하여 상업 지역보다 보안 요구 사항이 더 높습니다. IAM서비스를 통해 관리되는 모든 데이터는 ID 데이터로 간주됩니다.

AWS 리소스 탐색기 콘솔을 사용하여 옵트인 리전을 활성화할 수 있습니다. 자세한 내용은 리소스를 AWS 리전 인덱싱하려면 에서 리소스 탐색기 켜기를 참조하십시오.

옵트아웃 동작

옵트인 리전을 옵트아웃하기 전에 다음 동작을 고려하세요.

> **Important**
>
> 애그리게이터 인덱스가 있는 리전을 옵트아웃하기 전에 애그리게이터 인덱스를 삭제하거나 로컬 인덱스로 수준을 내리는 것이 좋습니다. Resource Explorer는 파티션 내 모든 리전에 걸쳐 하나의 애그리게이터 인덱스를 지원합니다.

- 인덱스는 삭제되지 않으며, 비활성화될 뿐입니다. 나중에 다시 옵트인하면 설정이 되돌아갑니다.
- IAM지역의 리소스에 IAM 대한 액세스를 비활성화합니다.
- Resource Explorer는 옵트아웃된 리전의 인덱스를 비활성화하고 데이터 수집을 중단합니다. 더 이상 지역 색인이 `ListIndexes` API 표시되지 않습니다.
- 애그리게이터 인덱스가 다른 리전에 있는 경우 Resource Explorer는 옵트아웃된 리전에서의 데이터 복제를 중지하고 24시간 이내에 데이터를 정리합니다.
- 애그리게이터 인덱스 리전을 옵트아웃한 경우 인덱스를 삭제하거나 수준을 내리려면 다시 옵트인해야 합니다.
- 해당 리전에 다시 옵트인하면 Resource Explorer가 인덱스를 다시 활성화하고 데이터를 수집하기 시작합니다.
- 옵트인 리전의 상태에 대한 모든 변경 사항이 적용되려면 약 24시간이 걸립니다.

애그리게이터 인덱스를 생성하여 리전 간 검색 활성화

리전 간 검색을 활성화하면 의 모든 리전에서 리소스를 검색할 수 있습니다 AWS 계정.

주제

애그리게이터 인덱스 정보

AWS 리소스 탐색기 는 리소스에 대해 수집한 정보를 Resource Explorer가 해당 리전에서 AWS 리전 생성하고 유지하는 로컬 인덱스에 저장합니다. 예를 들어 미국 서부(오레곤) 리전에 Amazon EC2 인스턴스가 있다고 가정합니다. Resource Explorer는 미국 서부(오레곤) 리전에 있는 로컬 인덱스에 해당 리소스에 대한 세부 정보를 저장합니다.

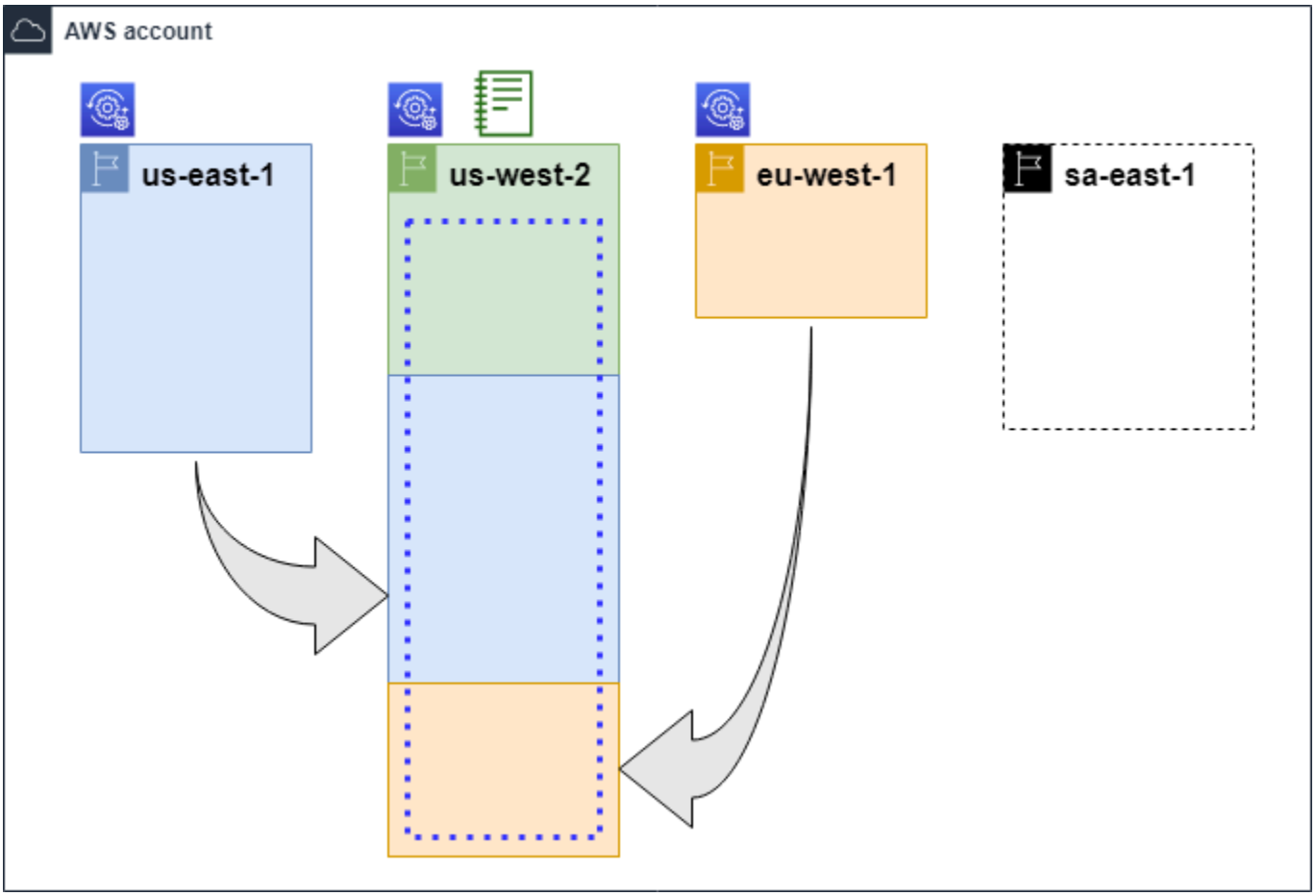
계정 AWS 리전 의 모든 리소스 검색을 지원하려면 한 리전의 로컬 인덱스를 계정의 애그리게이터 인덱스로 변환할 수 있습니다.

애그리게이터 인덱스에는 Resource Explorer를 활성화한 다른 모든 리전에 있는 로컬 인덱스 복제본이 포함되어 있습니다. 이렇게 하면 집계자 인덱스가 포함된 리전에서 뷰를 생성할 수 있습니다. 집계자 인덱스의 결과에는 계정 AWS 리전 의 모든 리소스가 포함될 수 있습니다.

다음 다이어그램에서는 애그리게이터 인덱스의 작동 방식의 예를 보여 줍니다. 이 예제 AWS 계정에서 관리자는 다음을 수행합니다.

- 해당 리전에서 인덱스를 생성하여 3 AWS 리전 (`us-east-1`, `us-west-2`및 `eu-west-1`)으로 Resource Explorer를 켭니다. 각 리전에는 자체 로컬 인덱스가 포함되어 있습니다.
- `sa-east-1` 리전에 인덱스를 생성하지 않도록 선택합니다. 사용자는 `sa-east-1`에서 검색을 수행할 수 없으며 해당 리전의 리소스는 검색 결과에 표시되지 않습니다.
- `us-west-2` 리전에 계정의 애그리게이터 인덱스를 생성합니다. 이렇게 하면 Resource Explorer는 Resource Explorer가 활성화된 다른 모든 리전의 로컬 인덱스에서 애그리게이터 인덱스로 정보를 복제합니다. 이를 통해 `us-west-2`에서 수행된 검색에 Resource Explorer가 활성화되어 있는 세 리전 모두의 리소스가 포함됩니다.

이 구성을 사용하면 사용자는 애그리게이터 인덱스가 포함된 **us-west-2**에서만 리전 간 검색을 수행할 수 있습니다. 해당 리전의 뷰만 계정에 있는 모든 리전의 결과를 반환할 수 있습니다.



범례	
	Resource Explorer는 이 에서 켜져 있으며 AWS 리전리소스는 해당 리전의 인덱스로 카탈로그화됩니다. 이 리전의 인덱스는 애그리게이터 인덱스 AWS 리전 가 포함된 에도 복제됩니다(화살표로 표시됨).
	여기에는 애그리게이터 인덱스가 AWS 리전 포함됩니다. Resource Explorer는 다른 모든 에서 수집된 리소스 정보를 이 리전 AWS 리전 으로 복제합니다.
	빠른 설정에서 생성한 기본 뷰에는 모든 AWS 리전의 모든 리소스가 포함됩니다.

로컬 인덱스를 계정의 애그리게이터 인덱스로 승격

AWS 리소스 탐색기을 처음 설정할 때 한 AWS 리전에 애그리게이터 인덱스를 생성할 수 있는 옵션이 있습니다. 자세한 내용은 Resource Explorer 설정 및 구성 섹션을 참조하세요. 이 절차는 초기 설정 시 수행하지 않은 경우 로컬 인덱스 중 하나를 계정의 애그리게이터 인덱스로 승격시키는 것입니다.

Important

- AWS 계정에는 하나의 애그리게이터 인덱스만 있을 수 있습니다. 계정에 이미 애그리게이터 인덱스가 있는 경우 먼저 이를 로컬 인덱스로 수준을 내리거나 삭제해야 합니다.
- 애그리게이터 인덱스가 포함된 리전을 삭제하거나 변경한 후 다른 인덱스를 애그리게이터 인덱스로 승격하려면 24시간을 기다려야 합니다.

AWS Management Console

로컬 인덱스를 계정의 애그리게이터 인덱스로 승격하려면

1. Resource Explorer 설정 페이지를 엽니다.
2. 인덱스 섹션에서 승격하려는 인덱스 옆의 확인란을 선택한 다음 인덱스 유형 변경을 선택합니다.
3. <리전 이름>의 인덱스 유형 변경 대화 상자에서 애그리게이터 인덱스를 선택한 다음 변경 내용 저장을 선택합니다.

AWS CLI

로컬 인덱스를 계정의 애그리게이터 인덱스로 승격하려면

다음 예제 명령은 지정된 AWS 리전에 있는 인덱스를 유형 LOCAL에서 유형 AGGREGATOR로 업데이트합니다. 애그리게이터 인덱스를 포함할 AWS 리전에서 작업을 호출해야 합니다.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
```

```
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"AGGREGATOR"
}
```

작업은 비동기적으로 작동하며 State가 UPDATING으로 설정된 상태에서 시작됩니다. 작업이 완료되었는지 확인하려면 다음 명령을 실행하고 ACTIVE 응답 필드에서 값 State를 찾을 수 있습니다. 확인하려는 인덱스가 포함된 리전에서 이 명령을 실행해야 합니다.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "AGGREGATOR"
}
```

애그리게이터 인덱스를 로컬 인덱스로 수준 내리기

애그리게이터 인덱스를 다른 AWS 리전으로 이동하려는 경우와 같이 애그리게이터 인덱스를 로컬 인덱스로 수준을 내릴 수 있습니다.

애그리게이터 인덱스를 로컬 인덱스로 수준을 내리면 Resource Explorer가 다른 AWS 리전의 인덱스 복제를 중지합니다. 또한 다른 리전에서 복제된 정보를 삭제하는 비동기 백그라운드 작업을 시작합니다. 해당 비동기 작업이 완료될 때까지 일부 교차 리전 결과가 검색 결과에 계속 표시될 수 있습니다.

> **참고**
>
> - 애그리게이터 인덱스의 수준을 내린 후 동일한 인덱스 또는 다른 리전에 있는 인덱스를 계정의 새 애그리게이터 인덱스로 승격하려면 24시간을 기다려야 합니다.

- 애그리게이터 인덱스를 수준을 내린 후 백그라운드 프로세스가 완료되고 이 리전에서 수행된 검색 결과에서 다른 리전의 모든 리소스 정보가 사라지기까지 최대 36시간이 걸릴 수 있습니다.
- 조직 전체 뷰에서 멤버 계정을 수준을 내리면 해당 멤버가 다중 계정 검색에서 제거될 수 있습니다.

설정 페이지에서 인덱스 목록을 보거나 작업을 사용하여 백그라운드 작업의 상태를 확인할 수 있습니다. GetIndex 비동기 작업이 완료되면 인덱스의 `Status` 필드가 `UPDATING`에서 `ACTIVE`로 변경됩니다. 이때 쿼리 결과에는 로컬 리전의 결과만 표시됩니다.

AWS Management Console

애그리게이터 인덱스를 로컬 인덱스로 수준을 내리려면

1. Resource Explorer 설정 페이지를 엽니다.
2. 인덱스 섹션에서 로컬 인덱스로 수준을 내리려는 애그리게이터 인덱스가 포함된 리전 옆의 확인란을 선택한 다음 인덱스 유형 변경을 선택합니다.
3. <리전 이름>의 인덱스 유형 변경 대화 상자에서 로컬 인덱스를 선택한 다음 변경 내용 저장을 선택합니다.

AWS CLI

애그리게이터 인덱스를 로컬 인덱스로 수준을 내리려면

다음 예제에서는 지정된 애그리게이터 인덱스를 로컬 인덱스로 수준을 내립니다. 현재 애그리게이터 인덱스가 포함된 AWS 리전에서 작업을 호출해야 합니다.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type LOCAL \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"LOCAL"
```

```
}
```

작업은 비동기적으로 작동하며 State가 UPDATING으로 설정된 상태에서 시작됩니다. 작업이 완료되었는지 확인하려면 다음 명령을 실행하고 ACTIVE 응답 필드에서 값 State를 찾을 수 있습니다. 확인하려는 인덱스가 포함된 리전에서 이 명령을 실행해야 합니다.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

다중 계정 검색 활성화

다중 계정 검색을 사용하면 사용자 AWS Organizations 또는 OU (조직 단위) 에 활성 색인이 있는 계정 전반에서 리소스를 검색할 수 있습니다.

주제

사전 조건

조직에 대한 다중 계정 검색을 켜려면 다음을 완료하세요.

- 옵트인 지역의 경우, 다중 계정 검색을 활성화하려는 관리 계정도 옵트인되어 있는지 확인하세요.
- 관리 사용자를 생성합니다.
- `aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com`를 사용하여 관리자 계정에 서비스 연결 역할을 생성합니다.
- 에서 신뢰할 수 있는 액세스를 활성화하세요. AWS Organizations 이렇게 하면 Resource Explorer와 완전히 통합되어 조직의 모든 계정에 걸쳐 리소스를 나열할 수 있습니다.
- 위임된 관리자를 할당합니다(권장). 자세한 내용은 사용 설명서의 Organizations와 함께 작동하는 AWS 서비스의 위임 관리자를 참조하십시오.AWS Organizations
  - Resource Explorer는 관리 계정과 유사한 작업을 수행하는 위임된 관리자를 한 명만 지원합니다.
  - 조직의 위임된 관리자를 제거하거나 변경하면 해당 계정에 생성된 모든 다중 계정 뷰가 제거됩니다.

다중 계정 검색 활성화

조직의 계정 전반에 걸쳐 리소스를 검색하고 발견하려면 다음 단계를 완료해야 합니다.

1. AWS 리소스 탐색기 에 있는 하나 이상의 계정에서 활성화하십시오. AWS Organizations
2. 애그리게이터 인덱스를 포함할 리전 하나를 등록합니다.

3. 애그리게이터 인덱스를 생성할 리전을 선택합니다. 이 지역은 모든 지역에서 일관되어야 합니다 AWS Organizations.
4. 사용자 AWS Organizations 또는 조직 단위로 범위가 지정된 리소스 탐색기 보기를 만드세요. 이전 단계의 애그리게이터 리전에 이 뷰를 생성합니다.
5. 조직 전반에 걸쳐 계정과 뷰를 공유합니다.

다중 계정 빠른 설정

빠른 설정을 통해 조직의 여러 계정에 걸쳐 Resource Explorer를 활성화할 수 있습니다.

> **Note**
>
> 이 프로세스는 관리 계정에 리소스를 배포하지 않습니다. 관리 계정을 사용 중이고 계정에 인덱스를 추가하려는 경우 Resource Explorer 온보딩 흐름을 사용하여 수동으로 인덱스를 추가해야 합니다.

1. Systems Manager 콘솔에서 Resource Explorer의 빠른 설정으로 이동합니다.
2. 애그리게이터 인덱스 리전을 선택합니다. 이렇게 하면 선택한 대상 계정의 모든 리전에 있는 리소스를 검색할 수 있습니다. 선택한 대상 계정 중 하나라도 이미 다른 리전에 애그리게이터 인덱스가 구성되어 있는 경우 기존 애그리게이터 인덱스가 자동으로 이 새 리전으로 대체됩니다.
3. 계정 대상을 선택합니다. 전체 조직 또는 특정 조직 단위에 대해 리소스 탐색기를 활성화할 수 있습니다 (OUs).

   > **Note**
   >
   > 한 번에 최대 50,000개의 AWS CloudFormation 스택을 배포할 수 있습니다. 여러 리전에 걸친 대규모 조직이 있는 경우 OU 수준에서 더 작은 배치로 배포해야 합니다.

4. 생성을 선택하기 전에 승인 요약을 읽어보세요.

Resource Explorer 다중 계정 검색에 대한 계정 작업의 영향

> **Note**
>
> 다중 계정 검색 결과에서 계정 및 리소스를 제거하는 데 최대 24시간이 걸립니다.

계정 작업은 AWS 리소스 탐색기 다중 계정 검색에 다음과 같은 영향을 미칩니다.

Resource Explorer 비활성화됨

계정에 대해 Resource Explorer를 비활성화하면 비활성화할 때 선택한 AWS 리전 의 계정에 대해서만 비활성화됩니다.

Resource Explorer가 활성화된 각 리전에서 별도로 비활성화해야 합니다.

24시간이 지나면 이 계정의 리소스가 검색 결과에 표시되지 않습니다.

기타 Resource Explorer 데이터 및 설정은 제거되지 않습니다.

조직에서 멤버 계정 제거됨

조직에서 멤버 계정이 제거되면 Resource Explorer 관리자 계정은 멤버 계정의 리소스를 볼 수 있는 권한을 잃게 됩니다.

제거된 계정이 관리자 또는 위임된 관리자 계정인 경우 이전에 이러한 계정으로 생성된 다중 계정 뷰도 모두 제거됩니다.

Resource Explorer는 두 계정 모두에서 계속 실행됩니다.

리소스 검색 결과에 더 이상 이 계정의 리소스가 포함되지 않습니다.

계정이 일시 중지됨

계정이 일시 중단되면 해당 계정은 리소스 탐색기에서 리소스를 볼 수 있는 권한을 잃게 됩니다. AWS 일시 중지된 계정의 관리자 계정은 기존 리소스를 볼 수 있습니다.

조직 계정의 경우 멤버 계정 상태가 계정 일시 중지됨으로 변경될 수도 있습니다. 관리자 계정이 계정을 활성화하려고 시도하는 것과 동시에 계정이 일시 중지된 경우 이런 상황이 발생합니다. 계정 일시 중지됨 계정의 관리자 계정은 해당 계정의 리소스를 볼 수 없습니다.

그 외에는 일시 중지됨 상태는 멤버 계정 상태에 영향을 주지 않습니다.

90일이 지나면 계정이 비활성화되거나 다시 활성화됩니다. 계정이 다시 활성화되면 해당 Resource Explorer 권한이 복원됩니다. 멤버 계정 상태가 계정 일시 중지됨인 경우 관리자 계정은 계정을 수동으로 활성화해야 합니다.

계정이 폐쇄되었습니다.

AWS 계정이 폐쇄되면 리소스 탐색기는 다음과 같이 폐쇄에 응답합니다.

- Resource Explorer는 계정 해지 발효일로부터 90일 동안 계정에 대한 리소스를 유지합니다. 90일의 기간이 종료되는 시점에 Resource Explorer는 계정의 모든 리소스를 영구적으로 삭제합니다.
- 리소스를 90일 이상 보존하려면 EventBridge 규칙이 있는 사용자 지정 작업을 사용하여 Amazon S3 버킷에 리소스를 저장할 수 있습니다. Resource Explorer가 리소스를 유지하는 한 해지된 계정을 다시 개설하면 Resource Explorer가 해당 계정의 리소스를 복원합니다.
- 계정이 Resource Explorer 관리자 계정인 경우 관리자 권한이 제거되고 모든 멤버 계정도 제거됩니다. 계정이 멤버 계정인 경우 해당 계정은 Resource Explorer 관리자 계정에서 멤버으로 분리되고 제거됩니다.
- 자세한 내용은 계정 해지를 참조하세요.

계정 옵트아웃

특정 리전에서 옵트아웃해도 최대 24시간 동안 검색 결과에 해당 리소스가 계속 표시됩니다.

24시간이 지나면 이 계정의 리소스가 검색 결과에 표시되지 않습니다. 자세한 내용은 옵트아웃 동작 단원을 참조하십시오.

AWS Management Console에서 통합 검색 지원

모든 콘솔 페이지 상단에 검색 창이 있습니다. AWS Management Console 이를 통해 모든 사용자에게 통합된 검색 환경을 제공합니다 AWS 서비스. 통합 검색 결과에는 다음과 같은 항목이 포함될 수 있습니다.

- AWS 서비스 및 콘솔 페이지 기능.
- AWS 설명서 페이지.
- AWS 블로그 및 기술 자료 문서
- 계정의 리소스 - 아래 단계를 따르면 됩니다.

통합 검색 결과에서 계정의 리소스를 보려면 다음 단계를 수행해야 합니다. 의 초기 설정 중에 이 작업을 수행할 수 AWS 리소스 탐색기있습니다. 빠른 설정 옵션을 사용하면 이 모든 작업이 자동으로 수행됩니다.

- 에 AWS 리전 대한 애그리게이터 인덱스 중 하나에 애그리게이터 인덱스를 만들어야 합니다. AWS 계정
- 애그리게이터 인덱스가 포함된 AWS 리전 에 기본 뷰를 생성해야 합니다.
- 통합 검색 창에서 리소스를 검색해야 하는 모든 보안 주체에게 해당 기본 뷰를 사용하여 검색할 수 있는 권한을 부여해야 합니다.

통합 검색에서는 항상 집계자 AWS 리전 색인이 포함된 의 기본 보기를 사용하여 모든 검색을 수행합니다.

조직의 계정에 Resource Explorer 배포

를 사용하면 AWS CloudFormation StackSets 조직에서 관리하는 모든 계정을 정의하고 배포할 수 AWS Organizations있습니다. 스택 세트를 정의할 때는 사용자 계정 AWS 리전 및 지정한 모든 대상 계정에서 생성하려는 AWS 리소스를 지정합니다. 모든 계정이 동일한 조직에 속해 있는 경우 AWS CloudFormation Organizations와의 통합을 활용하여 해당 서비스가 계정 간 역할 생성을 처리하도록 할 수 있습니다. 조직에서 자동 배포를 활성화하여 향후 대상 조직 또는 조직 구성 단위(OU)에 추가할 수 있는 새 계정에 스택 인스턴스를 자동으로 배포할 수 있습니다. 조직에서 계정을 제거하면 AWS CloudFormation 는 조직 스택 인스턴스의 일부로 배포된 모든 리소스를 자동으로 삭제합니다. 에 대한 StackSets 자세한 내용은 AWS CloudFormation 사용 AWS CloudFormation StackSets 설명서에서의 작업을 참조하십시오.

를 AWS CloudFormation StackSets 사용하여 조직의 모든 계정을 켜고 구성하고 AWS 리소스 탐색기 , 활성화된 각 지역에 색인을 만들고, 필요한 곳에 색인을 만들 수 있습니다.

> **Important**
>
> 한 리전에서 애그리게이터 인덱스를 설정하려는 경우 계정의 다른 리전에 기존 애그리게이터 인덱스가 없는지 확인해야 합니다. 애그리게이터 인덱스를 로컬 인덱스로 수준을 내린 후 다른 인덱스를 계정의 새 애그리게이터 인덱스로 승격하려면 24시간을 기다려야 합니다.

사전 조건

Resource Explorer를 사용하여 조직의 계정에 AWS CloudFormation StackSets 배포하려면 사용자 또는 조직의 관리자가 먼저 다음 단계를 수행하여 서비스 관리 권한으로 스택을 활성화해야 합니다.

1. 조직은 모든 기능을 활성화해야 합니다. 조직에서 통합 결제 기능만 활성화한 경우 서비스 관리형 권한이 있는 스택 세트를 생성할 수 없습니다.
2. AWS CloudFormation 와 조직 간의 신뢰할 수 있는 액세스를 활성화합니다. 이렇게 AWS CloudFormation 하면 조직의 관리 계정에 필요한 역할을 만들 수 있는 AWS CloudFormation 권한이 부여되며 구성원 계정은 Resource Explorer 색인과 뷰를 배포합니다.

이제 서비스 관리형 권한이 있는 스택 세트를 생성할 수 있습니다.

> **Important**
>
> 조직의 관리 계정에 스택 세트를 만들어야 합니다. AWS CloudFormation 은 지역 서비스이므로 스택 세트를 처음 생성한 지역에서만 생성한 스택 세트를 보고 관리할 수 있습니다.

Resource Explorer용 스택 세트 생성

Resource Explorer를 완전히 배포하려면 두 개의 스택 세트를 배포해야 합니다.

- 첫 번째 스택 세트는 사용자가 계정에 있는 모든 리전에 걸쳐 리소스를 검색할 수 있는 애그리게이터 인덱스와 기본 뷰를 생성합니다.

  애그리게이터 인덱스를 생성하려는 단일 리전에만 이 스택 세트를 배포합니다.
- 두 번째 스택 세트는 로컬 인덱스와 기본 뷰를 생성합니다. 로컬 인덱스는 해당 콘텐츠를 애그리게이터 인덱스에 복제합니다.

  애그리게이터 인덱스가 포함된 리전을 제외하고 계정에서 활성화된 모든 리전에 이 스택 세트를 배포합니다. 스택을 배포하는 계정에서 활성화되지 않은 리전은 선택하지 마세요. 그렇게 하면, 배포에 실패합니다.

다음 섹션에서는 각각에 대한 샘플 템플릿을 제공합니다. 이러한 템플릿을 사용하여 스택 세트를 만드는 방법에 대한 step-by-step 지침은 사용 AWS CloudFormation 설명서의 서비스 관리 권한으로 스택 세트 만들기를 참조하십시오.

이러한 스택 세트를 조직에 배포한 후에는 선택한 범위 내의 모든 계정(조직 또는 조직 단위)은 지정된 리전에는 애그리게이터 인덱스를, 다른 모든 리전에는 로컬 인덱스를 갖게 됩니다.

샘플 템플릿 AWS CloudFormation

다음 샘플 템플릿은 계정의 애그리게이터 인덱스와 인덱스를 배포한 계정에 있는 모든 리전에 걸쳐 리소스를 검색할 수 있는 기본 뷰를 생성합니다.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with an Aggregator Index, and a new Default
 View.
```

```
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with an Aggregator Index,
 and a new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
```

```
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

다음 샘플 템플릿은 애그리게이터 인덱스가 있는 계정을 제외한 모든 계정에서 활성화된 각 리전에 로컬 인덱스를 생성합니다. 또한 사용자가 해당 리전의 리소스만 검색할 수 있는 기본 뷰를 생성합니다. 사용자는 모든 리전에 걸쳐 리소스를 검색하려면 애그리게이터 리전의 뷰로 검색해야 합니다.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with a Local Index, and a new Default View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: LOCAL
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
```

```
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with a Local Index, and a
 new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "LOCAL",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

리소스 탐색기 끄기

더 이상 특정 AWS 리전지역의 리소스를 검색할 필요가 없는 경우 인덱스를 삭제하여 해당 AWS 리소스 탐색기 지역에서만 사용 중지하거나 Resource Explorer를 모두 삭제할 수 있습니다 AWS 리전. 이렇게 하면 Resource Explorer가 해당 리전에서 새 리소스 또는 업데이트된 리소스에 대한 검색을 중단합니다. 계정에 애그리게이터 인덱스가 포함된 경우 삭제된 인덱스에서의 복제가 중지되고, 삭제된 인덱스의 정보가 애그리게이터 인덱스에서 제거되고 검색 결과에 더 이상 표시되지 않습니다. 삭제된 인덱스의 모든 리소스가 애그리게이터 인덱스가 있는 리전의 검색 결과에서 사라지는 데 최대 24시간이 걸릴 수 있습니다.

> **Note**
>
> 처음 AWS 리전등록하면 리소스 탐색기는 `AWSServiceRoleForResourceExplorer` 에서 이름이 지정된 서비스 연결 역할 (SLR) 을 만듭니다 AWS 계정. 리소스 탐색기는 이를 SLR 자동으로 삭제하지 않습니다. 계정의 모든 지역에서 리소스 탐색기 색인을 삭제한 후 나중에 리소스 탐색기를 사용하지 않을 SLR 경우 IAM 콘솔을 사용하여 삭제할 수 있습니다. 역할을 삭제한 다음 최소한 한 AWS 리전번에서 리소스 탐색기를 다시 사용하도록 선택하면 리소스 탐색기가 서비스에 연결된 역할을 자동으로 다시 만듭니다.

리소스 탐색기를 한 번에 끄십시오. AWS 리전

를 사용하거나 AWS Command Line Interface (AWS CLI) 의 명령을 사용하거나 에서 API 작업을 사용하여 에서 리소스 탐색기를 끌 수 AWS SDK 있습니다. AWS 리전 AWS Management Console

한 멤버 계정에 대해 Resource Explorer를 비활성화하고 그 멤버가 조직 전체 뷰에 있는 경우 다중 계정 검색 결과에서 해당 멤버가 제거됩니다.

계정에 있는 하나 이상의 AWS 리전 에서 리소스 검색을 더 이상 지원하지 않으려면 다음 절차의 단계를 수행하세요.

> **Note**
>
> 삭제한 인덱스가 의 애그리게이터 인덱스인 경우 다른 로컬 인덱스를 계정의 애그리게이터 인덱스로 승격시키려면 24시간을 기다려야 합니다. AWS 계정사용자는 다른 애그리게이터 인덱스가 구성될 때까지 Resource Explorer를 사용하여 계정 전체 검색을 수행할 수 없습니다.

AWS Management Console

에서 리소스 탐색기 색인을 삭제하려면 AWS 리전

1. Resource Explorer 설정 페이지를 엽니다.
2. 색인 섹션에서 삭제하려는 색인이 AWS 리전 있는 옆의 확인란을 선택한 다음 삭제를 선택합니다.
3. 인덱스 삭제 페이지에서 삭제하려는 인덱스만 선택했는지 확인합니다. 확인 텍스트 상자에 **delete**을 입력한 다음 인덱스 삭제를 선택합니다.

   Resource Explorer는 페이지 상단에 녹색 배너를 표시하여 성공을 나타내거나, 선택한 리전 중 하나 이상에 오류가 있는 경우 빨간색 배너를 표시합니다.

AWS CLI

에서 리소스 탐색기 색인을 삭제하려면 AWS 리전

계정에 있는 하나 이상의 리소스 검색을 더 이상 지원하지 않으려면 다음 명령을 실행하세요. AWS 리전

삭제하려는 인덱스가 있는 각 리전에 대해 다음 명령을 실행합니다. 삭제하려는 인덱스가 있는 리전에서 명령을 실행해야 합니다. 다음 예제 명령은 미국 서부(오레곤)(us-west-2)에서 Resource Explorer 인덱스를 삭제합니다 .

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222 \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
    "State": "DELETING"
}
```

Resource Explorer는 일부 삭제 정리 작업을 백그라운드에서 비동기 작업으로 수행하므로 응답에 작업이 DELETING로 표시될 수 있습니다. 이 상태는 백그라운드 프로세스가 아직 완료되지 않았음을 나타냅니다. 다음 명령을 실행하여 State가 DELETED로 변경되는 것을 확인하여 최종 완료 여부를 확인할 수 있습니다.

```
$ aws resource-explorer-2 get-index \
```

```
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

리소스 탐색기를 모두 끕니다. AWS 리전

AWS 리소스 탐색기 완전히 끄려면 다음 절차를 수행하십시오.

> **Note**
>
> Resource Explorer는 계정에 AWS 리전 대한 첫 번째 인덱스를 만들 때 계정에 이름이 지정된 AWSServiceRoleForResourceExplorer 서비스 연결 역할을 생성합니다. Resource Explorer는 이 서비스 연결 역할을 자동으로 삭제하지 않습니다. 모든 지역에서 리소스 탐색기 색인을 삭제한 후 나중에 리소스 탐색기를 다시 사용하지 않을 것이 확실하다면 IAM 콘솔을 사용하여 역할을 삭제할 수 있습니다. 역할을 삭제한 다음 하나 AWS 리전이상에서 리소스 탐색기를 시작하도록 선택하면 리소스 탐색기가 서비스에 연결된 역할을 다시 생성합니다.

를 사용하거나, AWS Command Line Interface (AWS CLI) 의 명령을 사용하거나 AWS Management Console, 에서 API 작업을 사용하여 리소스 탐색기를 끌 수 있습니다. AWS SDK

AWS Management Console

내 어느 AWS 리전 곳에서든 리소스 검색을 더 이상 지원하지 않으려면 다음 절차의 단계를 수행하십시오. AWS 계정

리소스 탐색기를 모두 끄려면 AWS 리전

1. Resource Explorer 설정 페이지를 엽니다.
2. 색인 섹션에서 등록된 AWS 리전모든 항목 옆의 확인란을 선택한 다음 삭제를 선택합니다.

> **Tip**
>
> 인덱스 옆의 테이블 헤더 행에 있는 확인란을 선택하면 한 번에 모든 리전에 대한 확인란을 선택할 수 있습니다.

3. 인덱스 삭제 페이지에서 모든 인덱스를 삭제할 것인지 확인합니다. 확인 텍스트 상자에 **delete**을 입력한 다음 인덱스 삭제를 선택합니다.

   Resource Explorer는 페이지 상단에 녹색 배너를 표시하여 성공을 나타내거나, 선택한 리전 중 하나 이상에 오류가 있는 경우 빨간색 배너를 표시합니다.

AWS CLI

리소스 탐색기를 모두 끄려면 AWS 리전

계정의 리소스 검색을 더 이상 지원하지 않으려면 다음 명령을 실행하여 이전에 리소스 탐색기를 켠 각 ARN AWS 리전 색인의 모든 색인을 찾아보십시오. AWS 리전

```
$ aws resource-explorer-2 list-indexes --query Indexes[*].Arn[
"arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
"arn:aws:resource-explorer-2:us-west-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
"arn:aws:resource-explorer-2:us-west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd33333333"
]
```

각 응답에 대해 다음 명령을 실행하여 해당 리전의 Resource Explorer 인덱스를 삭제합니다.

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "State": "DELETING"
}
```

각 추가 리전에서 이전 명령을 반복합니다.

Resource Explorer는 일부 정리 작업을 백그라운드에서 비동기 작업으로 수행하므로 응답에 작업이 DELETING로 표시될 수 있습니다. 이 상태는 백그라운드 프로세스가 아직 완료되지 않았음을 나타냅니다. 다음 명령을 실행하여 상태가 DELETED로 변경되는 것을 확인하여 최종 완료 여부를 확인할 수 있습니다.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

검색에 대한 액세스를 제공하기 위한 Resource Explorer 뷰 관리

뷰는 리소스 검색의 핵심입니다. 모든 AWS 리소스 탐색기 검색 작업에는 뷰를 사용해야 합니다. 뷰는 관리자가 AWS 계정의 리소스에 대한 정보에 대한 액세스를 제어하는 데 사용할 수 있는 방법입니다.

뷰에는 해당 뷰를 사용할 권한이 있는 주도자 (IAM역할 또는 사용자) 만 액세스할 수 있습니다. 리소스 탐색기로 성공적으로 검색하려면 주도자가 뷰의 `resource-explorer-2:GetView` 및 `resource-explorer-2:Search` 작업에 모두 `Allow` 액세스할 수 있어야 합니다. ARN

뷰에는 관리자가 원하는 항목으로만 결과를 제한하는 데 사용할 수 있는 기본 제공 필터가 포함되어 있습니다. 예를 들어 특정 프로젝트와 관련된 리소스만 포함하는 뷰를 생성할 수 있습니다. 다른 프로젝트에 대한 정보를 볼 필요가 없는 사용자는 이 뷰를 사용하여 관심 있는 리소스만 볼 수 있습니다.

뷰는 리전 리소스입니다. 뷰는 특정 AWS 리전 에 생성되어 저장되며 해당 리전에 있는 인덱스 정보만 결과로 반환합니다. 계정에 있는 모든 리전 전반에 대한 결과를 포함하려면 뷰가 애그리게이터 인덱스가 포함된 리전에 있어야 합니다. 해당 리전에는 계정에 있는 다른 모든 리전의 인덱스 복제본이 포함되어 있습니다.

모든 뷰에는 다음과 같은 몇 가지 핵심 요소가 있습니다.

검색 권한

표준 AWS 권한 정책을 사용하여 각 뷰를 사용할 수 있는 사용자를 제어할 수 있습니다. 이는 보안 주체에게 연결된 자격 증명 기반 권한 정책을 통해 제공됩니다. 이를 통해 각 뷰에서 제공되는 정보를 볼 수 있는 사용자를 세밀하게 제어할 수 있습니다. 예를 들어, 프로덕션 서비스를 운영하는 엔지니어만 검색할 수 있도록 `Production-resources` 뷰에 대한 액세스 권한을 부여할 수 있습니다. 그런 다음 개발자가 사전 프로덕션 리소스를 검색할 수 있도록 `Pre-production-resources` 뷰에 다른 권한을 부여할 수 있습니다.

보안 주체와 이름이 지정된 AWS `AWSResourceExplorerReadOnlyAccess` 관리형 정책을 사용하면 보안 주체가 계정의 모든 뷰를 사용하여 검색할 수 있는 권한이 부여됩니다.

또는 자체 권한 정책을 생성하고 지정된 뷰에만 다음 권한을 부여할 수 있습니다.

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 다음 분야의 사용자 및 그룹: AWS IAM Identity Center

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따릅니다.

- ID 공급자를 IAM 통해 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. 사용 IAM설명서의 타사 ID 공급자 (페더레이션) 를 위한 역할 생성의 지침을 따르십시오.

- IAM사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. 사용 설명서의 IAM사용자 역할 생성에 나와 있는 지침을 따르십시오. IAM
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. 사용 설명서의 사용자 (콘솔) 에 권한 추가의 IAM 지침을 따르십시오.

뷰와 관련된 권한에 대한 자세한 내용은 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여를 참조하세요.

검색 필터링

뷰는 사용자가 계정의 리소스를 볼 수 있는 가상 창 역할을 합니다. 큰 그림을 각각 다르게 보여주는 여러 개의 뷰를 생성할 수 있습니다. 예를 들어, 리소스에 연결된 태그로 식별되는 사전 프로덕션 환경과 관련된 리소스만 검색할 수 있는 뷰를 생성할 수 있습니다. 그런 다음 태그의 다양한 값을 기반으로 프로덕션 환경의 리소스만 검색할 수 있는 별도의 뷰를 생성할 수 있습니다. 서로 다른 `FilterString` 값으로 여러 뷰를 구성하면 검색할 때마다 해당 쿼리 파라미터를 다시 입력할 필요가 없습니다.

또한 뷰는 결과에 포함할 리소스에 대한 선택적 정보를 지정할 수 있습니다. 기본 필드 목록은 항상 결과에 포함됩니다. 기본 목록 외에도 뷰에 리소스에 연결된 모든 태그 가 포함되도록 요청할 수 있습니다.

검색 범위

- 지역 범위 — 리소스 탐색기를 AWS 리전 사용하여 검색하면 해당 지역에서 색인된 리소스만 결과에 포함될 수 있습니다. 대부분의 리전에 있는 인덱스는 해당 리전 내의 리소스에 대한 정보만 포함되어 있으므로 `LOCAL`이라는 레이블이 지정됩니다. 해당 리전에서 검색하면 해당 리소스만 반환될 수 있습니다.
- 계정 범위 – 하나의 로컬 인덱스를 계정의 애그리게이터 인덱스로 승격할 수 있습니다. 이렇게 하면 Resource Explorer가 활성화되어 있는 다른 모든 리전이 해당 인덱스 정보를 애그리게이터 인덱스가 있는 리전에 복제합니다. 해당 리전에서 검색하면 해당 결과에 계정에 있는 모든 리전의

리소스가 포함됩니다. 빠른 설정 옵션을 사용하여 서버를 구성하면 Resource Explorer가 지정한 리전에 애그리게이터 인덱스를 자동으로 생성합니다. 또한 빠른 설정 옵션은 해당 리전에 기본 뷰를 생성하여 모든 리전에 걸쳐 계정의 모든 리소스를 검색할 수 있도록 지원합니다.

기본 뷰

사용자가 뷰를 명시적으로 지정하지 않고 검색을 시도하는 경우 Resource Explorer는 해당 AWS 리전에 대해 정의된 기본 뷰를 사용합니다.

해당 리전에 대한 기본 뷰가 없고 사용자가 사용할 뷰를 지정하지 않은 경우 검색이 실패하고 예외가 생성됩니다.

Resource Explorer는 다음과 같이 기본 뷰를 자동으로 생성합니다.

- 를 사용하여 리소스 탐색기를 켜고 빠른 설치 옵션을 선택하는 경우 계정의 애그리게이터 인덱스를 포함할 지역을 지정해야 합니다. AWS Management Console Resource Explorer는 지정된 애그리게이터 인덱스 리전에 기본 뷰를 자동으로 생성합니다.
- 를 사용하여 리소스 탐색기를 AWS Management Console 등록하고 고급 설정 옵션을 선택하면 선택적으로 지정된 지역의 계정에 대한 애그리게이터 인덱스를 만들도록 선택할 수 있습니다. 이렇게 하면 Resource Explorer가 자동으로 애그리게이터 인덱스 리전에 기본 뷰를 생성합니다.
- 콘솔을 사용하여 Resource Explorer를 등록하고 애그리게이터 인덱스 리전을 등록하지 않도록 선택하면 Resource Explorer가 각 리전에 있는 로컬 인덱스에 대한 기본 뷰를 생성합니다.
- AWS CLI 또는 API 작업을 사용하여 리소스 탐색기를 등록하는 경우 리소스 탐색기는 기본 보기를 자동으로 만들지 않습니다. 대신 사용자가 검색할 것으로 예상되는 각 리전의 기본 뷰를 수동으로 구성해야 합니다.

검색에 사용할 Resource Explorer 뷰 생성

모든 검색은 뷰를 사용해야 합니다. 뷰는 뷰를 사용하는 쿼리에서 반환할 수 있는 리소스를 결정하는 필터를 정의합니다. 또한 뷰는 리소스를 검색할 수 있는 사용자를 제어합니다.

뷰는 AWS 리전에 저장되며 해당 지역 색인의 검색 결과만 반환합니다. 리전에 애그리게이터 인덱스가 포함된 경우 뷰는 계정에 있는 모든 리전에 있는 인덱스로부터 검색 결과를 반환합니다.

다중 계정 뷰를 사용하면 조직 전반에 걸쳐 계정에 있는 리소스를 검색할 수 있습니다. 검색하려는 모든 계정에는 인덱스가 필요합니다. 조직의 관리 계정이나 위임된 관리자 계정만 다중 계정 뷰를 생성할 수 있습니다.

AWS 리소스 탐색기 Systems Manager 콘솔의 리소스 탐색기 빠른 설치 또는 고급 설치에서 관련 옵션을 선택한 경우 초기 설정 중에 기본 보기를 생성할 수 있습니다. 나중에 언제든지 사용자 집합별로 다른 필터를 사용하는 추가 뷰를 생성할 수 있습니다.

를 사용하거나 에서 AWS CLI 명령 AWS Management Console 또는 이에 상응하는 API 작업을 실행하여 보기를 만들 수 AWS SDK 있습니다.

최소 권한

이 절차를 실행하려면 다음 권한이 있어야 합니다.

- 작업: `resource-explorer-2:CreateView`

  리소스: 계정 내 어느 AWS 리전 곳에서든 뷰를 만들 수 있도록 * 하기 위한 것일 수 있습니다.

AWS Management Console

뷰를 생성하려면

1. Resource Explorer 콘솔 뷰 페이지를 열고 뷰 생성을 선택합니다.
2. 뷰 생성 페이지에서 이름 뷰의 이름을 입력합니다.

   이름은 64자를 넘지 않아야 하며 문자, 숫자, 하이픈(-) 문자를 포함할 수 있습니다. 이름은 해당 이름 내에서 고유해야 합니다 AWS 리전.
3. 뷰를 만들려는 이름을 선택합니다. AWS 리전 계정 내 모든 지역의 리소스를 반환하는 뷰를 만들려면 애그리게이터 인덱스가 AWS 리전 포함된 뷰를 선택하세요.
4. (선택 사항) 범위에서 검색 시 다중 계정 리소스를 반환할지 아니면 계정의 리소스만 반환할지를 선택합니다. 기본값은 계정 수준 범위입니다.

   관리 계정 또는 위임된 관리자만 다중 계정 뷰를 생성하는 옵션을 볼 수 있습니다.
5. 결과를 필터링할지 여부를 선택합니다.

   - 모든 리소스 포함

     쿼리 필터는 포함되어 있지 않습니다. 뷰와 연결된 인덱스의 모든 리소스가 검색 결과에 반환될 수 있습니다.
   - 지정된 필터와 일치하는 리소스만 포함

     필터 이름과 연산자를 선택할 수 있는 리소스 필터 확인란을 활성화합니다. 사용 가능한 각 필터 이름 및 연산자에 대한 설명은 필터를 참조하세요.

- 이 뷰의 결과에 포함할 선택적 리소스 속성을 선택합니다. 사용자가 태그 키 이름과 값을 기준으로 리소스를 검색할 수 있도록 하려면 태그 옆의 확인란을 선택합니다. 뷰에 태그를 포함하지 않으면 사용자가 태그 키와 값을 사용하여 결과를 추가로 필터링하는 검색 요청을 할 수 없습니다.
- 필요에 따라 뷰에 태그를 연결할 수 있습니다. 태그 상자를 확장하고 최대 50개의 태그 키/값 쌍을 입력합니다. 태그를 사용하여 리소스를 분류하거나 속성 기반 액세스 제어 () ABAC 보안 권한 전략의 일부로 사용할 수 있습니다. 자세한 내용은 뷰에 태그 추가 단원을 참조하십시오.
- 뷰 생성을 선택합니다.

콘솔은 새로운 뷰를 사용하여 검색을 수행할 수 있는 검색 페이지로 돌아갑니다.

다음 단계: 계정의 보안 주체에게 새로운 뷰로 검색할 수 있는 권한을 부여합니다. 자세한 내용은 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여 단원을 참조하세요.

AWS CLI

뷰를 생성하려면

지정된 AWS 리전에 뷰를 생성하려면 다음 명령을 실행합니다. 다음 예제는 Amazon EC2 서비스와 관련된 리소스 중 `Stage` 키와 값이 `prod` 태그가 지정된 리소스만 반환하는 뷰를 생성합니다.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name "My-EC2-Prod-Resources" \
    --filters FilterString="service:ec2 tag:stage=prod" \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": "service:ec2 tag:stage=prod"
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
```

```
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:123456789012:view/My-EC2-
Prod-Resources/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

조직 수준 뷰를 생성하려면

다음 예제에서는 조직 전반에 걸쳐 리소스를 반환하는 뷰를 생성합니다. 이는 조직의 관리 계정 또는 위임된 관리자 계정으로 수행해야 합니다.

1. aws organizations describe-organization명령을 실행하여 조직을 ARN 가져오십시오.
2. 다음 명령을 실행하여 지정된 조직에 대한 뷰를 생성합니다.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-org-view \
    --scope "arn:aws:organizations::111111111111:organization/o-exampleorgid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "111111111111",
        "Scope": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:111111111111:view/
entire-org-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

조직 단위 수준 뷰를 생성하려면

다음 예제에서는 이 조직 단위의 모든 멤버의 리소스를 반환하는 뷰를 생성합니다. 이 뷰는 조직 수준 뷰와 유사하게 작동합니다. 이는 조직의 관리 계정 또는 위임된 관리자 계정으로 수행해야 합니다.

1. aws organizations describe-organizational-unit명령을 실행하여 조직을 가져오세요ARN.

2. 다음 명령을 실행하여 지정된 조직 단위에 대한 뷰를 생성합니다.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-ou-view \
    --scope "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "222222222222",
        "Scope": "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:222222222222:view/
entire-ou-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

다음 단계: 계정의 보안 주체에게 새로운 뷰로 검색할 수 있는 권한을 부여합니다. 자세한 내용은 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여 섹션을 참조하세요.

검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여

사용자가 새로운 뷰로 검색할 수 있으려면 먼저 AWS 리소스 탐색기 뷰에 대한 액세스 권한을 부여해야 합니다. 이렇게 하려면 뷰로 검색해야 하는 AWS Identity and Access Management(IAM) 보안 주체에 대해 자격 증명 기반 권한 정책을 사용하세요.

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 사용자(콘솔)에 권한 추가의 지침을 따르세요.

다음 방법 중 하나를 사용할 수 있습니다.

- 기존 AWS 관리형 정책을 사용합니다. Resource Explorer는 사용자가 사용할 수 있도록 미리 정의된 여러 AWS 관리형 정책을 제공합니다. 사용 가능한 모든 AWS 관리형 정책에 대한 자세한 내용은 AWS 에 대한 관리형 정책 AWS 리소스 탐색기를 참조하세요.

  예를 들어 `AWSResourceExplorerReadOnlyAccess` 정책을 사용하여 계정의 모든 뷰에 검색 권한을 부여할 수 있습니다.
- 권한 정책을 직접 생성하여 보안 주체에게 할당합니다. 정책을 직접 생성하는 경우 정책 문의 `Resource` 요소에 각 뷰의 Amazon 리소스 이름(ARN)을 지정하여 단일 뷰 또는 사용 가능한 뷰의 하위 집합에 대한 액세스를 제한할 수 있습니다. 예를 들어, 다음 예제 정책을 사용하여 보안 주체에게 해당 뷰 하나만 사용하여 검색할 수 있는 권한을 부여할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyTestView/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
        }
    ]
}
```

  IAM 콘솔을 사용하여 권한 정책을 생성하고 해당 권한이 필요한 보안 주체와 함께 사용할 수 있습니다. IAM 권한에 대한 자세한 내용은 다음 항목을 참조하세요.

- IAM의 정책 및 권한
- IAM 자격 증명 권한 추가 및 제거
- 정책에 의해 부여된 권한 이해

태그 기반 권한 부여를 사용하여 뷰에 대한 액세스 제어

특정 리소스만 포함된 결과를 반환하는 필터를 사용하여 여러 뷰를 생성하려는 경우 해당 리소스를 확인해야 하는 보안 주체만 해당 뷰에 액세스할 수 있도록 제한할 수도 있습니다. ABAC(속성 기반 액세스 제어) 전략을 사용하여 계정의 뷰에 이러한 유형의 보안을 제공할 수 있습니다. ABAC에서 사용하는 속성은 AWS에서 작업을 시도하려는 보안 주체와 액세스하려는 리소스 모두에 연결된 태그입니다.

ABAC는 보안 주체에 연결된 표준 IAM 권한 정책을 사용합니다. 정책은 정책 문의 `Condition` 요소를 사용하여 요청 보안 주체에 연결된 태그와 영향을 받는 리소스에 연결된 태그가 모두 정책의 요구 사항과 일치하는 경우에만 액세스를 허용합니다.

예를 들어 회사의 프로덕션 애플리케이션을 지원하는 모든 AWS 리소스에 태그 `"Environment" = "Production"`를 추가할 수 있습니다. 프로덕션 환경에 액세스할 권한이 있는 보안 주체만 해당 리소스를 볼 수 있도록 하려면 해당 태그를 필터로 사용하는 Resource Explorer 뷰를 생성합니다. 그런 다음 뷰에 대한 액세스를 적절한 주체로만 제한하려면 다음 예제 요소와 비슷한 조건을 가진 정책을 사용하여 권한을 부여합니다.

```
{
    "Effect": "Allow",
    "Action": [ "service:Action1", "service:Action2" ],
    "Resource": "arn:aws:arn-of-a-resource",
    "Condition": { "StringEquals": {"aws:ResourceTag/Environment":
 "${aws:PrincipalTag/Environment}"} }
}
```

이전 예제의 `Condition`은 요청을 하는 보안 주체에 연결된 `Environment` 태그가 요청에 지정된 리소스에 연결된 `Environment` 태그와 일치하는 경우에만 요청을 허용하도록 지정했습니다. 이 두 태그가 정확히 일치하지 않거나 태그 중 하나가 누락된 경우 Resource Explorer는 요청을 거부합니다.

> **Important**
>
> ABAC를 사용하여 리소스에 대한 액세스를 보호하려면 먼저 보안 주체 및 리소스에 연결된 태그를 추가하거나 수정할 수 있는 기능에 대한 액세스를 제한해야 합니다. 사용자가 AWS 보안 주체 또는 리소스에 연결된 태그를 추가하거나 수정할 수 있는 경우 해당 사용자는 해당 태그

로 제어되는 권한에 영향을 미칠 수 있습니다. 안전한 ABAC 환경에서는 승인된 보안 관리자만 주체에 연결된 태그를 추가하거나 수정할 수 있는 권한을 가지며, 보안 관리자와 리소스 소유자만 리소스에 연결된 태그를 추가하거나 수정할 수 있습니다.

ABAC 전략을 성공적으로 구현하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 다음 주제를 참조하세요.

- IAM 자습서: 태그를 기반으로 AWS 리소스에 액세스할 수 있는 권한 정의
- 태그를 사용한 AWS 리소스 액세스 제어

필요한 ABAC 인프라를 마련한 후에는 태그 사용 시작을 사용하여 계정에서 Resource Explorer 뷰를 사용하여 검색할 수 있는 사용자를 제어할 수 있습니다. 원칙을 설명하는 정책의 예제를 보려면 다음 권한 정책 예를 참조하세요.

- 태그를 기반으로 뷰에 액세스 권한 부여
- 태그를 기반으로 뷰를 생성할 수 있는 액세스 권한 부여

AWS 리전에서 기본 뷰 설정

AWS 리소스 탐색기에서는 AWS 리전에서 여러 뷰를 정의할 수 있으며, 각 뷰는 서로 다른 검색 요구 사항을 처리합니다. 각 리전에 하나의 뷰를 해당 리전의 기본 뷰로 설정하는 것이 좋습니다.

Resource Explorer는 사용자가 검색을 수행할 때마다 기본 뷰를 사용하며 사용할 뷰를 명시적으로 지정하지 않습니다. 모든 AWS Management Console 페이지 상단의 통합 검색 창은 애그리게이터 인덱스가 포함된 리전의 기본 뷰를 자동으로 사용하여 사용자의 검색 쿼리와 일치하는 리소스를 찾습니다.

해당 리전에 있는 뷰만 해당 리전의 기본 뷰로 선택할 수 있습니다. 사용하려는 뷰가 다른 리전에 있는 경우 먼저 기본 뷰로 설정하려는 리전에서 해당 뷰의 복사본을 생성해야 합니다.

> **Tip**
>
> 뷰 복사 작업이 없습니다. 대상 리전에서 뷰를 생성한 다음 기존 뷰의 설정을 새로운 뷰로 복사해야 합니다.

AWS Management Console을 사용하거나 AWS SDK에서 AWS CLI 명령 또는 동등한 API 작업을 실행하여 뷰를 해당 리전의 기본 뷰로 지정할 수 있습니다.

AWS Management Console

기본 뷰를 설정하려면

1. Resource Explorer 뷰 페이지에서 해당 리전에 대해 기본값으로 설정하려는 뷰 옆의 옵션 버튼을 선택합니다.
2. 작업을 선택한 다음 기본으로 설정을 선택합니다.

AWS CLI

기본 뷰를 설정하려면

다음 명령을 실행하여 지정된 뷰를 해당 리전의 기본값으로 설정합니다. 다음 예제에서는 지정된 뷰를 us-east-1 리전에서 수행되는 모든 검색에 대한 기본값으로 설정합니다. 해당 뷰는 명령을 실행하는 리전에 있어야 합니다.

```
$ aws resource-explorer-2 associate-default-view \
    --region us-east-1 \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

뷰에 태그 추가

뷰에 태그를 추가하여 분류할 수 있습니다. 태그는 키 이름 문자열 및 연결된 선택적 값 문자열의 형태를 취하는 고객 제공 메타데이터입니다. AWS 리소스 태그 지정에 대한 자세한 내용은 Amazon Web Services 일반 참조의 AWS 리소스 태그 지정 단원을 참조하세요.

뷰에 태그 추가

AWS Management Console을 사용하거나 AWS SDK에서 AWS CLI 명령 또는 동등한 API 작업을 실행하여 Resource Explorer 뷰에 태그를 추가할 수 있습니다.

AWS Management Console

뷰에 태그를 추가하려면

1. Resource Explorer 뷰 페이지를 열고 태그를 지정하려는 뷰의 이름을 선택하여 해당 세부 정보 페이지를 표시합니다.
2. 태그에서 태그 관리를 선택합니다.
3. 태그를 추가하려면 태그 추가를 선택한 다음 해당 태그 키 이름과 값을 입력합니다.

> **Note**
>
> 태그 옆의 X를 선택하여 태그를 삭제할 수도 있습니다.

최대 50개의 사용자 정의 태그를 리소스에 연결할 수 있습니다. AWS에서 자동으로 생성하고 관리하는 모든 태그는 이 할당량에 포함되지 않습니다.

4. 모든 태그 변경 작업을 마치면 변경 사항 저장을 선택합니다.

AWS CLI

뷰에 태그를 추가하려면

다음 명령을 실행하여 뷰에 태그를 추가합니다. 다음 예제에서는 키 이름 `environment` 및 값 `production`가 있는 태그를 지정된 뷰에 추가합니다.

```
$ aws resource-explorer-2 tag-resource \
    --resource-id arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --tags environment=production
```

성공 시 이전 명령은 출력을 생성하지 않습니다.

> **Note**
>
> 뷰에서 기존 태그를 제거하려면 `untag-resource` 명령을 사용합니다.

태그로 권한 제어

태그 지정의 주요 용도 중 하나는 ABAC(속성 기반 액세스 제어) 전략을 지원하는 것입니다. ABAC를 사용하면 리소스에 태그를 지정할 수 있어 권한 관리를 간소화할 수 있습니다. 그런 다음 사용자에게 특정 방식으로 태그가 지정된 리소스에 대한 권한을 부여합니다.

예를 들어 다음 시나리오를 살펴보세요. `ViewA`이라는 뷰의 경우 태그 `environment=prod`(키 이름=값)를 연결합니다. 또 다른 `ViewB`에는 `environment=beta` 태그가 지정될 수 있습니다. 각 역할 또는 사용자가 액세스할 수 있어야 하는 환경에 따라 역할과 동일한 태그와 값으로 역할과 사용자에게 태그를 지정합니다.

그런 다음 IAM 역할, 그룹 및 사용자에게 AWS Identity and Access Management(IAM) 권한 정책을 할당할 수 있습니다. 정책은 검색을 요청하는 역할 또는 사용자가 뷰에 연결된 `environment` 태그와 동일한 값을 가진 `environment` 태그를 가지고 있는 경우에만 뷰를 사용하여 액세스하고 검색할 수 있는 권한을 부여합니다.

이 접근 방식의 이점은 동적이며 누가 어떤 리소스에 액세스할 수 있는지 목록을 관리할 필요가 없다는 것입니다. 대신 모든 리소스(뷰)와 보안 주체(IAM 역할 및 사용자)에 적절한 태그를 지정해야 합니다. 그러면 정책을 변경할 필요 없이 권한이 자동으로 업데이트됩니다.

ABAC 정책에서 태그 참조

뷰에 태그를 지정한 후 해당 태그를 사용하여 해당 뷰에 대한 액세스를 동적으로 제어하도록 선택할 수 있습니다. 다음 예제 정책에서는 IAM 보안 주체와 뷰 모두에 태그 키 `environment`와 일부 값으로 태그가 지정되어 있다고 가정합니다. 완료되면 다음 예제 정책을 보안 주체에 연결할 수 있습니다. 그러면 역할과 사용자는 보안 주체에 연결된 `environment` 태그와 정확히 일치하는 `environment` 태그 값으로 태그가 지정된 모든 뷰를 사용하여 `Search`할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
```

```
                    "aws:ResourceTag/environment": "${aws:PrincipalTag/environment}"
                }
            }
        }
    ]
}
```

보안 주체와 뷰 모두에 environment 태그가 있지만 값이 일치하지 않거나 둘 중 하나에 environment 태그가 없는 경우 Resource Explorer는 검색 요청을 거부합니다.

ABAC를 사용하여 리소스에 대한 액세스 권한을 안전하게 부여하는 방법에 대한 자세한 내용은 AWS 용 ABAC란 무엇인가요?를 참조하세요.

Resource Explorer 뷰 공유

의 보기는 AWS 리소스 탐색기 주로 리소스 기반 정책을 사용하여 액세스 권한을 부여합니다. Amazon S3 버킷 정책과 마찬가지로 이러한 정책은 뷰에 연결되며 뷰를 사용할 수 있는 사용자를 지정합니다. 이는 (IAM) 자격 증명 기반 정책과는 대조적 AWS Identity and Access Management 입니다. IAM 자격 증명 기반 정책은 역할, 그룹 또는 사용자에게 할당되며 역할, 그룹 또는 사용자가 액세스할 수 있는 작업 및 리소스를 지정합니다. Resource Explorer 뷰에서는 다음과 같이 두 가지 유형의 정책을 사용할 수 있습니다.

- 리소스를 소유한 관리 계정 또는 위임된 관리자 계정 내에서 해당 보안 주체에 대한 액세스를 명시적으로 거부하는 다른 정책이 없는 경우 두 정책 유형 중 하나를 사용하여 액세스 권한을 부여합니다.
- 계정 전반에 걸쳐 두 정책 유형을 모두 사용해야 합니다. 공유 계정의 뷰에 연결된 리소스 기반 정책은 다른 소비 계정과의 공유를 활성화합니다. 하지만 해당 정책은 소비 계정의 개별 사용자 또는 역할에 액세스 권한을 부여하지 않습니다. 또한 소비 계정의 관리자는 소비 계정의 원하는 역할과 사용자에게 자격 증명 기반 정책을 할당해야 합니다. 이 정책은 보기의 Amazon 리소스 이름(ARN)에 대한 액세스 권한을 부여합니다.

다른 계정과 뷰를 공유하려면 AWS Resource Access Manager (AWS RAM. AWS RAM hands of resource-based policies for you를 사용해야 합니다. 공유하기 전에 다음 작업을 수행해야 합니다.

- 다중 계정 검색 을 켭니다.
- 뷰를 공유 및 공유 해제하는 데 사용하는 리소스 기반 정책 또는 IAM 자격 증명 기반 정책에 및 resource-explorer-2:GetResourcePolicy resource-explorer-2:PutResourcePolicy resource-explorer-2:DeleteResourcePolicy 권한이 포함되어 있는지 확인합니다.

뷰를 공유하려면 조직의 관리 계정 또는 위임된 관리자여야 합니다. 리소스를 공유할 계정 또는 자격 증명을 지정합니다. 는 Resource Explorer 뷰를 AWS RAM 완벽하게 지원합니다. 는 공유하기로 선택한 보안 주체의 유형에 따라 다음 섹션에 설명된 것과 유사한 정책을 AWS RAM 사용합니다. 리소스 공유 방법에 대한 지침은AWS Resource Access Manager 사용 설명서의 AWS 리소스 공유를 참조하세요.

관리자와 위임된 관리자는 조직 범위 뷰, OU(조직 단위) 범위 뷰, 계정 수준 범위 뷰 등 3가지 유형의 뷰를 생성하고 공유할 수 있습니다. 조직, OUs또는 계정과 공유할 수 있습니다. 계정이 조직에 가입하거나 조직을 떠날 때 는 공유 뷰를 AWS RAM 자동으로 부여하거나 취소합니다.

AWS 계정와 뷰를 공유하기 위한 권한 정책

다음 예제 정책은 두 가지 다른 의 보안 주체가 뷰를 사용할 수 있도록 하는 방법을 보여줍니다 AWS 계정.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [ "111122223333", "444455556666" ]
            },
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            ],
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Condition": {"StringEquals": {"aws:PrincipalOrgID": "o-123456789012"},
                "StringNotEquals": {"aws:PrincipalAccount": "123456789012"}
            }
        }
    ]
    }"
}
```

지정된 각 계정의 관리자는 이제 역할, 그룹 및 사용자에 자격 증명 기반 권한 정책을 연결하여 뷰에 액세스할 수 있는 역할과 사용자를 지정해야 합니다. 계정 111122223333 또는 444455556666의 관리자는 다음과 같은 예제 정책을 생성할 수 있습니다. 그런 다음 원래 계정에서 공유된 뷰를 사용하여 검색할 수 있는 해당 계정의 역할, 그룹 및 사용자에게 정책을 할당할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    ]
}
```

이러한 IAM 자격 증명 기반 정책을 속성 기반 액세스 제어(ABAC) 보안 전략의 일부로 사용할 수 있습니다. 해당 패러다임에서는 모든 리소스와 모든 자격 증명에 태그가 지정되도록 해야 합니다. 그런 다음 액세스를 허용하려면 자격 증명과 리소스 간에 일치해야 하는 태그 키와 값을 정책에 지정합니다. 계정의 뷰에 태그를 지정하는 방법에 대한 자세한 내용은 뷰에 태그 추가를 참조하세요. 속성 기반 액세스 제어에 대한 자세한 내용은 IAM 사용 설명서의 태그 를 사용하여 리소스에 ABAC 대한 액세스 제어 AWS및 의 정의 섹션을 참조하세요. AWS

Resource Explorer에서 뷰 삭제

AWS 리소스 탐색기 뷰를 더 이상 사용할 필요가 없는 경우 삭제할 수 있습니다. AWS Management Console을 사용하거나 AWS SDK에서 AWS CLI 명령 또는 동등한 API 작업을 실행하여 뷰를 삭제할 수 있습니다.

> **Note**
>
> 현재 AWS 리전의 기본 뷰로 지정된 뷰는 삭제할 수 없습니다. 뷰를 삭제하려면 뷰를 기본값에서 제거해야 합니다. 이렇게 하려면 해당 리전에서 DisassociateDefaultView API 작업을 실행할 수 있습니다.

최소 권한

이 절차를 실행하려면 다음 권한이 있어야 합니다.

- 작업: `resource-explorer-2:DeleteView`

리소스: 삭제하려는 뷰의 ARN

AWS Management Console

뷰를 삭제하려면

1. Resource Explorer 콘솔 뷰 페이지에서 삭제하려는 뷰 옆의 옵션 버튼을 선택합니다.
2. 작업을 선택한 후 삭제를 선택합니다.
3. 확인 대화 상자에서 뷰 이름을 입력한 다음 삭제를 선택합니다.

AWS CLI

뷰를 삭제하려면

다음 명령을 실행하여 지정된 Amazon 리소스 이름(ARN)을 가진 뷰를 삭제합니다.

```
$ aws resource-explorer-2 delete-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

리소스 검색에 AWS 리소스 탐색기 사용

AWS 계정에서 AWS 리소스 탐색기을 활성화하는 주요 목적은 사용자가 계정에서 리소스를 검색할 수 있도록 하는 것입니다. Resource Explorer를 사용하여 리소스를 검색하려면 AWS Management Console 또는 AWS Command Line Interface(AWS CLI)을 사용하세요.

다음은 Resource Explorer 검색의 주요 특징 중 일부입니다.

- 모든 검색은 뷰를 사용해야 합니다.

  뷰는 Resource Explorer가 리소스를 확인할 수 있는 권한을 가진 사용자를 결정하는 데 사용되는 것입니다. Resource Explorer 검색 작업에서 뷰를 사용하려면 사용자는 지정된 뷰에 대해 `resource-explorer-2:Search` 작업에 `Allow`이 있어야 합니다. 이 권한은 요청하는 보안 주체에게 연결된 자격 증명 기반 권한 정책에서 비롯됩니다.

  뷰에는 결과에 포함할 수 있는 리소스를 제한하는 필터가 포함될 수 있습니다. 필터를 사용하는 다양한 뷰를 생성하고 여러 보안 주체에게 서로 다른 뷰에 대한 액세스 권한을 부여함으로써 각 사용자 그룹이 자신과 관련된 리소스만 볼 수 있는 환경을 구성할 수 있습니다.

  뷰에 대한 자세한 내용은 검색에 대한 액세스를 제공하기 위한 Resource Explorer 뷰 관리를 참조하세요.

- Resource Explorer는 비동기 백그라운드 프로세스를 사용하여 인덱스를 유지 관리합니다.

  Resource Explorer의 인덱싱 프로세스가 새로 생성되거나 수정된 리소스를 검색하여 로컬 인덱스에 추가하는 데에는 다소 시간이 걸릴 수 있습니다. Resource Explorer가 로컬 인덱스의 변경 내용을 애그리게이터 인덱스에 복제하는 데 시간이 더 걸릴 수 있습니다.

  삭제하는 리소스도 마찬가지입니다. 리소스를 삭제한 후 인덱싱 프로세스에서 해당 삭제 항목이 검색되고 해당 리소스의 정보가 로컬 인덱스에서 제거되기까지 다소 시간이 걸릴 수 있습니다. Resource Explorer가 로컬 인덱스에서 해당 삭제를 계정의 애그리게이터 인덱스로 복제하려면 추가 시간이 필요합니다.

  리소스에 대한 추가, 수정 및 삭제는 Resource Explorer가 Resource Explorer를 활성화한 모든 리전의 검색 결과에 해당 변경 내용을 표시하는 데 최대 36시간이 걸릴 수 있습니다.

- Resource Explorer의 검색은 AWS 리전 내에서 이루어집니다.

  Resource Explorer를 활성화하는 각 리전에는 해당 리전에 저장된 리소스의 인덱스만 포함됩니다. 뷰는 리전과도 연결되며 해당 리전의 인덱스에 있는 리소스만 반환할 수 있습니다. 이에 대한 한 가

지 예외는 애그리게이터 인덱스로, 계정에 있는 모든 리전에 걸쳐 검색을 지원하기 위해 모든 로컬 인덱스의 복제본을 수신합니다.

- 교차 리전 검색에는 계정의 애그리게이터 인덱스가 필요합니다.

  사용자가 모든 AWS 리전에 걸쳐 리소스를 검색할 수 있도록 하려면 관리자는 계정의 애그리게이터 인덱스를 포함할 하나의 리전을 지정해야 합니다. 모든 로컬 인덱스의 복제본이 자동으로 애그리게이터 인덱스에 복제됩니다.

  이로 인해 어그리게이터 인덱스 리전의 뷰만 계정에 있는 모든 AWS 리전의 리소스를 포함하는 결과를 반환할 수 있습니다.

- 쿼리는 임의의 수의 자유 형식 텍스트 키워드와 필터로 구성됩니다.

  자유 형식 키워드는 논리 **OR** 연산자를 사용하여 쿼리에 결합됩니다. Resource Explorer에서 정의한 필터 이름을 사용하는 필터는 논리 **AND**연산자를 사용하여 쿼리에 결합됩니다. 다음 예제 쿼리를 살펴보세요.

  ```
  test instance service:EC2 region:us-west-2
  ```

  Resource Explorer는 이를 다음과 같이 평가합니다.

  ```
  test OR instance AND service:EC2 AND region:us-west-2
  ```

  이 쿼리를 사용하려면 일치하는 리소스가 미국 서부(오레곤) 리전의 Amazon EC2 리소스여야 하고 이름, 설명 또는 태그 등 어떤 방식으로든 키워드(테스트, 인스턴스) 중 하나 이상이 연결되어 있어야 합니다.

  > **Note**
  >
  > 암시적 AND로 인해 리소스와 연결된 값을 하나만 가질 수 있는 속성에 대해 하나의 필터만 사용할 수 있습니다. 예를 들어, 리소스는 하나의 AWS 리전에만 속할 수 있습니다. 따라서 다음 쿼리는 결과를 반환하지 않습니다.
  >
  > ```
  > region:us-east-1 region:us-west-1
  > ```
  >
  > 이 제한은 동시에 여러 값을 가질 수 있는 속성(예: `tag:`, `tag.key:`, `tag.value:`)의 필터에는 적용되지 않습니다.

- 검색은 처음 1,000개의 결과만 반환할 수 있습니다.

이 요구 사항에는 모든 리소스와 일치하는 빈 쿼리 문자열을 사용한 검색이 포함됩니다. 빈 쿼리 문자열에서 반환되는 1,000개 이상의 리소스를 보려면 쿼리를 사용하여 일치하는 결과를 보려는 결과로 제한하고 일치 항목 수를 1,000개 미만으로 제한해야 합니다.

- 수행할 수 있는 검색 작업 수에는 계정당 할당량이 있습니다.

  할당량은 초당 만들 수 있는 쿼리 수와 매월 만들 수 있는 쿼리 수를 제한합니다. 구체적인 할당량 수는 Resource Explorer 할당량를 참조하세요.

AWS Management Console

Resource Explorer를 사용하여 리소스를 검색하려면

1. 리소스 검색 페이지에서 사용하려는 뷰를 선택하는 것으로 시작합니다. 액세스 권한이 있는 뷰 중에서만 선택할 수 있습니다.
2. 쿼리에 확인하려는 리소스를 식별하는 검색어와 필터를 입력합니다. 사용 가능한 모든 구문 옵션에 대한 자세한 내용은 Resource Explorer에 대한 검색 쿼리 구문 참조를 참조하세요.
3. Enter 키를 눌러 쿼리를 제출합니다.

   Resource Explorer는 뷰에 정의된 `Filter`와 사용자가 제공하는 쿼리 모두와 일치하는 모든 결과를 표시합니다. 결과는 관련성을 기준으로 정렬되며, 쿼리 용어와 더 많이 일치하는 리소스는 목록의 위쪽에 표시되고 더 적은 용어와 일치하는 리소스는 목록 아래쪽에 표시됩니다.
4. 리소스 식별자를 선택하면 해당 리소스 유형의 기본 콘솔로 이동합니다. 여기에서 해당 서비스가 지원하는 모든 방식으로 리소스와 상호 작용할 수 있습니다.

AWS CLI

Resource Explorer를 사용하여 리소스를 검색하려면

지정된 뷰를 사용하여 리소스를 검색하려면 다음 명령을 실행합니다. 해당 뷰는 작업을 실행하는 리전에 있어야 합니다. 다음 예제에서는 미국 동부(오하이오)(us-east-2)에서 `env=production` 태그가 지정된 Amazon EC2 인스턴스를 검색합니다. `query-string` 파라미터에 사용 가능한 모든 구문 옵션에 대한 자세한 내용은 Resource Explorer에 대한 검색 쿼리 구문 참조를 참조하세요.

```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
```

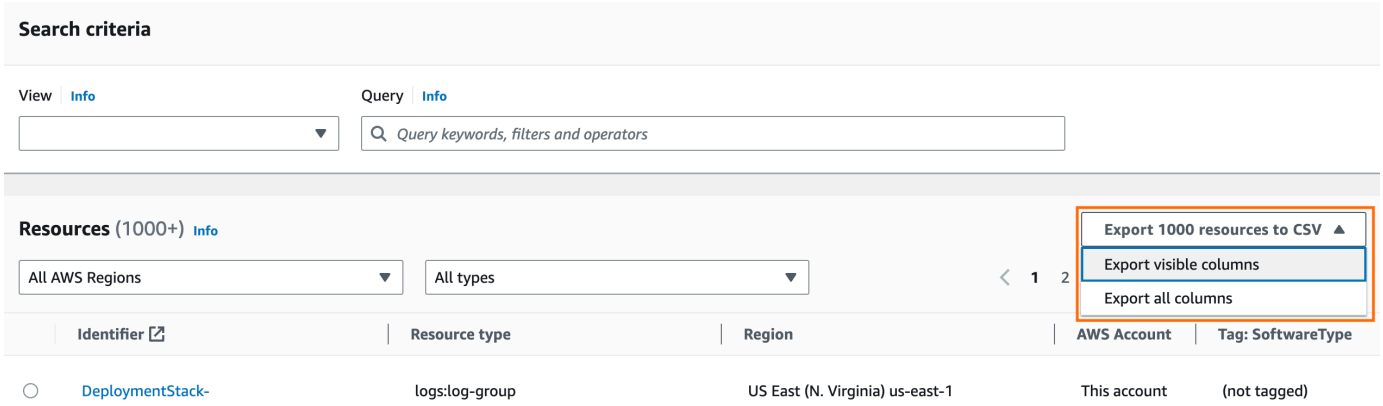
```
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

검색 결과를.csv 파일로 내보내기

리소스 검색 쿼리의 결과를 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. .csv 파일에는 식별자, 리소스 유형, 리전, AWS 계정, 총 태그 수 및 컬렉션의 각 고유 태그 키에 대한 열이 포함됩니다. .csv 파일을 사용하면 조직에서 AWS 리소스를 구성하거나 리소스 전반에 걸쳐 태그 지정 시 중복되거나 불일치가 있는 부분을 확인할 수 있습니다.

1. 리소스 검색 쿼리 결과에서 리소스를 CSV로 내보내기를 선택합니다.

   현재 볼 수 있는 열만 포함해서 결과를 내보내거나, 사용 가능한 열을 모두 포함해서 내보내도록 선택할 수 있습니다.



2. 브라우저에서 메시지가 표시되면 .csv 파일을 열기로 선택하거나 파일을 편리한 위치에 저장하기로 선택합니다.

Resource Explorer로 검색할 수 있는 리소스 유형

Resource Explorer는 다양한 AWS 서비스에서 리소스 유형을 지원합니다.

주제

일부 리소스 유형은 다른 리소스 유형과 공통 형식을 공유하는 Amazon 리소스 이름(ARN) 문자열로 식별됩니다. 이러한 일이 발생하면 Resource Explorer는 다른 리소스 유형과 같은 리소스를 보고할 수 있습니다. 이 문제의 영향을 받는 리소스 유형 목록은 다른 유형으로 나타나는 리소스 유형를 참조하세요.

현재 역할 또는 사용자와 같이 AWS Identity and Access Management (IAM) 리소스에 연결된 태그는 검색에 사용할 수 없습니다.

일부 리소스에 대해 암호화된 액세스 권한이 있는 경우 Resource Explorer에서 해당 리소스를 검색할 수 없습니다. 검색 결과에 이러한 리소스가 표시되지 않습니다.

다음 표에는 AWS 리소스 탐색기검색에 지원되는 리소스 유형이 나열되어 있습니다.

> **Note**
>
> 2024년 7월 9일부터 Resource Explorer는 더 이상 다음 리소스 유형을 지원하지 않습니다.
>
> - Amazon Elastic Container Service — `ecs:task`
> - AWS Systems Manager — `ssm:automation-execution`
> - AWS Systems Manager — `ssm:patchbaseline`
>
> 이러한 리소스 유형은 자체 서비스에서 계속 사용할 수 있지만 Resource Explorer에서는 더 이상 인덱싱되거나 검색할 수 없습니다.

지원되는 서비스 및 리소스 유형

지원됨 AWS 서비스

- Amazon API Gateway
- AWS App Runner
- Amazon AppStream 2.0
- AWS AppSync
- Amazon Athena
- AWS Backup
- AWS Batch
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Evidently
- Amazon CloudWatch Logs
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru Profiler
- AWS CodePipeline
- AWS CodeConnections
- Amazon Cognito
- Amazon Connect
- Amazon Q Connect
- Amazon Detective
- Amazon DynamoDB
- EC2 이미지 빌더
- Amazon ECR 퍼블릭
- AWS Elastic Beanstalk

- Amazon ElastiCache
- Amazon Elastic Compute Cloud(AmazonEC2)
- Amazon Elastic 컨테이너 레지스트리
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- AWS Elemental MediaPackage
- AWS Elemental MediaTailor
- Amazon EMR Serverless
- Amazon EventBridge
- AWS Fault Injection Service
- Amazon Forecast
- Amazon Fraud Detector
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Identity and Access Management
- Amazon Interactive Video Service
- AWS IoT
- AWS IoT Analytics
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- Amazon Kinesis
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda

- Amazon Lex
- Amazon Location Service
- Amazon Lookout for Metrics
- Amazon Lookout for Vision
- Amazon Managed Service for Apache Flink
- Amazon Managed Service for Prometheus
- Amazon Managed Service for Prometheus
- Amazon Managed Streaming for Apache Kafka
- AWS Migration Hub Refactor Spaces
- AWS Network Firewall
- AWS Network Manager
- Amazon OpenSearch Service
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service(AmazonRDS)
- AWS Resilience Hub
- AWS Resource Groups
- AWS 리소스 탐색기
- Amazon Route 53
- Amazon Route 53 Recovery Readiness
- Amazon Route 53 Resolver
- Amazon SageMaker
- AWS Secrets Manager
- AWS Service Catalog
- Amazon Simple Notification Service
- Amazon Simple Queue Service

- Amazon Simple Storage Service(S3)
- AWS Step Functions
- AWS Systems Manager
- AWS Verified Access
- AWS Wavelength

Amazon API Gateway

- `apigateway:restapis`

AWS App Runner

- `apprunner:vpcconnector`

Amazon AppStream 2.0

- `appstream:appblock`
- `appstream:application`
- `appstream:fleet`
- `appstream:stack`

AWS AppSync

- `appsync:apis`

Amazon Athena

- `athena:datacatalog`
- `athena:workgroup`

AWS Backup

- `backup:backupplan`

AWS Batch

- batch:computeenvironment
- batch:jobqueue
- batch:schedulingpolicy

AWS CloudFormation

- cloudformation:stack
- cloudformation:stackset

Amazon CloudFront

- cloudfront:cache-policy
- cloudfront:distribution
- cloudfront:function
- cloudfront:fieldlevelencryptionconfig
- cloudfront:fieldlevelencryptionprofile
- cloudfront:origin-access-identity
- cloudfront:originaccesscontrol
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy

AWS CloudTrail

- cloudtrail:trail

Amazon CloudWatch

- cloudwatch:alarm
- cloudwatch:dashboard

- cloudwatch:insight-rule
- cloudwatch:metric-stream
- evidently:project

Amazon CloudWatch Evidently

- evidently:project/experiment
- evidently:project/feature
- evidently:project/launch

Amazon CloudWatch Logs

- logs:destination
- logs:log-group

AWS CodeArtifact

- codeartifact:domain
- codeartifact:repository

AWS CodeBuild

- codebuild:project

AWS CodeCommit

- codecommit:repository

Amazon CodeGuru Profiler

- codeguru-profiler:profilingGroup

AWS CodePipeline

- codepipeline:pipeline

AWS CodeConnections

- codestarconnections:connect

Amazon Cognito

- cognito:identitypool
- cognito:userpool

Amazon Connect

- appintegrations:eventintegration

Amazon Q Connect

- wisdom:assistant
- wisdom:association
- wisdom:knowledge-base

Amazon Detective

- detective:graph

Amazon DynamoDB

- dynamodb:table

EC2 이미지 빌더

- imagebuilder:component
- imagebuilder:containerrecipe
- imagebuilder:distributionconfiguration
- imagebuilder:image
- imagebuilder:imagepipeline
- imagebuilder:imagerecipe
- imagebuilder:infrastructureconfiguration

Amazon ECR 퍼블릭

- ecrpublic:repository

AWS Elastic Beanstalk

- elasticbeanstalk:application
- elasticbeanstalk:applicationversion
- elasticbeanstalk:configurationtemplate
- elasticbeanstalk:environment

Amazon ElastiCache

- elasticache:cluster
- elasticache:globalreplicationgroup
- elasticache:parametergroup
- elasticache:replicationgroup
- elasticache:reserved-instance
- elasticache:snapshot
- elasticache:subnetgroup
- elasticache:user
- elasticache:usergroup

Amazon Elastic Compute Cloud(AmazonEC2)

- ec2:capacity-reservation
- ec2:capacity-reservation-fleet
- ec2:client-vpn-endpoint
- ec2:customer-gateway
- ec2:dedicated-host
- ec2:dhcp-options
- ec2:egress-only-internet-gateway
- ec2:elastic-gpu
- ec2:elastic-ip
- ec2:fleet
- ec2:fpga-image
- ec2:host-reservation
- ec2:image
- ec2:instance
- ec2:instance-event-window
- ec2:internet-gateway
- ec2:ipam
- ec2:ipam-pool
- ec2:ipam-scope
- ec2:ipv4pool-ec2
- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path

- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances
- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request
- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table
- ec2:transitgatewayroutetableannouncement
- ec2:volume
- ec2:vpc
- ec2:vpc-endpoint
- ec2:vpc-flow-log
- ec2:vpc-peering-connection
- ec2:vpn-connection
- ec2:vpn-gateway

Amazon Elastic 컨테이너 레지스트리

- ecr:repository

Amazon Elastic Container Service

- ecs:cluster
- ecs:container-instance
- ecs:service
- ecs:task-definition
- ecs:task-set

Amazon Elastic File System

- efs:filesystem
- efs:accesspoint

Elastic Load Balancing

- elasticloadbalancing:listener
- elasticloadbalancing:listener-rule
- elasticloadbalancing:listener-rule/app
- elasticloadbalancing:listener/app
- elasticloadbalancing:listener/net
- elasticloadbalancing:loadbalancer
- elasticloadbalancing:loadbalancer/app
- elasticloadbalancing:loadbalancer/net
- elasticloadbalancing:targetgroup

AWS Elemental MediaPackage

- mediapackage:channel

- mediapackage:originendpoint
- mediapackage-vod:packaging-configurations
- mediapackage-vod:packaging-groups

AWS Elemental MediaTailor

- mediatailor:playbackConfiguration

Amazon EMR Serverless

- emr-serverless:applications

Amazon EventBridge

- events:event-bus
- events:rule

AWS Fault Injection Service

- fis:experimenttemplate

Amazon Forecast

- forcast:dataset
- forcast:dataset-group

Amazon Fraud Detector

- frauddetector:detector
- frauddetector:entity-type
- frauddetector:event-type
- frauddetector:label
- frauddetector:outcome

- frauddetector:variable

Amazon GameLift

- gamelift:alias

AWS Global Accelerator

- globalaccelerator:accelerator
- globalaccelerator:accelerator/listener
- globalaccelerator:accelerator/listener/endpoint-group

AWS Glue

- glue:database
- glue:job
- glue:table
- glue:trigger

AWS Glue DataBrew

- databrew:dataset
- databrew:recipe
- databrew:ruleset

AWS Identity and Access Management

- iam:group
- iam:instance-profile
- iam:oidc-provider
- iam:policy
- iam:role

- iam:saml-provider
- iam:server-certificate
- iam:user
- iam:virtualmfadevice

Amazon Interactive Video Service

- ivs:channel
- ivs:streamkey

AWS IoT

- iot:authorizer
- iot:jobtemplate
- iot:mitigationaction
- iot:policy
- iot:provisioningtemplate
- iot:rolealias
- iot:securityprofile
- iot:thing
- iot:topicrule

AWS IoT Analytics

- iotanalytics:channel
- iotanalytics:dataset
- iotanalytics:datastore
- iotanalytics:pipeline

AWS IoT Events

- iotevents:alarmModel

- iotevents:detectorModel
- iotevents:input

AWS IoT Greengrass Version 1

- greengrass:components
- greengrass:groups

AWS IoT SiteWise

- iotsitewise:asset
- iotsitewise:assetmodel
- iotsitewise:gateway

AWS IoT TwinMaker

- iottwinmaker:workspace
- iottwinmaker:workspace/component-type
- iottwinmaker:workspace/entity

AWS Key Management Service

- kms:key

Amazon Kinesis

- kinesis:stream

Amazon Data Firehose

- kinesisfirehose:deliverystream

Amazon Kinesis Video Streams

- kinesisvideo:stream

AWS Lambda

- lambda:code-signing-config
- lambda:event-source-mapping
- lambda:function

Amazon Lex

- lex:bot

Amazon Location Service

- geo:place-index
- geo:tracker

Amazon Lookout for Metrics

- lookoutmetrics:Alert

Amazon Lookout for Vision

- lookoutvision:project

Amazon Managed Service for Apache Flink

- kinesisanalytics:application

Amazon Managed Service for Prometheus

- aps:rulegroupsnamespace
- aps:workspace

Amazon Managed Service for Prometheus

- memorydb:cluster
- memorydb:parametergroup
- memorydb:user

Amazon Managed Streaming for Apache Kafka

- kafka:cluster
- kafka:configuration

AWS Migration Hub Refactor Spaces

- refactor-spaces:environment
- refactor-spaces:environment/application
- refactor-spaces:environment/application/route
- refactor-spaces:environment/application/service

AWS Network Firewall

- network-firewall:firewall-policy

AWS Network Manager

- networkmanager:core-network
- networkmanager:device
- networkmanager:global-network
- networkmanager:link

Amazon OpenSearch Service

- es:domain

AWS Panorama

- panorama:package

Amazon Personalize

- personalize:dataset
- personalize:dataset-group
- personalize:schema

AWS Private Certificate Authority

- acmpca:certificateauthority

Amazon QLDB

- qldb:ledger
- qldb:stream

Amazon Redshift

- redshift:cluster
- redshift:eventsubscription
- redshift:parametergroup
- redshift:snapshot
- redshift:snapshotcopygrant
- redshift:snapshotschedule
- redshift:subnetgroup
- redshift:usagelimit

Amazon Rekognition

- rekognition:project

Amazon Relational Database Service(AmazonRDS)

- rds:auto-backup
- rds:cev
- rds:cluster
- rds:cluster-endpoint
- rds:cluster-pg
- rds:cluster-snapshot
- rds:db
- rds:db-proxy
- rds:db-proxy-endpoint
- rds:deployment
- rds:es
- rds:global-cluster
- rds:og
- rds:pg
- rds:ri
- rds:secgrp
- rds:snapshot
- rds:subgrp

AWS Resilience Hub

- resiliencehub:resiliencypolicy

AWS Resource Groups

- resourcegroups:group

AWS 리소스 탐색기

- resource-explorer-2:index
- resource-explorer-2:view

Amazon Route 53

- route53:healthcheck
- route53:hostedzone

Amazon Route 53 Recovery Readiness

- route53-recover-readiness:recovery-group
- route53-recover-readiness:resource-set

Amazon Route 53 Resolver

- route53resolver:firewalldomainlist
- route53resolver:firewallrulegroup
- route53resolver:resolverendpoint
- route53resolver:resolverrule

Amazon SageMaker

- sagemaker:model
- sagemaker:notebookinstance

AWS Secrets Manager

- secretsmanager:secret

AWS Service Catalog

- servicecatalog:applications
- servicecatalog:attribute-groups

Amazon Simple Notification Service

- sns:topic

Amazon Simple Queue Service

- sqs:queue

Amazon Simple Storage Service(S3)

- s3:accesspoint
- s3:bucket
- s3:storage-lens

AWS Step Functions

- states:statemachine
- stepfunctions:activity

AWS Systems Manager

- ssm:association
- ssm:document
- ssm:maintenancewindow
- ssm:managed-instance
- ssm:parameter
- ssm:resourcedatasync
- ssm:windowtarget

- ssm:windowtask

AWS Verified Access

- ec2:verifiedaccessendpoint
- ec2:verifiedaccessgroup
- ec2:verifiedaccessinstance
- ec2:verifiedaccesstrustprovider

AWS Wavelength

- ec2:carriergateway

지원되는 리소스 유형 목록에 프로그래밍 방식으로 액세스

코드에서 지원되는 리소스 유형 목록에 액세스하려면 모든 에서 ListSupportedResourceTypes 작업을 호출할 수 있습니다 AWS SDK.

예를 들어 다음 예제와 같이 list-supported-resource-types AWS Command Line Interface (AWS CLI) 명령을 실행할 수 있습니다.

```
$ aws resource-explorer-2 list-supported-resource-types
{
    "ResourceTypes": [
        {
            "ResourceType": "acm-pca:certificate-authority",
            "Service": "acm-pca"
        },
        {
            "ResourceType": "airflow:environment",
            "Service": "airflow"
        },
        {
            "ResourceType": "amplify:branches",
            "Service": "amplify"
        },
... truncated for brevity ...
```

다른 유형으로 나타나는 리소스 유형

일부 리소스 유형은 다른 리소스 유형과 공통 형식을 공유하는 Amazon 리소스 이름(ARN) 문자열로 식별됩니다. 이러한 일이 발생하면 Resource Explorer는 다른 리소스 유형과 같은 리소스를 보고할 수 있습니다. 이는 다음 표의 리소스 유형에 영향을 미칩니다.

실제 리소스 유형	리소스 유형으로 보고됨
ec2:securitygroupegress ec2:securitygroupingress	ec2:security-group-rule
elasticloadbalancingv2:loadbalancer	elasticloadbalancing:loadbalancer
docdb:dbcluster neptune:dbcluster rds:dbcluster	rds:cluster
docdb:dbclusterparametergroup neptune:dbclusterparametergroup rds:dbclusterparametergroup	rds:cluster-pg
docdb:clustersnapshot neptune:dbclustersnapshot rds:clustersnapshot	rds:cluster-snapshot
docdb:dbinstance neptune:dbinstance rds:dbinstance	rds:db
docdb:eventsubscription neptune:eventsubscription	rds:es

실제 리소스 유형	리소스 유형으로 보고됨
rds:eventsubscription	
docdb:globalcluster rds:globalcluster	rds:global-cluster
neptune:dbparametergroup rds:dbparametergroup	rds:pg
docdb:dbsubnetgroup neptune:dbsubnetgroup rds:dbsubnetgroup	rds:subgrp

Resource Explorer에 대한 검색 쿼리 구문 참조

AWS 리소스 탐색기 는 에서 개별 AWS 리소스를 찾는 데 도움이 됩니다 AWS 계정. 원하는 리소스를 정확히 찾을 수 있도록 Resource Explorer는 이 항목에 설명된 구문을 지원하는 검색 쿼리 문자열을 허용합니다. 여기에 설명된 기능을 사용하는 방법을 보여 주는 쿼리의 예제는 Resource Explorer 검색 쿼리 예제를 참조하세요.

> **Note**
>
> 현재 역할 또는 사용자와 같이 AWS Identity and Access Management (IAM) 리소스에 연결된 태그는 인덱싱되지 않습니다.

Resource Explorer에서 쿼리가 작동하는 방식

검색 쿼리는 항상 뷰를 사용합니다. 명시적으로 지정하지 않으면 Resource Explorer는 작업 AWS 리전 중인 의 기본값으로 지정된 보기를 사용합니다.

뷰는 쿼리에 사용할 수 있는 리소스를 결정합니다. 각각 다른 리소스 세트를 반환하는 다양한 뷰를 생성할 수 있습니다.

예를 들어 키 `Environment` 및 값 `Production`으로 태그가 지정된 리소스만 포함하는 뷰를 생성할 수 있습니다. 그런 다음 해당 리소스를 봐야 하는 업무상 이유가 있는 사용자에게만 해당 뷰에 대한 액세스 권한을 부여하도록 선택할 수 있습니다. `Alpha` 또는 `Beta` 환경 리소스가 포함된 별도의 뷰에는 해당 리소스를 확인해야 하는 여러 사용자가 액세스할 수 있습니다. 각 뷰에 액세스할 수 있는 사용자를 제어하는 방법에 대한 자세한 내용은 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여를 참조하세요.

쿼리 문자열 구문

이 섹션에서는 쿼리 구문, 필터 및 필터 연산자의 기본 측면에 대한 정보를 제공합니다.

기본 사항

가장 기본적으로 `QueryString`은 논리 **`OR`** 연산자로 암시적으로 결합되는 자유 형식 텍스트 키워드 세트입니다. 다음 예제와 같이 공백을 사용하여 각 키워드를 다른 키워드와 구분합니다.

```
ec2 billing test gamma
```

Resource Explorer는 이 키워드 목록을 다음과 같은 의미로 평가합니다.

```
ec2 OR billing OR test OR gamma
```

Resource Explorer는 관련성을 기준으로 결과를 정렬하여 더 많은 수의 검색어와 일치하는 리소스에 더 높은 우선 순위를 부여합니다. 하나 이상의 용어와 일치하지 않는 리소스는 결과에서 제외되지 않습니다. 하지만 Resource Explorer는 관련성이 낮은 것으로 간주하여 검색 결과에서 더 아래로 밀어냅니다.

`QueryString` 파라미터에 빈 문자열을 지정하는 경우 쿼리는 작업에 사용된 뷰를 통해 사용할 수 있는 첫 1,000개의 리소스를 반환합니다. 쿼리에서 반환할 수 있는 최대 리소스 수는 1,000개입니다.

> **Note**
>
> AWS 는 자유 형식 텍스트 키워드를 평가하기 위해 일치하는 로직 및 관련성 알고리즘을 업데이트하여 고객에게 가장 적절한 결과를 제공할 수 있는 권한을 보유합니다. 따라서 자유 형식 텍스트 키워드를 사용한 동일한 쿼리에 대해 반환되는 결과는 시간이 지남에 따라 변경될 수 있습니다. 보다 확실한 결과가 필요한 경우 필터를 사용하는 것이 좋습니다. 필터 매칭 로직은 시간이 지나도 변경되지 않습니다.

필터

필터를 포함하면 쿼리 결과를 더 엄격하게 제한할 수 있습니다. 텍스트 키워드와 달리 필터는 AND 연산자를 사용하여 쿼리에서 평가됩니다. 예를 들어 두 개의 자유 형식 키워드와 두 개의 필터로 구성된 다음 쿼리를 생각해 보세요.

```
test instance service:EC2 region:us-west-2
```

이 쿼리는 다음과 같이 평가됩니다.

```
( test OR instance ) AND service:EC2 AND region:us-west-2
```

필터는 항상 AND 논리적 연산자를 사용하여 평가됩니다. 리소스가 필터와 일치하지 않는 경우 해당 리소스는 결과에 포함되지 않습니다. 예제 쿼리 결과에는 Amazon과 연결되어 EC2 있고 미국 서부(오레곤)에 있으며 어떤 방식으로든 키워드 중 하나 이상이 연결된 리소스 AWS 리전 가 포함됩니다.

> **Note**
>
> 암시적 AND로 인해 리소스와 연결된 값을 하나만 가질 수 있는 속성에 대해 하나의 필터만 사용할 수 있습니다. 예를 들어, 리소스는 하나의 AWS 리전에만 속할 수 있습니다. 따라서 다음 쿼리는 결과를 반환하지 않습니다.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> 이 제한은 동시에 여러 값을 가질 수 있는 속성(예: `tag:`, `tag.key:`, `tag.value:`)의 필터에는 적용되지 않습니다.

다음 표에는 Resource Explorer 검색 쿼리에 사용할 수 있는 사용 가능한 필터 이름이 나열되어 있습니다.

필터 이름	설명 및 예제
`accountid:`	리소스를 소유 AWS 계정 한 . Resource Explorer는 지정된 계정이 소유한 리소스만 결과에 포함합니다. `accountid:123456789012`

`application:`	이 필터를 사용하면 `awsApplication` 태그 키와 리소스 그룹 값을 사용하여 리소스를 검색할 수 있습니다. 애플리케이션 이름 또는 애플리케이션 리소스 그룹 으로 검색할 수 있습니다ARN.
	
	`application:MyApplicationName`
	
	`application:arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`
	
	`arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`

필터 이름	설명 및 예제
	Note 이 필터를 사용하려면 뷰에 태그 지정 데이터에 대한 액세스 권한이 있어야 합니다.
`id:`	개별 리소스의 식별자로, Amazon 리소스 이름(ARN)으로 표시됩니다. `id:arn:aws:license-manager:  us-east-1 :12345678 9012:license-configuration:lic-ecbd5574fd92cb 0d312baea26EXAMPLE`
`region:`	리소스가 있는 AWS 리전 위치입니다. Resource Explorer는 결과에 지정된 에 있는 리소스만 포함합니다 AWS 리전. `region:us-east-1` **Note** 리전 코드만 입력하면(예: `us-east-1` 와 같은 필터 없이) `region:us-east-1` 와 동일한 결과를 반환하지 않습니다. 이 결과는 필터가 아닌 자유 형식 텍스트 키워드로서 리전 코드가 개별 조각으로 분류되기 때문입니다. 예를 들어, `us-east-1` 은 `us`, `east`, `1`로 검색됩니다. `region:` 접두사를 사용하면 이러한 구성 요소 분류가 발생하지 않습니다.

필터 이름	설명 및 예제
`region:global`	개인과 연결되지는 AWS 리전 않았지만 범위가 글로벌로 간주되는 리소스를 찾는 데 사용할 수 있는 `region:` 필터의 특수 사례입니다. `region:global` **Note** 키워드 `global`만 입력하면 리터럴 단어 “global”이 글로벌 리소스에 연결되지 않기 때문에 `region:global` 과 동일한 결과가 반환되지 않습니다. `global`을 키워드로 입력하면 해당 리소스와 연결된 리터럴 문자열이 있는 리소스만 반환됩니다.
`resourcetype:`	*`service`*`:`*`type`* 표기법의 리소스 유형입니다. Resource Explorer는 지정된 유형의 리소스만 결과에 포함합니다. `resourcetype:ec2:instance`
`resourcetype.supports:`	이 필터를 사용하면 태그를 지원하는 리소스를 검색할 수 있습니다. `tags`는 지원되는 유일한 값입니다. Resource Explorer는 태그 지정 가능한 리소스만 결과에 포함합니다. `resourcetype.supports:tags`
`service:`	리소스 유형과 AWS 서비스 연결된 . Resource Explorer는 지정된 서비스에 의해 생성되고 관리되는 리소스만 결과에 포함합니다. `service:ec2`
`tag:`	`<key>=<value>` 으로 표현되는 태그 키/값 쌍입니다. Resource Explorer는 일치하는 키와 지정된 값이 모두 있는 태그가 있는 리소스만 결과에 포함합니다. `tag:environment=production`

필터 이름	설명 및 예제
`tag:all`	Resource Explorer에서 리소스 유형이 지원되지 않더라도 하나 이상의 사용자 생성 태그가 연결된 리소스를 검색할 수 있는 `tag:` 필터의 특수 사례입니다. **Note** AWS 서비스 생성 태그가 있는 리소스는 여전히 이 필터의 결과에 표시됩니다.
`tag:none`	사용자가 생성한 태그가 연결되지 않은 리소스를 검색할 수 있는 `tag:` 필터의 특이 케이스입니다. **Note** AWS 서비스 생성 태그가 있는 리소스는 여전히 이 필터의 결과에 표시됩니다.
`tag.key:`	태그 키. Resource Explorer는 값에 관계없이 일치하는 키가 있는 태그가 있는 리소스만 결과에 포함합니다. `tag.key:environment`
`tag.value:`	태그 값. Resource Explorer는 키 이름에 관계없이 일치하는 값이 있는 태그가 있는 리소스만 결과에 포함합니다. `tag.value:production`

필터 연산자

다음 표에 표시된 연산자 중 하나를 문자열의 일부로 포함하여 키워드와 필터를 수정할 수 있습니다.

연산자	설명 및 예제
`"multiple word phrase"`	단일 키워드로 취급해야 하는 여러 단어로 구성된 구문을 큰따옴표(" ")로 묶습니다. Resource Explorer는 전체 구문과 모든 단어가 함께 지정된 순서대로 일치하는 리소스만 포함합니다.

연산자	설명 및 예제

또는
 	
"hyphenated-phrase "
	큰따옴표를 사용하지 않으면 Resource Explorer는 구문을 공백이나 하이픈으로 구성 요소로 나누고, 함께 있지 않거나 순서가 다르더라도 개별 구성 요소와 일치하는 리소스를 포함합니다. 견적은 연산자 뒤의 모든 것에 관한 것이어야 합니다.
	
	`"This matches only resources with the whole sentence."`
	
	`This matches resources with any of the words.`
	
	`"us-east-1"` - 정확한 리전과 연결된 리소스만 일치합니다.
	
	`us-east-1` - “us”, “east” 또는 “1"을 포함하는 모든 리소스와 일치합니다.
	
	`-tag:"environment=production"`

*keyword**	접두사 와일드카드 매칭. 문자열의 끝에만 와일드카드 문자(별표 *)를 넣을 수 있습니다. Resource Explorer는 * 앞에 접두사 텍스트로 시작하는 값이 있는 리소스만 결과에 포함합니다. 다음 예제는 로 시작하는 모든 와 일치 AWS 리전 합니다`us-east`. `region:us-east*` **Important** 통합 검색은 문자열의 첫 번째 키워드 끝에 와일드카드 문자(*) 연산자를 자동으로 삽입합니다. 즉, 통합 검색 결과에는 지정된 키워드로 시작하는 모든 문자열과 일치하는 리소스가 포함됩니다. Resource Explorer 콘솔의 리소스 검색 페이지에 있는 쿼리 텍스트 상자에서 수행되는 검색에는 와일드카드 문자가 자동으로 추가되지 않습니다. 검색 문자열에서 용어 뒤에 *를 수동으로 삽입할 수 있습니다.

연산자	설명 및 예제

-keyword	Not 연산자. 키워드 또는 필터의 시작 부분에 하이픈(-)을 삽입하여 검색 결과를 반전시킬 수 있습니다. Resource Explorer는 이 연산자 다음에 오는 키워드 또는 필터와 일치하는 모든 리소스를 결과에서 제외합니다. 다음 예제에서는 Amazon EC2 서비스와 연결된 모든 리소스를 결과에서 제외합니다.
	
	`-service:ec2`
	
	Important
	
	명령을 사용하고 AWS CLI `search --query-string` 파라미터 값에 - 연산자가 첫 번째 문자인 경우 파라미터 이름을 일반 공백 문자 대신 동일한 기호 문자(=)로 해당 값과 분리해야 합니다. 공백 문자를 사용하면 가 문자열을 CLI 잘못 해석합니다. 예를 들어 다음 쿼리는 실패합니다.
	
	`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`
	
	공백을 =으로 대체하는 다음 수정된 쿼리 문자열은 예상대로 작동합니다.
	
	`aws resource-explorer-2 search --query-string ="-tag:none region:us-east-1"`
	
	-가 파라미터 값의 첫 번째 문자가 되지 않도록 쿼리 문자열에서 필터 순서를 변경하는 경우 표준 공백 문자를 사용할 수 있습니다. 다음 쿼리 문자열은 작동합니다.
	
	`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"`

연산자	설명 및 예제

\<*special character*>	해석하지 않고 표시된 대로 정확히 포함해야 하는 특수 문자를 이스케이프할 수 있습니다. 텍스트에 특수 문자(* " - : = \) 중 하나가 포함된 경우 문자 그대로 해석되도록 하려면 해당 문자 앞에 백슬래시(\)를 붙여야 합니다. 다음은 하이픈(-) 문자("my-key-word")가 포함된 자유 형식 텍스트 키워드를 사용하는 방법을 나타낸 예제입니다.
	
	또한 Resource Explorer에서 하이픈의 표현식을 세 개의 개별 키워드로 분리하지 않도록 문구 전체를 큰따옴표로 묶을 수 있습니다.
	
	`"my\-key\-word"`
	
	리터럴 백슬래시를 삽입하려면 두 개의 백슬래시 문자를 연속으로 삽입하세요. 첫 번째 백슬래시는 이스케이프 문자로 해석되고 두 번째 백슬래시는 삽입할 리터럴 문자입니다.
	
	`"some_text\\some_more_text"`

> **Note**
>
> 뷰에 리소스에 연결된 태그가 포함되어 있는 경우 유효하지 않은 필터가 자유 형식 텍스트 검색으로 해석될 수도 있기 때문에 Search 작업 시 검색 문자열에 대한 검증 오류가 발생하지 않습니다. 예를 들어 `cat:blue`가 필터처럼 보이더라도 `cat:`는 유효하고 정의된 필터 중 하나가 아니기 때문에 Resource Explorer는 이를 하나로 구문 분석할 수 없습니다. 대신 Resource Explorer는 전체 문자열을 자유 형식 검색 문자열로 해석하여 태그 키 이름이나 의 일부와 일치시킬 수 있습니다ARN.
> 다음 중 하나가 true일 경우 작업 시 검증 오류가 발생합니다.
>
> - 뷰에 태그에 대한 정보가 포함되지 않음
> - 검색 쿼리가 명시적으로 태그 필터(`tag.key:`, `tag.value:` 또는 `tag:`)를 사용함

Resource Explorer 검색 쿼리 예제

다음 예제는 AWS 리소스 탐색기에서 사용할 수 있는 일반적인 쿼리 유형에 대한 구문을 보여줍니다.

Important

AWS CLI `search` 명령을 사용하고 `--query-string` 파라미터 값의 첫 번째 문자로 `-` 연산자를 사용하는 경우 일반적인 공백 문자 대신 등호 문자(=)를 사용하여 파라미터 이름과 해당 값을 구분해야 합니다. 공백 문자를 사용하면 CLI가 문자열을 잘못 해석합니다. 예를 들어 다음 쿼리는 실패합니다.

```
aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
```

공백을 =으로 대체하는 다음 수정된 쿼리는 예상대로 작동합니다.

```
aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
```

`-`가 파라미터 값의 첫 번째 문자가 되지 않도록 쿼리 문자열에서 필터 순서를 변경하는 경우 표준 공백 문자를 사용할 수 있습니다. 다음 쿼리는 작동합니다.

```
aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
```

태그가 지정되지 않은 리소스 검색

계정에서 ABAC(속성 기반 액세스 제어)를 사용하거나, 비용 기반 할당을 사용하거나, 리소스에 대해 태그 기반 자동화를 수행하려는 경우 계정에서 태그가 누락되었을 수 있는 리소스를 알아야 합니다. 다음 예제 쿼리에서는 특이 케이스 필터 태그: 없음을 사용하여 사용자 생성 태그가 누락된 모든 리소스를 반환합니다.

`tag:none` 필터는 사용자가 생성한 태그에만 적용됩니다. AWS에서 생성하고 유지 관리하는 태그는 이 필터에서 제외되며 결과에는 계속 표시됩니다.

```
tag:none
```

모든 AWS 생성된 시스템 태그도 제외하려면 다음 예제와 같이 두 번째 필터를 추가합니다. 쿼리 문자열의 첫 번째 요소는 사용자가 생성한 모든 태그를 필터링하여 이전 예제를 복제합니다. AWS 생성된

시스템 태그는 항상 문자 aws로 시작됩니다. 따라서 tag.key 필터와 함께 논리 부정(NOT) 연산자(-)를 사용하여 aws로 시작되는 키 이름을 가진 태그가 있는 모든 리소스도 제외할 수도 있습니다.

```
tag:none -tag.key:aws*
```

태그가 지정된 리소스 검색

모든 유형의 태그가 있는 리소스를 모두 찾으려면 다음과 같이 특이 케이스 태그: 없음 필터와 함께 논리 부정(NOT) 연산자(-)를 사용할 수 있습니다.

```
-tag:none
```

특정 태그가 누락된 리소스 검색

또한 ABAC와 관련하여, 지정된 키가 있는 태그가 없는 모든 리소스를 검색할 수도 있습니다. 다음 예제에서는 논리 부정(NOT) 연산자 -를 사용하여 키 이름이 Department인 태그가 없는 모든 리소스를 반환합니다.

```
-tag.key:Department
```

잘못된 태그 값을 가진 리소스 검색

규정 준수를 위해 중요한 태그에서 태그 값이 누락되었거나 철자가 틀린 모든 리소스를 검색하는 것이 좋습니다. 다음 예제에서는 키 이름이 environment인 태그가 있는 모든 리소스를 반환합니다. 하지만 쿼리는 유효한 값 prod, integ, dev 중 하나를 가진 모든 리소스를 필터링합니다. 이 쿼리에서 나타나는 모든 결과에는 조사하고 수정해야 하는 다른 값이 있습니다.

> **Important**
>
> Resource Explorer 검색은 대/소문자를 구분하지 않으므로 대/소문자 표기만 다른 키 이름과 값을 구분할 수 없습니다. 예를 들어 다음 예제의 값은PROD, prod, PrOd 또는 모든 변형과 일치합니다. 그러나 일부 애플리케이션에서는 대/소문자를 구분하여 태그를 사용합니다. 소문자 태그 키 이름 및 값만 사용하는 등 조직에 맞게 대문자 사용 전략을 표준화하는 것이 좋습니다. 일관된 접근 방식을 취하면 대/소문자 표기만 다른 태그로 인해 발생할 수 있는 혼란을 피할 수 있습니다.

```
tag.key:environment -tag:environment=prod -tag:environment=integ -tag:environment=dev
```

AWS 리전의 하위 집합에서 리소스 검색

전 세계 특정 리전의 모든 리전을 일치시키려면 '*' 와일드카드 연산자를 사용하세요. 다음 예제는 유럽(Europe) 리전에 있는 모든 리소스를 반환합니다.

```
region:eu-*
```

글로벌 리소스 검색

region: 필터에 특이 케이스 global 값을 사용하여 글로벌 리소스로 간주되고 개별 리전과 연결되지 않은 리소스를 찾을 수 있습니다.

```
region:global
```

특정 리전에 있는 특정 유형의 리소스 검색

여러 필터를 사용하는 경우 Resource Explorer는 접두사를 암시적 논리 AND 연산자와 결합하여 표현식을 평가합니다. 다음 예제에서는 아시아 태평양(홍콩) 리전 AND에 있는 모든 리소스가 Amazon EC2 인스턴스임을 반환합니다.

```
region:ap-east-1 resourcetype:ec2:instance
```

> **Note**
>
> 암시적 AND로 인해 리소스와 연결된 값을 하나만 가질 수 있는 속성에 대해 하나의 필터만 사용할 수 있습니다. 예를 들어, 리소스는 하나의 AWS 리전에만 속할 수 있습니다. 따라서 다음 쿼리는 결과를 반환하지 않습니다.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> 이 제한은 동시에 여러 값을 가질 수 있는 속성(예: tag:, tag.key:, tag.value:)의 필터에는 적용되지 않습니다.

여러 단어로 구성된 용어가 있는 리소스 검색

여러 단어로 구성된 용어를 큰따옴표(")로 묶으면 전체 용어가 지정된 순서대로 포함된 결과만 반환됩니다. 큰따옴표를 사용하지 않으면 Resource Explorer는 해당 용어를 구성하는 개별 단어와 일치하는 리소스를 반환합니다. 예를 들어 다음 쿼리는 큰따옴표를 사용하여 용어 `"west wing"`과 일치하는 리소스만 반환합니다. 쿼리는 `us-west-2` AWS 리전(또는 해당 코드에 `west`가 포함된 다른 리전)의 리소스 또는 “west”라는 단어 없이 “wing”이라는 단어와 일치하는 리소스와 일치하지 않습니다.

```
"west wing"
```

지정된 CloudFormationStack의 일부인 리소스 검색

AWS CloudFormation 스택의 일부로 리소스를 생성하면 자동으로 모든 리소스에 스택의 이름으로 태그가 지정됩니다. 다음 예제에서는 지정된 스택의 일부로 생성된 모든 리소스를 반환합니다.

```
tag:aws:cloudformation:stack-name=my-stack-name
```

AWS Management Console에서 통합 검색 사용

AWS Management Console에는 모든 AWS 콘솔 페이지 상단에 검색 창이 포함되어 있습니다. 이 검색 창을 통해 AWS 서비스 설명서 및 블로그 주제를 검색하고 AWS 서비스 콘솔 페이지로 직접 이동할 수 있습니다. 필요한 Resource Explorer 기능을 활성화하여 통합 검색 기능을 활성화하면 AWS 계정의 리소스를 반환할 수도 있습니다.

통합 검색을 사용하면 사용자는 먼저 AWS 리소스 탐색기 콘솔로 이동할 필요 없이 모든 AWS 서비스 콘솔에서 리소스를 검색할 수 있습니다.

> **Tip**
>
> 통합 검색 창을 사용하여 리소스를 구체적으로 검색하려면 **/Resources**을 입력하여 검색 쿼리를 시작하세요. 이렇게 하면 AWS 리소스는 리소스를 나타내지 않는 결과보다 검색 결과에서 더 높은 순위를 차지하게 됩니다.

주제

> **Important**
>
> 통합 검색은 문자열의 첫 번째 키워드 끝에 와일드카드 문자(*) 연산자를 자동으로 삽입합니다. 즉, 통합 검색 결과에는 지정된 키워드로 시작하는 모든 문자열과 일치하는 리소스가 포함됩니다.
>
> Resource Explorer 콘솔의 리소스 검색 페이지에 있는 쿼리 텍스트 상자에서 수행되는 검색에는 와일드카드 문자가 자동으로 추가되지 않습니다. 검색 문자열에서 용어 뒤에 *를 수동으로 삽입할 수 있습니다.

통합 검색이 활성화되었는지 확인

AWS 계정에서 통합 검색이 활성화되어 있는지 확인하려면 설정 페이지 상단을 확인하세요. Resource Explorer에는 각 요구 사항의 현재 상태가 표시됩니다. 통합 검색 요구 사항은 다음과 같습니다.

- 최소한 하나 이상의 AWS 리전에서 Resource Explorer를 활성화해야 합니다. Resource Explorer 인덱스가 있는 리전의 리소스만 통합 검색 결과에 표시될 수 있습니다.
- 선택한 리전에 애그리게이터 인덱스를 생성해야 합니다. 이 리전에서 수행한 검색은 계정에 등록된 모든 리전의 결과를 반환합니다.
- 애그리게이터 인덱스가 포함된 리전에 기본 뷰를 생성해야 합니다. 리소스에 대한 통합 검색을 사용해야 하는 모든 사용자는 이 기본 뷰를 사용할 수 있는 권한이 있어야 합니다.
- 사용자는 `resource-explorer-2:Get*`, `resource-explorer-2:List*`, `resource-explorer-2:Describe*`, `resource-explorer-2:Search` 작업을 수행할 수 있는 권한을 부여하는 AWS Identity and Access Management(IAM) 권한 정책을 IAM 보안 주체에 할당해야 합니다. 자체 사용자 지정 IAM 정책을 사용하여 이러한 권한을 부여할 수 있습니다. 이러한 권한은 사용할 수 있는 다음 AWS 관리형 정책의 일부로 이미 포함되어 있습니다.
  - AWSResourceExplorerReadOnlyAccess
  - AWSResourceExplorerFullAccess

통합 검색 활성화

모든 AWS 콘솔에서 통합 검색에 대한 검색 결과에 계정의 리소스를 포함하려면 다음 단계를 완료해야 합니다.

1. 계정에서 하나 이상의 AWS 리소스 탐색기에서 AWS 리전을 활성화합니다.
2. 애그리게이터 인덱스를 포함할 리전 하나를 등록합니다.
3. 애그리게이터 인덱스가 있는 리전에 기본 뷰를 생성합니다.

CloudFormation을 통해 Resource Explorer 리소스 생성

AWS 리소스 탐색기은 AWS CloudFormation과 통합하여 AWS 리소스를 모델링 및 설정할 수 있는 서비스입니다. 이러한 통합을 통해 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있습니다. 원하는 모든 AWS리소스를 설명하는 템플릿을 생성하면 CloudFormation에서 해당 리소스를 프로비저닝하고 구성합니다. 리소스의 예로는 인덱스, 뷰 또는 AWS 리전에 대한 기본 뷰 할당 등이 있습니다.

CloudFormation을 사용할 때 템플릿을 재사용하여 Resource Explorer 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 및 리전에서 동일한 리소스를 반복적으로 프로비저닝할 수 있습니다.

Resource Explorer를 AWS Organizations에 배포하는 데 AWS CloudFormation 사용

AWS CloudFormation StackSets를 사용하여 Resource Explorer를 조직의 모든 계정에 배포할 수 있습니다. 조직에서 멤버 계정을 추가하거나 생성할 때 StackSets는 지정한 애그리게이터 인덱스를 포함하여 각 AWS 리전의 인덱스를 각 새 멤버 계정에 자동으로 구성할 수 있습니다. 지침은 조직의 계정에 Resource Explorer 배포 단원을 참조하세요.

Resource Explorer 및 CloudFormation 템플릿

Resource Explorer 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이 템플릿은 CloudFormation 스택에서 프로비저닝할 리소스에 대해 설명합니다. JSON 또는 YAML에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하면 CloudFormation 템플릿을 시작하는 데 도움이 됩니다. 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

Resource Explorer는 CloudFormation에서 다음 리소스 유형 생성을 지원합니다.

- 인덱스 - 리전에 인덱스를 생성하고 해당 리전에서 Resource Explorer를 활성화합니다. AWS 계정의 인덱스를 로컬 인덱스가 되도록 지정하거나 애그리게이터 인덱스가 되도록 지정할 수 있습니다. 자세한 정보는 에서 리소스 탐색기를 켜서 리소스를 인덱싱합니다. AWS 리전 및 애그리게이터 인덱스를 생성하여 리전 간 검색 활성화 섹션을 참조하세요.
- 뷰 - 사용자가 검색을 수행할 때 나타날 수 있는 결과를 결정하는 뷰를 생성합니다. 모든 검색 작업은 뷰를 지정해야 합니다. 액세스하려는 뷰를 사용할 수 있는 권한을 사용자에게 부여해야 합니다. 자세한 내용은 검색에 대한 액세스를 제공하기 위한 Resource Explorer 뷰 관리 섹션을 참조하세요.

> **Note**
>
> 동일한 리전에서 뷰를 생성하려면 먼저 해당 리전에 인덱스를 생성해야 합니다. 인덱스와 뷰를 동일한 스택의 일부로 생성하는 경우 다음 예제 템플릿에 표시된 대로 뷰의 DependsOn 속성을 사용하여 인덱스가 먼저 생성되도록 합니다.

- DefaultViewAssociation - 지정된 뷰를 해당 리전의 기본 뷰로 지정합니다. 사용자가 검색 작업에 사용할 뷰를 명시적으로 지정하지 않으면 Resource Explorer는 사용자가 검색을 수행하는 리전과 연결된 기본 뷰를 사용하려고 합니다. 자세한 정보는 AWS 리전에서 기본 뷰 설정 섹션을 참조하세요.

다음 예제는 동일한 리전에 하나의 인덱스와 뷰를 생성하고 해당 뷰를 해당 리전의 기본 뷰로 설정하는 방법을 보여줍니다.

YAML

```
Description: >-
  Sample CFN Stack setting up Resource Explorer with an aggregator index and a default
 view
Resources:
  SampleIndex:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
  SampleView:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: mySampleView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
    DependsOn: SampleIndex
  SampleDefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref SampleView
```

JSON

```
{
    "Description": "Sample CFN Stack setting up Resource Explorer with an aggregator
 index and a default view ",
    "Resources": {
        "SampleIndex": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer Sample Stack"
                }
            }
        },
        "SampleView": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "mySampleView",
                "IncludedProperties": [
                    {
                        "Name": "tags"
                    }
                ],
                "Tags": {
                    "Purpose": "ResourceExplorer Sample CFN Stack"
                }
            },
            "DependsOn": "SampleIndex"
        },
        "SampleDefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "SampleView"
                }
            }
        }
    }
}
```

Resource Explorer 인덱스와 뷰에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 ResourceExplorer2 리소스 유형 참조를 참조하세요.

AWS CloudFormation에 대해 자세히 알아보기

CloudFormation에 대한 자세한 내용은 다음 리소스를 참조하세요.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

리소스 검색에 AWS Chatbot 사용

AWS Chatbot 자연어 질문을 통해 AWS 서비스 및 AWS 리소스에 대한 정보를 검색하고 발견할 수 있습니다. AWS Chatbot는 관련 AWS 설명서 및 지원 문서 발췌문을 통해 채팅 채널에서 서비스 관련 질문에 직접 답변합니다. AWS Chatbot는 Resource Explorer를 사용하여 리소스 관련 질문에 대한 답변을 검색하고 찾습니다.

자세한 내용은 AWS Chatbot 관리자 안내서의 AWS Chatbot란 무엇인가요?를 참조하세요.

AWS 리소스 질문

AWS Chatbot는 Resource Explorer를 사용하여 리소스를 검색하고 발견합니다. AWS Chatbot는 이러한 검색 결과를 목록으로 표시합니다. 이 목록에는 일치하는 상위 5개 리소스가 표시되며 리소스 유형, AWS 리전, 태그별로 결과를 추가로 필터링할 수 있는 기능이 포함되어 있습니다.

사전 조건

AWS Chatbot 리소스 관련 질문을 하려면 다음을 수행해야 합니다.

- AWS 리전에 기본 뷰가 하나 이상 있는 활성 인덱스와 뷰가 있는지 확인하세요. 인덱스와 뷰를 사용하면 Resource Explorer에서 리소스를 분류하고 쿼리할 수 있습니다. 자세한 정보는 Resource Explorer 용어 및 개념 섹션을 참조하세요.
- 채널의 권한 체계에 따라 채널 역할 또는 각 적절한 사용자 역할에 AWSResourceExplorerReadOnlyAccess 정책을 추가합니다.
- 채널 가드레일 정책에서 권한을 AWSResourceExplorerReadOnlyAccess 허용하는지 확인하세요.

자주 묻는 리소스 질문

채팅 채널에서 직접 이러한 질문을 할 수 있습니다. 빨간색 텍스트로 된 단어를 사용자의 정보로 대체하세요.

```
@aws What services am I using in Region?

@aws What are the resources in my account with tags?

@aws What lambda functions do I have?
```

보안 내부 AWS 리소스 탐색기

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

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

- 클라우드 보안 — AWS AWS 서비스 클라우드에서 실행되는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. Resource Explorer에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램의 범위별 범위AWS 서비스 내 규정 준수 프로그램별 참조하십시오AWS 서비스 .
- 클라우드에서의 보안 — AWS 서비스 사용하는 항목에 따라 책임이 결정됩니다. 또한 여러분은 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다

이 설명서는 공동 책임 모델을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 AWS 리소스 탐색기됩니다. 보안 및 규정 준수 목표에 맞게 Resource Explorer를 구성하는 방법을 보여줍니다. 또한 Resource Explorer 리소스를 모니터링하고 보호하는 데 도움이 AWS 서비스 되는 기타 리소스를 사용하는 방법도 알아봅니다.

내용

IAM정책을 다음으로 업그레이드 IPv6

AWS 리소스 탐색기 고객은 IAM 정책을 사용하여 허용되는 IP 주소 범위를 설정하고 구성된 범위를 벗어나는 IP 주소가 Resource APIs Explorer에 액세스할 수 없도록 합니다.

리소스 탐색기-2.*region*리소스 탐색기가 호스팅되는.api.aws 도메인은 추가로 지원하도록 업그레이드 APIs 중입니다. IPv6 IPv4

IPv6주소를 처리하도록 IP 주소 필터링 정책을 업데이트하지 않으면 클라이언트가 Resource Explorer 도메인의 리소스에 대한 액세스 권한을 상실할 수 있습니다. API

에서 IPv4 로 업그레이드하여 영향을 받는 고객 IPv6

aws:가 포함된 정책과 함께 이중 주소 지정을 사용하는 고객은 이번 sourceIp 업그레이드의 영향을 받습니다. 이중 주소 지정은 네트워크가 및 를 모두 지원함을 의미합니다. IPv4 IPv6

이중 주소 지정을 사용하는 경우 현재 형식 주소로 구성된 IAM 정책을 업데이트하여 IPv4 형식 주소를 IPv6 포함해야 합니다.

액세스 문제에 대한 도움이 필요하면 AWS Support에 문의하세요.

> **Note**
>
> 다음 고객은 이번 업그레이드의 영향을 받지 않습니다.
>
> - IPv4네트워크에만 있는 고객.
> - IPv6네트워크에만 있는 고객.

이게 IPv6 뭐죠?

IPv6차세대 IP 표준은 결국 대체될 예정입니다IPv4. 이전 IPv4 버전에서는 32비트 주소 지정 체계를 사용하여 43억 개의 장치를 지원합니다. IPv6대신 128비트 주소 지정을 사용하여 약 340조 조 (또는 2에서 128번째 전력) 의 장치를 지원합니다.

```
2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

IAM에 대한 정책 업데이트 IPv6

IAM정책은 현재 `aws:SourceIp` 필터를 사용하여 허용되는 IP 주소 범위를 설정하는 데 사용됩니다.

이중 주소 지정은 AND IPV6 트래픽을 IPv4 모두 지원합니다. 네트워크에서 이중 주소 IAM 지정을 사용하는 경우 IP 주소 필터링에 사용되는 모든 정책이 주소 범위를 IPv6 포함하도록 업데이트되었는지 확인해야 합니다.

예를 들어, 이 Amazon S3 버킷 정책은 허용된 IPv4 주소 `192.0.2.0.*` 범위와 `203.0.113.0.*` `Condition` 요소에서 식별합니다.

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*",
                    "*203.0.113.0/24*"
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
    }
}
```

이 정책을 업데이트하려면 정책 `Condition` 요소가 IPv6 주소 범위 `2001:DB8:1234:5678::/64` 및 `2001:cdba:3257:8593::/64` 를 포함하도록 업데이트됩니다.

> **Note**
>
> 기존 IPv4 주소는 이전 버전과의 호환성을 위해 필요하므로 그대로 사용하십시오. NOT REMOVE

```
"Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*", <<DO NOT REMOVE existing IPv4 address>>
                    "*203.0.113.0/24*", <<DO NOT REMOVE existing IPv4 address>>
                    "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
                    "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
                ]
```

```
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
```

를 사용하여 IAM 액세스 권한을 관리하는 방법에 대한 자세한 내용은 사용 AWS Identity and Access Management 설명서의 관리형 정책 및 인라인 정책을 참조하십시오.

클라이언트가 지원할 수 있는지 확인하세요. IPv6

리소스 탐색기-2를 사용하는 고객. {region} .api.aws 엔드포인트는 해당 클라이언트가 이미 활성화된 다른 엔드포인트에 액세스할 수 있는지 확인하는 것이 좋습니다. AWS 서비스 IPv6 다음 단계는 이러한 엔드포인트를 확인하는 방법을 설명합니다.

이 예시에서는 Linux 및 curl 버전 8.6.0을 사용하고 api.aws 도메인에 있는 엔드포인트를 IPv6 활성화한 Amazon Athena 서비스 엔드포인트를 사용합니다.

> **Note**
>
> 클라이언트가 위치한 동일한 지역으로 AWS 리전 전환하십시오. 이 예에서는 미국 동부 (버지니아 북부) — `us-east-1` 엔드포인트를 사용합니다.

1. 다음 curl 명령을 사용하여 엔드포인트가 IPv6 주소로 확인되는지 확인합니다.

   ```
   dig +short AAAA athena.us-east-1.api.aws
   2600:1f18:e2f:4e05:1a8a:948e:7c08:d2d6
   2600:1f18:e2f:4e03:4a1e:83b0:8823:4ce5
   2600:1f18:e2f:4e04:34c3:6e9a:2b0d:dc79
   ```

2. 다음 curl 명령을 IPv6 사용하여 클라이언트 네트워크를 연결할 수 있는지 확인합니다.

   ```
   curl --ipv6 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
    %{response_code}\n" https://athena.us-east-1.api.aws

   remote ip: 2600:1f18:e2f:4e05:1a8a:948e:7c08:d2d6
   response code: 404
   ```

   원격 IP가 식별되었지만 응답 코드가 확인되지 않은 **0** 경우 를 사용하여 IPv6 엔드포인트에 성공적으로 네트워크가 연결되었습니다.

원격 IP가 비어 있거나 응답 코드가 비어 있는 경우 클라이언트 네트워크 또는 엔드포인트에 대한 네트워크 경로는 IPv4 전용입니다. `0` 다음 curl 명령으로 이 구성을 확인할 수 있습니다.

```
curl -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
 %{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 3.210.103.49
response code: 404
```

원격 IP가 식별되었지만 응답 코드가 없는 **`0`** 경우 를 사용하여 IPv4 엔드포인트에 성공적으로 네트워크 연결이 이루어진 것입니다. 운영 체제는 클라이언트에 유효한 프로토콜을 선택해야 하므로 원격 IP는 IPv4 주소여야 합니다. 원격 IP가 IPv4 주소가 아닌 경우 다음 명령을 사용하여 curl을 강제로 사용하십시오IPv4.

```
curl --ipv4 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
 %{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 35.170.237.34
response code: 404
```

에 대한 자격 증명 및 액세스 관리 AWS 리소스 탐색기

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 Resource Explorer 리소스를 사용할 수 있는 인증(로그인) 및 권한 부여(권한 보유) 대상을 제어합니다. IAM 는 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

고객

사용 방법 AWS Identity and Access Management (IAM)은 Resource Explorer에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Resource Explorer 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Resource Explorer 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Resource Explorer의 기능에 액세스할 수 없는 경우 AWS 리소스 탐색기 권한 문제 해결를 참조하세요.

서비스 관리자 - 회사에서 Resource Explorer 리소스를 책임지고 있다면 Resource Explorer 리소스에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Resource Explorer 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 이해합니다IAM. 회사가 Resource ExplorerIAM를 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요리소스 탐색기의 작동 방식 IAM.

IAM 관리자 - IAM 관리자인 경우 Resource Explorer에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. 에서 사용할 수 있는 Resource Explorer 자격 증명 기반 정책 예제를 보려면 섹션을 IAM참조하세요AWS 리소스 탐색기 자격 증명 기반 정책 예제.

ID를 통한 인증

인증은 자격 증명 AWS 으로 에 로그인하는 방법입니다. 로 AWS 계정 루트 사용자, IAM 사용자로 또는 IAM 역할을 수임하여 인증(에 로그인 AWS)되어야 합니다.

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

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

AWS 프로그래밍 방식으로 에 액세스하는 경우 는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공하여 자격 증명을 사용하여 요청에 암호화 방식으로 서명합니다. AWS 도구를 사용

하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 요청 서명을 참조하세요 AWS API.

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

AWS 계정 루트 사용자

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

사용자 및 그룹

IAM 사용자는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능한 경우 암호 및 액세스 키와 같은 장기 보안 인증 정보가 있는 IAM 사용자를 생성하는 대신 임시 보안 인증 정보를 사용하는 것이 좋습니다. 그러나 IAM 사용자와 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례에 대한 액세스 키 정기적으로 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 라는 이름의 그룹을 지정IAMAdmins하고 해당 그룹에 IAM 리소스를 관리할 수 있는 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 (역할 대신) IAM 사용자를 생성할 시기를 참조하세요.

역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 유사하지만 특정 사람과는 관련이 없습니다. IAM 역할을 전환 AWS Management Console 하여 에서 역할을 일시적으로 수임할 수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-

console.html 또는 AWS API 작업을 호출 AWS CLI 하거나 사용자 지정 를 사용하여 역할을 수임할 수 있습니다URL. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자에 대한 역할 생성을 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 의 역할과 상호 연관시킵니다IAM. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 특정 작업에 대해 일시적으로 다른 권한을 맡을 IAM 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 누군가(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 크로스 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 에서 크로스 계정 리소스 액세스를 IAM 참조하세요.
- 교차 서비스 액세스 - 일부 는 다른 에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가 Amazon에서 애플리케이션을 실행EC2하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하면 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 액세스 세션 전달을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 에 권한을 위임할 역할 생성을 AWS 서비스 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

- Amazon에서 실행되는 애플리케이션 EC2 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 보안 인증을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장하는 것보다 좋습니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행 중인 프로그램이 임시 보안 인증을 가져올 수 있습니다. 자세한 내용은 IAM 사용 설명서EC2의 IAM 역할 사용을 참조하세요.

IAM 역할 또는 IAM 사용자를 사용할지 여부를 알아보려면 IAM 사용 설명서의 IAM 역할 생성 시기(사용자 대신)를 참조하세요.

정책을 사용한 액세스 관리

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

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하기 위해 IAM 관리자는 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI또는 에서 역할 정보를 가져올 수 있습니다 AWS API.

보안 인증 기반 정책

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

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 의 여러 사용자, 그룹 및 역할에 연결할

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

리소스 기반 정책

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

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책IAM에서는 의 AWS 관리형 정책을 사용할 수 없습니다.

AWS 리소스 탐색기 는 리소스 기반 정책을 지원하지 않습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs 는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지는 않습니다.

Amazon S3 AWS WAF및 AmazonVPC은 를 지원하는 서비스의 예입니다ACLs. 에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 ACLs참조하세요.

AWS 리소스 탐색기 는 를 지원하지 않습니다ACLs.

기타 정책 타입

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

- 권한 경계 - 권한 경계는 자격 증명 기반 정책이 IAM 개체(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM엔터티에 대한 권한 경계를 참조하세요.

- 서비스 제어 정책(SCPs) - 의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. SCPs AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러 을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직의 모든 기능을 활성화하면 서비스 제어 정책(SCPs)을 모든 계정에 적용할 수 있습니다. 는 각 를 포함하여 멤버 계정의 엔터티에 대한 권한을 SCP 제한합니다 AWS 계정 루트 사용자. 조직 및 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 SCPs참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

리소스 탐색기의 작동 방식 IAM

IAM을 사용하여 액세스를 관리하려면 AWS 리소스 탐색기먼저 리소스 탐색기에서 사용할 수 있는 IAM 기능을 이해해야 합니다. 리소스 탐색기 및 기타 기능이 어떻게 AWS 서비스 작동하는지 자세히 알아보려면 IAM사용 설명서의AWS 서비스 해당 IAM 기능을 참조하십시오. IAM

주제

- Resource Explorer 자격 증명 기반 정책
- Resource Explorer 태그 기반 권한 부여
- 리소스 탐색기 IAM 역할

다른 모든 것과 AWS 서비스마찬가지로 리소스 탐색기에도 해당 작업을 사용하여 리소스와 상호 작용할 수 있는 권한이 필요합니다. 검색하려면 사용자에게 뷰에 대한 세부 정보를 검색하고 뷰를 사용하여 검색할 수 있는 권한이 있어야 합니다. 인덱스 또는 뷰를 생성하거나, 이를 수정하거나 Resource Explorer 설정을 수정하려면 추가 권한이 있어야 합니다.

해당 권한을 부여하는 IAM ID 기반 정책을 적절한 IAM 주체에게 할당하세요. Resource Explorer는 공통 권한 집합을 미리 정의하는 여러 관리형 정책을 제공합니다. 이를 주체에게 할당할 수 있습니다. IAM

Resource Explorer 자격 증명 기반 정책

IAMID 기반 정책을 사용하면 특정 리소스에 대한 허용 또는 거부 작업과 해당 작업의 허용 또는 거부 조건을 지정할 수 있습니다. Resource Explorer는 특정 작업, 리소스 및 조건 키를 지원합니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 사용 IAM설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

작업

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

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

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

Resource Explorer의 정책 작업은 작업 앞에 `resource-explorer-2` 서비스 접두사를 사용합니다. 예를 들어 리소스 탐색기 `Search` API 작업을 통해 다른 사용자에게 뷰를 사용하여 검색할 수 있는 권한을 부여하려면 해당 주도자에게 할당된 정책에 `resource-explorer-2:Search` 작업을 포함해야 합니다. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Resource Explorer는 이 서비스로 수행할 수 있는 태스크를 설명하는 고유한 작업 세트를 정의합니다. 이는 리소스 탐색기 API 작업과 일치합니다.

단일 명령문에서 여러 작업을 지정하려면 다음 예제와 같이 쉼표로 구분합니다.

```
"Action": [
      "resource-explorer-2:action1",
      "resource-explorer-2:action2"
]
```

와일드카드 문자(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `Describe`라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

```
"Action": "resource-explorer-2:Describe*"
```

Resource Explorer 작업 목록은AWS 서비스 권한 부여 참조의 AWS 리소스 탐색기에서 정의한 작업을 참조하세요.

리소스

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

`Resource`JSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. Amazon 리소스 이름 (ARN) 을 사용하여 리소스를 지정하는 것이 가장 좋습니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

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

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

뷰

기본 Resource Explorer 리소스 유형은 뷰입니다.

리소스 탐색기 뷰 리소스의 ARN 형식은 다음과 같습니다.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${unique-id}
```

리소스 탐색기 ARN 형식은 다음 예제에 나와 있습니다.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Search-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> ARN뷰용 뷰는 모든 뷰가 고유한지 확인하기 위해 끝에 고유 식별자를 포함합니다. 이렇게 하면 삭제된 이전 뷰에 대한 액세스 권한을 부여한 IAM 정책을 사용하여 이전 뷰와 이름이 같은 새 뷰에 실수로 액세스 권한을 부여하는 것을 방지할 수 있습니다. 모든 새 뷰에는 마지막에 새로운 고유 ID가 ARNs 부여되므로 재사용되지 않습니다.

형식에 대한 자세한 내용은 Amazon 리소스 이름 (ARNs) 을 참조하십시오. ARNs

IAM보안 주체에 할당된 IAM ID 기반 정책을 사용하고 보기를 로 지정합니다. Resource 이렇게 하면 하나의 뷰를 통해 하나의 보안 주체 세트에 검색 액세스 권한을 부여하고 완전히 다른 뷰를 통해 다른 보안 주체 세트에 대한 액세스 권한을 부여할 수 있습니다.

예를 들어, IAM 정책 설명에 이름이 지정된 단일 ProductionResourcesView 뷰에 권한을 부여하려면 먼저 뷰의 Amazon 리소스 이름 (ARN) 을 가져옵니다. 콘솔의 뷰 페이지를 사용하여 뷰의 세부 정보를 보거나 ListViews 작업을 호출하여 원하는 뷰 전체를 ARN 가져올 수 있습니다. 그런 다음, 하나의 뷰에 대한 정의만 수정할 수 있는 권한을 부여하는 다음 예제에 나타난 것과 같이 이를 정책 문에 포함합니다.

```
"Effect": "Allow",
"Action": "UpdateView",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
ProductionResourcesView/<unique-id>"
```

특정 계정에 속하는 모든 뷰에서 작업을 허용하려면 의 해당 부분에 와일드카드 문자 (*) 를 사용하십시오. ARN 다음 예제에서는 지정된 AWS 리전 및 계정의 모든 뷰에 검색 권한을 부여합니다.

```
"Effect": "Allow",
"Action": "Search",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*"
```

CreateView와 같은 일부 Resource Explorer 작업은 다음 예제와 같이 리소스가 아직 존재하지 않기 때문에 특정 리소스에 대해 수행되지 않습니다. 이 경우 전체 리소스에 와일드카드 문자 (*) 를 사용해야 합니다. ARN

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "*"
```

와일드카드 문자로 끝나는 경로를 지정하는 경우 승인된 경로만 사용하여 뷰를 생성하도록 CreateView 작업을 제한할 수 있습니다. 다음 예제 정책 부분에서는 보안 주체가 view/ ProductionViews/ 경로에만 뷰를 생성하도록 허용하는 방법을 보여줍니다.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/ProductionViews/*""
```

인덱스

Resource Explorer 기능에 대한 액세스를 제어하는 데 사용할 수 있는 또 다른 리소스 유형은 인덱스입니다.

인덱스와 상호 작용하는 기본 방법은 해당 리전에 인덱스를 생성하여 AWS 리전 에서 Resource Explorer를 활성화하는 것입니다. 그 후에는 뷰와 상호 작용하여 다른 거의 모든 작업을 수행할 수 있습니다.

인덱스로 수행할 수 있는 한 가지 작업은 각 리전에서 뷰를 생성할 수 있는 사용자를 제어하는 것입니다.

> **Note**
>
> 뷰를 만든 후에는 인덱스가 아닌 해당 뷰에 대해서만 다른 모든 뷰 작업을 IAM 승인합니다.
> ARN

색인에는 권한 정책에서 참조할 수 ARN있는 항목이 있습니다. 리소스 탐색기 색인의 ARN 형식은 다음과 같습니다.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${unique-id}
```

리소스 탐색기 색인의 다음 예를 참조하십시오ARN.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd22222222
```

일부 Resource Explorer 작업은 여러 리소스 유형에 대한 인증을 확인합니다. 예를 들어 CreateView작업은 리소스 탐색기에서 만든 이후와 마찬가지로 인덱스와 뷰 모두에 대해 권한을 부여합니다. ARN ARN 관리자에게 Resource Explorer 서비스를 관리할 권한을 부여하려면 `"Resource": "*"`를 사용하여 모든 리소스, 인덱스 또는 뷰에 대한 작업을 승인할 수 있습니다.

또는 지정된 Resource Explorer 리소스로만 작업할 수 있도록 보안 주체를 제한할 수 있습니다. 예를 들어 특정 지역의 리소스 탐색기 리소스로만 작업을 제한하려면 인덱스와 뷰는 모두 일치하지만 단일 지역만 호출하는 ARN 템플릿을 포함할 수 있습니다. 다음 예제에서 는 지정된 계정의 `us-west-2` 지역에서만 인덱스 또는 뷰를 모두 ARN 일치시킵니다. 의 세 번째 필드에 지역을 지정하고ARN, 모든 리소스 유형과 일치시키려면 마지막 필드에 와일드카드 문자 (*) 를 사용하십시오.

```
"Resource": "arn:aws:resource-explorer-2:us-west-2:123456789012:*
```

자세한 정보는AWS 서비스 권한 부여 참조의 AWS 리소스 탐색기에서 정의한 리소스를 참조하세요. 각 리소스에 어떤 작업을 지정할 수 있는지 알아보려면 작업 정의를 참조하십시오. ARN AWS 리소스 탐색기

조건 키

Resource Explorer는 서비스별 조건 키를 제공하지 않지만, 일부 글로벌 조건 키 사용은 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM사용 설명서의 AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

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

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

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

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 리소스에 IAM 사용자 이름이 태그가 지정된 경우에만 리소스에 대한 액세스 권한을 IAM 사용자에게 부여할 수 있습니다. 자세한 내용은 IAM사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM사용 설명서의AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

Resource Explorer와 사용할 수 있는 조건 키 목록을 보려면AWS 서비스 권한 부여 참조의 AWS 리소스 탐색기의 조건 키를 참조하세요. 조건 키와 함께 사용할 수 있는 작업 및 리소스를 알아보려면 AWS 리소스 탐색기에서 정의한 작업을 참조하세요.

예

Resource Explorer 자격 증명 기반 정책의 예를 보려면 AWS 리소스 탐색기 자격 증명 기반 정책 예제을 참조하세요.

Resource Explorer 태그 기반 권한 부여

Resource Explorer 뷰에 태그를 연결하거나 Resource Explorer에 대한 요청을 통해 태그를 전달할 수 있습니다. 태그에 근거하여 액세스를 제어하려면 `resource-explorer-2:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다. Resource Explorer 리소스 태그 지정에 대한 자세한 내용은 뷰에 태그 추가를 참조하세요. Resource Explorer에서 태그 기반 권한 부여를 사용하는 방법은 태그 기반 권한 부여를 사용하여 뷰에 대한 액세스 제어를 참조하세요.

리소스 탐색기 IAM 역할

IAM역할은 특정 권한을 AWS 계정 가진 사용자 내의 주도자입니다.

Resource Explorer에서 임시 보안 인증 사용

임시 자격 증명을 사용하여 페더레이션으로 로그인하거나, 역할을 수임하거나, 계정 간 IAM 역할을 수임할 수 있습니다. AssumeRole또는 GetFederationToken와 같은 AWS Security Token Service (AWS STS) API 작업을 호출하여 임시 보안 자격 증명을 얻을 수 있습니다.

Resource Explorer는 임시 보안 인증 사용을 지원합니다.

서비스 연결 역할

서비스 연결 역할을 사용하면 다른 서비스의 AWS 서비스 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 표시되며 서비스에서 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

Resource Explorer는 서비스 연결 역할을 사용하여 작업을 수행합니다. Resource Explorer 서비스 연결 역할에 대한 자세한 내용은 Resource Explorer에 대한 서비스 연결 역할 사용를 참조하세요.

AWS 리소스 탐색기 자격 증명 기반 정책 예제

기본적으로 역할, 그룹, 사용자와 같은 AWS Identity and Access Management(IAM) 보안 주체는 Resource Explorer 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface(AWS CLI) 또는 AWS API를 사용해 태스크를 수행할 수 없습니다. IAM 관리자는 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 보안 주체에 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 보안 주체에 이러한 정책을 할당해야 합니다.

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 사용자(콘솔)에 권한 추가의 지침을 따르세요.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- Resource Explorer 콘솔 사용
- 태그를 기반으로 뷰에 액세스 권한 부여
- 태그를 기반으로 뷰를 생성할 수 있는 액세스 권한 부여
- 보안 주체가 자신이 권한을 볼 수 있도록 허용

정책 모범 사례

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

- AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 관리형 정책은 AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 특정 AWS 서비스(예: AWS CloudFormation)를 통해 사용되는 경우에만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer policy validation(IAM Access Analyzer 정책 검증)을 참조하세요.
- 다중 인증(MFA) 필요 – AWS 계정 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 설정합니다. API 작업을 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

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

Resource Explorer 콘솔 사용

보안 주체가 AWS 리소스 탐색기 콘솔에서 검색하려면 최소 권한 세트가 있어야 합니다. 최소 필수 권한으로 보안 인증 정보 기반 정책을 만들지 않으면 Resource Explorer 콘솔이 계정의 보안 주체에 대해 의도한 대로 작동하지 않습니다.

`AWSResourceExplorerReadOnlyAccess`라는 이름이 지정된 AWS 관리형 정책을 사용하면 Resource Explorer 콘솔을 사용해 계정의 모든 뷰를 사용하여 검색할 수 있는 권한을 부여할 수 있습니다. 단일 뷰만 사용하여 검색할 수 있는 권한을 부여하려면 검색을 위해 Resource Explorer 뷰에 대한 액세스 권한 부여 및 다음 두 섹션의 및 예를 참조하세요.

AWS CLI 또는 AWS API만 호출하는 보안 주체에는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신 보안 주체가 수행해야 하는 API 작업과 일치하는 작업에만 액세스 권한을 부여하도록 선택할 수 있습니다.

태그를 기반으로 뷰에 액세스 권한 부여

이 예제에서는 계정의 보안 주체에게 AWS 계정의 Resource Explorer 뷰에 대한 액세스 권한을 부여하려고 합니다. 이렇게 하려면 Resource Explorer에서 검색할 수 있도록 하려는 보안 주체에 IAM 자격 증명 기반 정책을 할당하세요. 다음 예제 IAM 정책은 호출 보안 주체에 연결된 `Search-Group` 태그가 요청에 사용된 뷰에 연결된 동일한 태그의 값과 정확히 일치하는 모든 요청에 대한 액세스 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:*:*:view/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Search-Group": "${aws:PrincipalTag/
Search-Group}"}
            }
        }
    ]
}
```

이 정책을 계정의 IAM 보안 주체에 할당할 수 있습니다. `Search-Group=A` 태그가 있는 보안 주체가 Resource Explorer 뷰를 사용하여 검색을 시도하는 경우 뷰에도 태그가 `Search-Group=A`로 지정되어야 합니다. 그렇지 않으면 보안 주체의 액세스가 거부됩니다. 조건 키 이름은 대소문자를 구분하지 않기 때문에 태그 키 `Search-Group`는 `Search-group` 및 `search-group` 모두와 일치합니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

> **Important**
>
> AWS Management Console의 통합 검색 결과에서 리소스를 보려면 보안 주체에게 애그리게이터 인덱스가 포함된 AWS 리전의 기본 뷰에 대한 두 가지 `GetView` 및 `Search` 권한이 모두 있어야 합니다. 이러한 권한을 부여하는 가장 간단한 방법은 빠른 설정 또는 고급 설정을 사용하여 Resource Explorer를 활성화했을 때 뷰에 연결된 기본 리소스 기반 권한을 그대로 두는 것입니다.

이 시나리오에서는 민감한 리소스를 필터링하도록 기본 뷰를 설정한 다음 이전 예제에서 설명한 대로 태그 기반 액세스를 허용하는 추가 뷰를 설정하는 것을 고려할 수 있습니다.

태그를 기반으로 뷰를 생성할 수 있는 액세스 권한 부여

이 예제에서는 인덱스와 동일한 태그가 지정된 보안 주체만 인덱스가 포함된 AWS 리전에서 뷰를 생성할 수 있도록 허용하려고 합니다. 이렇게 하려면 보안 주체가 뷰를 통해 검색할 수 있도록 자격 증명 기반 권한을 생성하세요.

이제 뷰를 생성할 수 있는 권한을 부여할 준비가 되었습니다. 이 예제의 정책 문을 적절한 보안 주체에게 Search 권한을 부여하는 데 사용하는 것과 동일한 권한 정책에 추가할 수 있습니다. 작업은 뷰와 연결할 작업 및 인덱스를 호출하는 보안 주체에 연결된 태그에 따라 허용되거나 거부됩니다. 다음 예제 IAM 정책은 호출자의 보안 주체에 연결된 `Allow-Create-View` 태그의 값이 뷰가 생성된 리전에 있는 인덱스에 연결된 동일한 태그의 값과 정확히 일치하지 않는 경우 뷰 생성 요청을 거부합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "resource-explorer-2:CreateView",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {"aws:ResourceTag/Allow-Create-View":
 "${aws:PrincipalTag/Allow-Create-View}"}
            }
        }
    ]
}
```

보안 주체가 자신이 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI나 AWS API를 사용하여 프로그래밍 방식으로 이 태스크를 완료할 수 있는 권한이 포함됩니다.

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

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Organizations 및 리소스 탐색기에 대한 서비스 제어 정책 예시

AWS 리소스 탐색기 서비스 제어 정책 (SCP) 을 지원합니다. SCP는 조직 내 구성 요소에 연결하여 해당 조직 내의 권한을 관리하는 정책입니다. SCP는 SCP를 연결하는 요소에 속한 조직의 모든 AWS 계정 사람에게 적용됩니다. SCP는 조직의 모든 계정에 사용 가능한 최대 권한을 중앙에서 제어합니다. 이를 통해 조직의 액세스 제어 AWS 계정 지침을 준수할 수 있습니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.

사전 조건

SCP를 사용하려면 먼저 다음 사항을 수행해야 합니다.

- 조직 내에서 모든 기능을 활성화합니다. 자세한 내용은AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.
- 조직에 대해 SCP를 활성화합니다. 자세한 내용은AWS Organizations 사용 설명서의 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

다음은 ABAC(속성 기반 액세스 제어)를 사용하여 Resource Explorer의 관리 작업에 대한 액세스를 제어하는 방법을 나타낸 예제입니다. 이 예제 정책은 요청을 수행하는 IAM 보안 주체가 `ResourceExplorerAdmin=TRUE`로 태그를 지정되지 않은 한 검색에 필요한 두 가지 `resource-explorer-2:Search` 및 `resource-explorer-2:GetView` 권한을 제외한 모든 Resource Explorer 작업에 대한 액세스를 거부합니다. Resource Explorer에서 ABAC를 사용하는 방법에 대한 자세한 내용은 태그 기반 권한 부여를 사용하여 뷰에 대한 액세스 제어를 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView""
      ],
```

```
      "Resource": [
        "*"
      ],
      "Condition": {
          "StringNotEqualsIgnoreCase": {"aws:PrincipalTag/ResourceExplorerAdmin":
 "TRUE"}
      }
    ]
}
```

AWS 에 대한 관리형 정책 AWS 리소스 탐색기

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

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

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

리소스 탐색기 권한을 포함하는 일반 AWS 관리형 정책

- AdministratorAccess— 리소스에 대한 전체 액세스 권한을 AWS 서비스 부여합니다.
- ReadOnly액세스 — 리소스에 대한 읽기 전용 액세스 권한을 AWS 서비스 부여합니다.
- ViewOnly액세스 - 리소스 및 기본 메타데이터를 볼 수 있는 권한을 부여합니다. AWS 서비스

> **Note**
>
> `ViewOnlyAccess` 정책에 포함된 Resource Explorer `Get*` 권한은 리전에 하나의 인덱스와 하나의 기본 뷰만 포함될 수 있기 때문에 단일 값만 반환하지만 `List` 권한과 유사하게 수행됩니다.

AWS 리소스 탐색기의 관리형 정책

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

AWS 관리형 정책: AWSResourceExplorerFullAccess

`AWSResourceExplorerFullAccess` 정책을 IAM 자격 증명에 할당할 수 있습니다.

이 정책은 Resource Explorer 서비스에 대한 전체 관리 제어를 허용하는 권한을 부여합니다. 계정의 AWS 리전 에서 Resource Explorer를 활성화하고 관리하는 데 관련된 모든 작업을 수행할 수 있습니다.

권한 세부 정보

이 정책에는 리소스 탐색기 켜기/끄기, 계정에 대한 애그리게이터 인덱스 만들기 또는 삭제 AWS 리전, 보기 만들기, 업데이트, 삭제, 검색 등 리소스 탐색기의 모든 작업을 허용하는 권한이 포함됩니다. 이 정책에는 Resource Explorer에 포함되지 않은 권한도 포함되어 있습니다.

- `ec2:DescribeRegions` – Resource Explorer가 계정의 리전에 대한 세부 정보에 액세스할 수 있도록 허용합니다.
- `ram:ListResources` – Resource Explorer가 리소스가 속한 리소스 공유를 나열할 수 있도록 허용합니다.
- `ram:GetResourceShares` – Resource Explorer가 사용자가 소유하거나 공유한 리소스 공유에 대한 세부 정보를 식별할 수 있도록 허용합니다.
- `iam:CreateServiceLinkedRole` – 첫 번째 인덱스를 생성하여 Resource Explorer를 활성화할 때 Resource Explorer가 필요한 서비스 연결 역할을 생성할 수 있도록 허용합니다.
- `organizations:DescribeOrganization` – Resource Explorer가 조직에 대한 정보에 액세스할 수 있도록 허용합니다.

이 AWS 관리형 정책의 최신 버전을 보려면 `AWSResourceExplorerFullAccess` 관리형 정책 참조 AWS 안내서를 참조하십시오.

AWS 관리형 정책: AWSResourceExplorerReadOnlyAccess

`AWSResourceExplorerReadOnlyAccess` 정책을 IAM 자격 증명에 할당할 수 있습니다.

이 정책은 사용자에게 리소스를 검색할 수 있는 기본 검색 액세스를 허용하는 읽기 전용 권한을 부여합니다.

권한 세부 정보

이 정책에는 사용자가 Resource Explorer `Get*`, `List*`, `Search` 작업을 수행하여 Resource Explorer 구성 요소 및 구성 설정에 대한 정보를 볼 수는 있지만 사용자가 이를 변경할 수는 없는 권한이 포함되어 있습니다. 사용자는 검색도 할 수 있습니다. 이 정책에는 Resource Explorer에 포함되지 않은 두 가지 권한도 포함되어 있습니다.

- `ec2:DescribeRegions` – Resource Explorer가 계정의 리전에 대한 세부 정보에 액세스할 수 있도록 허용합니다.
- `ram:ListResources` – Resource Explorer가 리소스가 속한 리소스 공유를 나열할 수 있도록 허용합니다.
- `ram:GetResourceShares` – Resource Explorer가 사용자가 소유하거나 공유한 리소스 공유에 대한 세부 정보를 식별할 수 있도록 허용합니다.
- `organizations:DescribeOrganization` – Resource Explorer가 조직에 대한 정보에 액세스할 수 있도록 허용합니다.

이 AWS 관리형 정책의 최신 버전을 보려면 `AWSResourceExplorerReadOnlyAccess` 관리형 정책 참조 안내서를 참조하십시오.AWS

AWS 관리형 정책: AWSResourceExplorerServiceRolePolicy

`AWSResourceExplorerServiceRolePolicy`을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Resource Explorer가 사용자를 대신하여 작업을 수행할 수 있도록 해 주는 서비스 연결 역할에만 연결할 수 있도록 허용합니다. 자세한 정보는 Resource Explorer에 대한 서비스 연결 역할 사용을 참조하세요.

이 정책은 Resource Explorer가 리소스에 대한 정보를 검색하는 데 필요한 권한을 부여합니다. 리소스 탐색기는 등록한 각 AWS 리전 항목에서 유지 관리하는 색인을 채웁니다.

이 AWS 관리형 정책의 최신 버전을 보려면 IAM 콘솔을 참조하십시오`AWSResourceExplorerServiceRolePolicy`.

AWS 관리형 정책: AWSResourceExplorerOrganizationsAccess

`AWSResourceExplorerOrganizationsAccess`를 IAM 자격 증명에 할당할 수 있습니다.

이 정책은 Resource Explorer에 관리자 권한을 부여하고 이 AWS 서비스 액세스를 지원하는 다른 사용자에게는 읽기 전용 권한을 부여합니다. AWS Organizations 관리자는 콘솔에서 다중 계정 검색을 설정하고 관리하려면 이러한 권한이 필요합니다.

권한 세부 정보

이 정책에는 관리자가 조직에 대한 다중 계정 검색을 설정할 수 있는 권한이 포함되어 있습니다.

- `ec2:DescribeRegions` – Resource Explorer가 계정의 리전에 대한 세부 정보에 액세스할 수 있도록 허용합니다.
- `ram:ListResources` – Resource Explorer가 리소스가 속한 리소스 공유를 나열할 수 있도록 허용합니다.
- `ram:GetResourceShares` – Resource Explorer가 사용자가 소유하거나 공유한 리소스 공유에 대한 세부 정보를 식별할 수 있도록 허용합니다.
- `organizations:ListAccounts` – Resource Explorer가 조직 내 계정을 식별할 수 있도록 허용합니다.
- `organizations:ListRoots` – Resource Explorer가 조직 내 루트 계정을 식별할 수 있도록 허용합니다.
- `organizations:ListOrganizationalUnitsForParent` – Resource Explorer가 상위 조직 단위 또는 루트의 조직 단위(OU)를 식별할 수 있도록 허용합니다.
- `organizations:ListAccountsForParent` – Resource Explorer가 지정된 대상 루트 또는 OU에 포함된 조직의 계정을 식별할 수 있도록 허용합니다.
- `organizations:ListDelegatedAdministrators`— 리소스 탐색기에서 이 조직에서 위임된 관리자로 지정된 AWS 계정을 식별할 수 있습니다.
- `organizations:ListAWSServiceAccessForOrganization`— 리소스 탐색기에서 조직과 통합할 수 AWS 서비스 있는 목록의 목록을 식별할 수 있습니다.
- `organizations:DescribeOrganization` – Resource Explorer가 사용자 계정이 속한 조직에 대한 정보를 검색할 수 있도록 허용합니다.
- `organizations:EnableAWSServiceAccess`— 리소스 탐색기를 사용하여 AWS 서비스 (에서 지정한 서비스`ServicePrincipal`) 를 다음과 통합할 수 AWS Organizations있습니다.
- `organizations:DisableAWSServiceAccess`— 리소스 탐색기가 AWS 서비스 (에서 지정한 서비스 ServicePrincipal) 와 통합을 비활성화할 수 있도록 AWS Organizations합니다.
- `organizations:RegisterDelegatedAdministrator`— 리소스 탐색기에서 지정된 멤버 계정으로 조직의 지정된 AWS 서비스 기능을 관리할 수 있도록 합니다.

- `organizations:DeregisterDelegatedAdministrator`— 리소스 탐색기에서 지정된 구성원을 지정된 구성원의 AWS 계정 위임 관리자로 제거할 수 있습니다. AWS 서비스
- `iam:GetRole` – Resource Explorer가 역할의 경로, GUID, ARN 및 역할을 수임할 수 있는 권한을 부여하는 역할의 신뢰 정책을 포함하여 지정된 역할에 대한 정보를 검색할 수 있도록 허용합니다.
- `iam:CreateServiceLinkedRole` – 첫 번째 인덱스를 생성하여 Resource Explorer를 활성화할 때 Resource Explorer가 필요한 서비스 연결 역할을 생성할 수 있도록 허용합니다.

이 AWS 관리형 정책의 최신 버전을 보려면 IAM `AWSResourceExplorerOrganizationsAccess` 콘솔을 참조하십시오.

리소스 탐색기의 AWS 관리형 정책 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후 리소스 탐색기의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Resource Explorer 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSResourceExplorerServiceRolePolicy- 추가 리소스 유형을 볼 수 있도록 정책 권한이 업데이트되었습니다.	리소스 탐색기는 서비스 연결 역할 정책에 리소스 탐색기에서 추가 리소스 유형을 볼 수 `AWSResourceExplorerServiceRolePolicy` 있는 권한을 추가했습니다. • `apprunner:ListVpcConnectors` • `backup:ListReportPlans` • `emr-serverless:ListApplications` • `events:ListEventBuses` • `geo:ListPlaceIndexes` • `geo:ListTrackers`	2023년 12월 12일

변경 사항	설명	날짜
	• greengrass:ListComponents • greengrass:ListComponentVersions • iot:ListRoleAliases • iottwinmaker:ListComponentTypes • iottwinmaker:ListEntities • iottwinmaker:ListScenes • kafka:ListConfigurations • kms:ListKeys • kinesisanalytics:ListApplications • lex:ListBots • lex:ListBotAliases • mediapackage-vod:ListPackagingConfigurations • mediapackage-vod:ListPackagingGroups • mq:ListBrokers • personalize:ListDatasetGroups • personalize:ListDatasets • personalize:ListSchemas	

변경 사항	설명	날짜
	• `route53:ListHealthChecks` • `route53:ListHostedZones` • `secretsmanager:ListSecrets`	
새 관리형 정책	리소스 탐색기에 다음과 같은 AWS 관리형 정책이 추가되었습니다. • AWSResourceExplorerOrganizationsAccess	2023년 11월 14일
관리형 정책 업데이트	리소스 탐색기는 다중 계정 검색을 지원하도록 다음과 같은 AWS 관리형 정책을 업데이트했습니다. • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess	2023년 11월 14일

변경 사항	설명	날짜
AWSResourceExplorerServiceRolePolicy—Organizations를 통한 다중 계정 검색을 지원하도록 정책 업데이트	Resource Explorer는 Organizations에 대한 다중 계정 검색을 지원할 수 있도록 허용하는 서비스 연결 역할 정책 AWSResourceExplorerServiceRolePolicy 에 권한을 추가했습니다. • organizations:ListAWSServiceAccessForOrganization • organizations:DescribeAccount • organizations:DescribeOrganization • organizations:ListAccounts • organizations:ListDelegatedAdministrators	2023년 11월 14일

변경 사항	설명	날짜
AWSResourceExplorerServiceRolePolicy— 추가 리소스 유형을 지원하도록 정책이 업데이트되었습니다.	Resource Explorer가 서비스가 다음 리소스 유형을 인덱싱할 수 있도록 허용하는 서비스 연결 역할 정책 AWSResourceExplorerServiceRolePolicy 에 권한을 추가했습니다. • accessanalyzer:analyzer • acmpca:certificateauthority • amplify:app • amplify:backendenvironment • amplify:branch • amplify:domainassociation • amplifyuibuilder:component • amplifyuibuilder:theme • appintegrations:eventintegration • apprunner:service • appstream:appblock • appstream:application • appstream:fleet • appstream:imagebuilder • appstream:stack • appsync:graphqlapi • aps:rulegroupsnamespace • aps:workspace • apigateway:restapi • apigateway:deployment • athena:datacatalog	2023년 10월 17일

변경 사항	설명	날짜
	• athena:workgroup • autoscaling:autoscalinggroup • backup:backupplan • batch:computeenvironment • batch:jobqueue • batch:schedulingpolicy • cloudformation:stack • cloudformation:stackset • cloudfront:fieldlevelencryptionconfig • cloudfront:fieldlevelencryptionprofile • cloudfront:originaccesscontrol • cloudtrail:trail • codeartifact:domain • codeartifact:repository • codecommit:repository • codeguruprofiler:profilinggroup • codestarconnections:connection • databrew:dataset • databrew:recipe • databrew:ruleset • detective:graph • directoryservices:directory • ec2:carriergateway • ec2:verifiedaccessendpoint	

변경 사항	설명	날짜
	• ec2:verifiedaccessgroup • ec2:verifiedaccessinstance • ec2:verifiedaccesstrustprovider • ecr:repository • elasticache:cachesecuritygroup • elasticfilesystem:accesspoint • events:rule • evidently:experiment • evidently:feature • evidently:launch • evidently:project • finspace:environment • firehose:deliverystream • faultinjectionsimulator:experimenttemplate • forecast:datasetgroup • forecast:dataset • frauddetector:detector • frauddetector:entitytype • frauddetector:eventtype • frauddetector:label • frauddetector:outcome • frauddetector:variable • gamelift:alias • globalaccelerator:accelerator	

변경 사항	설명	날짜
	• globalaccelerator:endpointgroup • globalaccelerator:listener • glue:database • glue:job • glue:table • glue:trigger • greengrass:group • healthlake:fhirdatastore • iam:virtualmfadevice • imagebuilder:componentbuildversion • imagebuilder:component • imagebuilder:containerrecipe • imagebuilder:distributionconfiguration • imagebuilder:imagebuildversion • imagebuilder:imagepipeline • imagebuilder:imagerecipe • imagebuilder:image • imagebuilder:infrastructureconfiguration • iot:authorizer • iot:jobtemplate • iot:mitigationaction • iot:provisioningtemplate • iot:securityprofile • iot:thing	

변경 사항	설명	날짜
	• iot:topicruledestination • iotanalytics:channel • iotanalytics:dataset • iotanalytics:datastore • iotanalytics:pipeline • iotevents:alarmmodel • iotevents:detectormodel • iotevents:input • iotsitewise:assetmodel • iotsitewise:asset • iotsitewise:gateway • iottwinmaker:workspace • ivs:channel • ivs:streamkey • kafka:cluster • kinesisvideo:stream • lambda:alias • lambda:layerversion • lambda:layer • lookoutmetrics:alert • lookoutvision:project • mediapackage:channel • mediapackage:origi nendpoint • mediatailor:playbackconfigu ration • memorydb:acl • memorydb:cluster • memorydb:parametergroup	

변경 사항	설명	날짜
	• memorydb:user • mobiletargeting:app • mobiletargeting:segment • mobiletargeting:template • networkfirewall:firewallpolicy • networkfirewall:firewall • networkmanager:glo balnetwork • networkmanager:device • networkmanager:link • networkmanager:attachment • networkmanager:cor enetwork • panorama:package • qldb:journalkinesisstreamsf orledger • qldb:ledger • rds:bluegreendeployment • refactorspaces:application • refactorspaces:environment • refactorspaces:route • refactorspaces:service • rekognition:project • resiliencehub:app • resiliencehub:resiliencypol icy • resourcegroups:group • route53:recoverygroup • route53:resourceset • route53:firewalldomain	

변경 사항	설명	날짜
	• route53:firewallrulegroup • route53:resolverendpoint • route53:resolverrule • sagemaker:model • sagemaker:notebook instance • signer:signingprofile • ssmincidents:responseplan • ssm:inventoryentry • ssm:resourcedatasync • states:activity • timestream:database • wisdom:assistant • wisdom:assistantassociation • wisdom:knowledgebase	

변경 사항	설명	날짜
AWSResourceExplorerServiceRolePolicy— 추가 리소스 유형을 지원하도록 정책이 업데이트되었습니다.	Resource Explorer가 서비스가 다음 리소스 유형을 인덱싱할 수 있도록 허용하는 서비스 연결 역할 정책 AWSResourceExplorerServiceRolePolicy 에 권한을 추가했습니다. • codebuild:project • codepipeline:pipeline • cognito:identitypool • cognito:userpool • ecr:repository • efs:filesystem • elasticbeanstalk:application • elasticbeanstalk:applicationversion • elasticbeanstalk:environment • iot:policy • iot:topicrule • stepfunctions:statemachine • s3:bucket	2023년 8월 1일

변경 사항	설명	날짜
AWSResourceExplorerServiceRolePolicy— 추가 리소스 유형을 지원하도록 정책이 업데이트되었습니다.	Resource Explorer가 서비스가 다음 리소스 유형을 인덱싱할 수 있도록 허용하는 서비스 연결 역할 정책 AWSResourceExplorerServiceRolePolicy 에 권한을 추가했습니다. • elasticache:cluster • elasticache:globalreplicationgroup • elasticache:parametergroup • elasticache:replicationgroup • elasticache:reserved-instance • elasticache:snapshot • elasticache:subnetgroup • elasticache:user • elasticache:usergroup • lambda:code-signing-config • lambda:event-source-mapping • sqs:queue	2023년 3월 7일

변경 사항	설명	날짜
새 관리형 정책	리소스 탐색기에 다음과 같은 AWS 관리형 정책이 추가되었습니다. • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess • AWSResourceExplorerServiceRolePolicy	2022년 11월 7일
Resource Explorer에서 변경 사항 추적 시작	리소스 탐색기가 AWS 관리형 정책의 변경 내용을 추적하기 시작했습니다.	2022년 11월 7일

Resource Explorer에 대한 서비스 연결 역할 사용

AWS 리소스 탐색기 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 리소스 탐색기에 직접 연결된 고유한 IAM 역할 유형입니다. 서비스 연결 역할은 Resource Explorer에서 미리 정의되며 서비스가 사용자를 대신하여 다른 사람을 호출하는 데 필요한 모든 권한을 포함합니다. AWS 서비스

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Resource Explorer를 더 쉽게 구성할 수 있습니다. Resource Explorer에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Resource Explorer만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 모두 포함되며 이 권한 정책은 다른 엔티티에 할당할 수 없습니다. IAM

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 IAM사용 IAM 설명서에서 함께 작동하는AWS 서비스를 참조하십시오. 거기에서 서비스 연결 역할 열에 예라고 표시된 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Resource Explorer에 대한 서비스 연결 역할 권한

Resource Explorer에서는 `AWSServiceRoleForResourceExplorer`라는 이름이 지정된 서비스 연결 역할을 사용합니다. 이 역할은 사용자를 대신하여 리소스 탐색기 서비스에 리소스와 AWS

CloudTrail 이벤트를 조회하고 검색을 지원하기 위해 해당 리소스를 인덱싱할 수 있는 권한을 부여합니다. AWS 계정

`AWSServiceRoleForResourceExplorer` 서비스 연결 역할은 다음 서비스 보안 주체가 있는 서비스만 신뢰하여 역할을 수임합니다.

- `resource-explorer-2.amazonaws.com`

이름이 지정된 역할 권한 정책을 AWSResourceExplorerServiceRolePolicy 사용하면 Resource Explorer에서 지원되는 AWS 리소스의 리소스 이름과 속성을 검색할 수 있는 읽기 전용 액세스가 허용됩니다. Resource Explorer가 지원하는 서비스와 리소스를 보려면 Resource Explorer로 검색할 수 있는 리소스 유형을 참조하세요. IAM콘솔에서 `AWSResourceExplorerServiceRolePolicy` 정책을 보면 이 역할이 수행할 수 있는 모든 작업의 전체 목록을 볼 수 있습니다.

보안 주체는 사용자, 그룹 또는 역할과 같은 IAM 엔티티입니다. Resource Explorer가 계정의 첫 번째 리전에 인덱스를 생성할 때 자동으로 서비스 연결 역할을 생성하도록 허용하면 작업을 수행하는 보안 주체는 Resource Explorer 인덱스를 생성하는 데 필요한 권한만 있으면 됩니다. 를 사용하여 IAM 수동으로 서비스 연결 역할을 만들려면 작업을 수행하는 주도자에게 서비스 연결 역할을 만들 수 있는 권한이 있어야 합니다. 자세한 내용은 사용 설명서의 서비스 연결 역할 권한을 참조하십시오. IAM

Resource Explorer에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 에서 리소스 탐색기를 켜거나 또는 를 사용하여 계정의 첫 AWS 리전 번째 탐색기를 실행하면 CreateIndex리소스 탐색기가 서비스 연결 역할을 자동으로 생성합니다. AWS Management Console AWS CLI AWS API

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 계정의 첫 번째 지역을 방문하면 RegisterResourceExplorer리소스 탐색기가 서비스 연결 역할을 다시 생성합니다.

Resource Explorer에 대한 서비스 연결 역할 편집

Resource Explorer에서는 `AWSServiceRoleForResourceExplorer` 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 를 사용하여 역할에 대한 설명을 편집할 수 있습니다. IAM 자세한 내용은 사용 IAM설명서의 서비스 연결 역할 편집을 참조하십시오.

Resource Explorer에 대한 서비스 연결 역할 삭제

IAM콘솔 AWS CLI, 또는 를 사용하여 서비스 연결 역할을 수동으로 삭제할 수 있습니다. AWS API 이렇게 하려면 먼저 계정의 모든 AWS 리전 계정에서 리소스 탐색기 색인을 제거한 다음 서비스 연결 역할을 수동으로 삭제해야 합니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Resource Explorer 서비스가 해당 역할을 사용 중이면 삭제에 실패할 수 있습니다. 그런 경우 모든 리전의 모든 인덱스가 삭제되었는지 확인한 다음 몇 분 기다렸다가 작업을 다시 시도하세요.

를 사용하여 서비스 연결 역할을 수동으로 삭제하려면 IAM

IAM콘솔 AWS CLI, 또는 를 AWS API 사용하여 `AWSServiceRoleForResourceExplorer` 서비스 연결 역할을 삭제합니다. 자세한 내용은 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오. IAM

Resource Explorer 서비스 연결 역할을 지원하는 리전

Resource Explorer에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은Amazon Web Services 일반 참조의 AWS 서비스 엔드포인트를 참조하세요.

AWS 리소스 탐색기 권한 문제 해결

다음 정보를 사용하면 리소스 탐색기 및 AWS Identity and Access Management (IAM) 작업 시 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

주제

- Resource Explorer에서 작업을 수행할 권한이 없음
- 외부 사용자가 내 리소스 탐색기 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

Resource Explorer에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 이 작업을 시도하는 데 사용한 보안 인증 정보를 제공한 사람입니다.

예를 들어, IAM 역할 `MyExampleRole`가 콘솔을 사용하여 뷰에 대한 세부 정보를 보려고 하지만 `resource-explorer-2:GetView` 권한이 없는 경우 다음 오류가 발생합니다.

```
User: arn:aws:iam::123456789012:role/MyExampleRole is not authorized to perform:
 resource-explorer-2:GetView on resource: arn:aws:resource-explorer-2:us-
east-1:123456789012:view/EC2-Only-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

이 경우 역할을 사용하는 사용자는 관리자에게 `resource-explorer-2:GetView` 작업을 사용하여 뷰에 액세스할 수 있도록 역할의 권한 정책을 업데이트하도록 요청해야 합니다.

외부 사용자가 내 리소스 탐색기 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

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

자세히 알아보려면 다음을 참조하십시오.

- Resource Explorer에서 이러한 기능을 지원하는지 여부를 알아보려면 리소스 탐색기의 작동 방식 IAM를 참조하세요.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 페더레이션)을 참조하십시오.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

의 데이터 보호 AWS 리소스 탐색기

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS 리소스 탐색기. 이 모델에 설명된 대로 AWS 는 모든 를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 섹션을 FAQ참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 책임 공유 모델 및 GDPR 블로그 게시물을 참조하세요.

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

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 FIPS 를 AWS 통해 에 액세스할 때 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 API사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 Resource Explorer 또는 콘솔, 또는 를 사용하는 기타 AWS 서비스 에서 작업하는 경우가 포함됩니다API AWS CLI AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL를 제공하는 경우 해당 서버에 대한 요청을 검증URL하기 위해 에 보안 인증 정보를 포함하지 않는 것이 좋습니다.

저장 중 암호화

Resource Explorer에서 저장하는 데이터에는 고객이 ARNs 사용하는 리소스 및 관련 리소스의 인덱싱된 목록과 리소스에 액세스하는 뷰가 포함됩니다.

이 데이터는 256비트 AWS Key Management Service 키(-256-AWS KMS)를 사용하여 Galois 카운터 모드()에서 고급 암호화 표준()을 구현하는 () 대칭 암호화 키를 사용하여 저장 시 암호화됩니다 AESGCM. AES GCM

전송 중 암호화

고객 요청 및 모든 관련 데이터는 전송 중 Transport Later Security(TLS) 1.2 이상을 사용하여 암호화됩니다. 모든 Resource Explorer 엔드포인트는 전송 중인 데이터를 HTTPS 암호화할 수 있습니다.

Resource Explorer 서비스 엔드포인트 목록은AWS 일반 참조의 AWS 리소스 탐색기 엔드포인트 및 할당량을 참조하세요.

AWS 리소스 탐색기의 규정 준수 확인

AWS 서비스가 특정 규정 준수 프로그램의 범위에 포함되는지 알아보려면 규정 준수 프로그램 제공 범위의 AWS 서비스를 참조하세요. 일반적인 정보는 AWS규정 준수 프로그램을 참조하세요.

AWS Artifact을(를) 사용하여 제3자 감사 보고서를 다운로드할 수 있습니다. 자세한 정보는 AWS Artifact 사용 설명서의 AWS Artifact의 보고서 다운로드를 참조하세요.

Resource Explorer 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다. AWS는 규정 준수를 지원할 다음과 같은 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서: 이 배포 안내서에서는 아키텍처 고려 사항에 관해 설명하고 AWS에서 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services에서 HIPAA 보안 및 규정 준수 기술 백서 설계 - 이 백서는 기업에서 AWS를 사용하여 HIPAA를 준수하는 애플리케이션을 만드는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스에 HIPAA 자격이 있는 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조 섹션을 참조하십시오.

- AWS 규정 준수 리소스: 고객 조직이 속한 산업 및 위치에 적용될 수 있는 워크북 및 가이드 콜렉션입니다.
- AWS Config 개발자 가이드의 규칙을 사용하여 리소스 평가: AWS Config를 사용하여 리소스 구성이 내부 사례, 업계 지침, 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub: 이 AWS 서비스는 보안 산업 표준 및 모범 사례 규정 준수 여부를 확인하는 데 도움이 되도록 AWS 내 보안 상태를 종합적으로 보여줍니다.

AWS 리소스 탐색기의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장

애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

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

의 인프라 보안 AWS 리소스 탐색기

매니지드 서비스로서 AWS 글로벌 네트워크 보안으로 AWS 리소스 탐색기 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 리소스 탐색기에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안 (TLS). TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- (임시 디피-헬만) 또는 (타원 곡선 임시 디피-헬만PFS) 와 같이 완벽한 순방향 기밀성 DHE () 을 갖춘 암호 제품군. ECDHE Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 보안 주체와 연결된 비밀 액세스 키를 사용하여 요청에 서명해야 합니다. IAM 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

AWS 글로벌 네트워크 보안 절차에 대한 자세한 내용은 Amazon Web Services: 보안 프로세스 개요 백서를 참조하십시오.

AWS 리소스 탐색기 모니터링

AWS 리소스 탐색기 및 다른 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하려면 모니터링이 중요합니다. AWS는 Resource Explorer를 모니터링하고, 이상이 있을 때 이를 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail은 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 리소스 탐색기 API 호출 로깅 및 AWS CloudTrail 사용 설명서를 참조하세요.

AWS CloudTrail을 사용하여 AWS 리소스 탐색기 API 호출 로깅

AWS 리소스 탐색기은 Resource Explorer에서 사용자, 역할, 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Resource Explorer에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Resource Explorer 콘솔로부터의 호출과 Resource Explorer API 작업에 대한 코드 호출이 포함됩니다.

추적을 생성하면 Resource Explorer에 대한 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Resource Explorer에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Resource Explorer 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. Resource Explorer에서 활동이 발생하면, 해당 활동이 이벤트 기록에 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트 로그에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

> **Important**
>
> 이벤트 소스 = resource-explorer-2.amazonaws.com을 검색하면 모든 Resource Explorer 이벤트를 찾을 수 있습니다.

Resource Explorer에 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 AWS CloudTrail 사용 설명서에서 다음 주제를 참조하십시오.

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

모든 Resource Explorer 작업은 CloudTrail에서 로깅되고 AWS 리소스 탐색기 API 참조에 기록됩니다. 예를 들어 `CreateIndex`, `DeleteIndex` 및 `UpdateIndex` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

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

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

> **Important**
>
> 보안상의 이유로 CloudTrail 추적 항목에서 `Tags`, `Filters`, `QueryString` 값이 모두 편집되었습니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Resource Explorer 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.

주제

- CreateIndex
- DeleteIndex
- UpdateIndexType
- 검색
- CreateView
- DeleteView
- DisassociateDefaultView

CreateIndex

다음은 `CreateIndex` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예제입니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-166EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-166EXAMPLE",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:13:59Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-index",
    "requestParameters": {
        "ClientToken": "792ee665-58af-423c-bfdb-d7c9aEXAMPLE"
    },
    "responseElements": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "State": "CREATING",
        "CreatedAt": "2022-08-23T19:13:59.775Z"
    },
    "requestID": "a193afe9-17ff-4f30-ae0a-73bb0EXAMPLE",
    "eventID": "2ec50598-4de6-474d-bd0e-f5c00EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


DeleteIndex

다음은 `DeleteIndex` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예제입니다.

> **Note**
>
> 또한 이 작업을 수행하면 해당 리전의 계정에 대한 모든 뷰가 비동기적으로 삭제되므로 삭제된 각 뷰에 대해 `DeleteView` 이벤트가 발생합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:My-Role-Name",
        "arn": "arn:aws:sts::123456789012:assumed-role/My-Admin-Role/My-Delegated-
Role",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/My-Admin-Role",
                "accountId": "123456789012",
                "userName": "My-Admin-Role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T18:33:06Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:04:06Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-index",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "State": "DELETING",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "requestID": "d7d80bd2-cd2d-47fb-88d6-5133aEXAMPLE",
```

```
    "eventID": "675eab39-c514-4d32-989d-0ea98EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

UpdateIndexType

다음은 인덱스를 LOCAL에서 AGGREGATOR로 승격시키는 UpdateIndexType 작업을 보여주는 CloudTrail 로그 항목을 나타낸 예제입니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:21:18Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "UpdateIndexType",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
```

```
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.update-index-type",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "Type": "AGGREGATOR"
    },
    "responseElements": {
        "Type": "AGGREGATOR",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "LastUpdatedAt": "2022-08-23T19:21:17.924Z",
        "State": "UPDATING"
    },
    "requestID": "a145309d-df14-4c2e-a9f6-8ed45EXAMPLE",
    "eventID": "ed33ab96-f5c6-4a77-a69a-8585aEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


검색

다음은 Search 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예제입니다.

> **Note**
>
> 보안상의 이유로 CloudTrail 추적 항목에서 Tag, Filters, QueryString 파라미터에 대한 모든 참조가 편집되었습니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-03T16:50:11Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "Search",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.search",
    "requestParameters": {
        "QueryString": "***"
    },
    "responseElements": null,
    "requestID": "22320db5-b194-446f-b9f4-e603bEXAMPLE",
    "eventID": "addb3bca-0c41-46bf-a5e6-42299EXAMPLE",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


CreateView

다음은 `CreateView` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예제입니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-01-20T21:54:48Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-view",
    "requestParameters": {
        "ViewName": "CTTagsTest",
        "Tags": "***"
    },
    "responseElements": {
        "View": {
            "Filters": "***",
            "IncludedProperties": [],
            "LastUpdatedAt": "2023-01-20T21:54:48.079Z",
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    },
    "requestID": "b22d8ced-4905-42c4-b1aa-ef713EXAMPLE",
    "eventID": "f62e339f-1070-41a8-a6ec-12491EXAMPLE",
```

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

DeleteView

다음은 동일한 AWS 리전에서 `DeleteIndex` 작업으로 인해 `DeleteView` 작업이 자동으로 시작될 때 발생할 수 있는 이벤트를 보여주는 CloudTrail 로그 항목을 나타낸 예제입니다.

> **Note**
>
> 삭제된 뷰가 해당 리전의 기본 뷰인 경우, 이 작업은 비동기적으로 뷰와 기본 뷰의 연결을 끊습니다. 이는 `DisassociateDefaultView` 이벤트를 생성합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
```

```
    "eventTime": "2022-09-16T19:33:27Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "cd174d1e-0a24-4b47-8b67-d024aEXAMPLE",
    "readOnly": false,
    "resources": [{
        "accountId": "334026708824",
        "type": "AWS::ResourceExplorer2::View",
        "ARN": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

DisassociateDefaultView

다음은 현재 기본 보기의 DeleteView 작업으로 인해 DisassociateDefaultView 작업이 자동으로 시작될 때 발생할 수 있는 이벤트를 보여주는 CloudTrail 로그 항목을 나타낸 예제입니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "resource-explorer-2.amazonaws.com"
    },
    "eventTime": "2022-09-16T19:33:26Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DisassociateDefaultView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.disassociate-default-view",
    "requestParameters": null,
    "responseElements": null,
```

```
    "eventID": "d8016cb1-5c23-4ea4-bda2-70b03EXAMPLE",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Resource Explorer 문제 해결

Resource Explorer 작업 시 문제가 발생한다면 이 섹션의 주제를 참조하세요. 이 안내서의 보안 섹션에 있는 AWS 리소스 탐색기 권한 문제 해결도 참조하세요.

주제

일반 문제

주제

Resource Explorer에 대한 링크를 받았지만 링크를 열면 콘솔에 오류만 표시됩니다.

일부 타사 도구는 Resource Explorer의 페이지에 대한 링크 URL을 생성합니다. 해당 URL에 콘솔을 특정 AWS 리전으로 연결하는 파라미터가 포함되지 않는 경우도 있습니다. 이러한 링크를 열면 Resource Explorer 콘솔에 사용할 리전이 표시되지 않으며 사용자가 마지막으로 로그인한 리전을 사용하도록 기본 설정됩니다. 사용자에게 해당 리전의 Resource Explorer에 액세스할 권한이 없는 경우 콘솔은 미국 동부(버지니아 북부)(`us-east-1`) 리전을 사용하려고 시도하며, 콘솔이 `us-east-1`에 닿을 수 없는 경우 미국 서부(오레곤)(`us-west-2`) 리전을 사용하려고 시도합니다.

사용자에게 이러한 리전에 있는 인덱스에 액세스할 수 있는 권한이 없는 경우 Resource Explorer 콘솔은 오류를 반환합니다.

모든 사용자에게 다음과 같은 권한이 있는지 확인함으로써 이 문제를 방지할 수 있습니다.

- `ListIndexes` - 특정 리소스가 없습니다. *를 사용하세요.
- 계정에 생성된 각 인덱스의 ARN에 대한 `GetIndex`입니다. 인덱스를 삭제하고 다시 생성할 경우 권한 정책을 다시 실행할 필요가 없도록 하려면 *를 사용하는 것이 좋습니다.

이를 달성하기 위한 최소 정책은 다음 예제와 같습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetIndex",
                "resource-explorer-2:ListIndexes",
            ],
            "Resource": "*"
        }
    ]
}
```

Resource Explorer를 사용해야 하는 모든 사용자에게 AWS 관리 권한 `AWSResourceExplorerReadOnlyAccess`를 연결하는 것을 고려해 볼 수 있습니다. 그러면 이러한 필수 권한과 함께 리전에서 사용 가능한 뷰를 확인하고 해당 뷰를 사용하여 검색하는 데 필요한 권한도 부여됩니다.

콘솔의 통합 검색으로 인해 CloudTrail 로그에 '액세스 거부됨' 오류가 발생하는 이유는 무엇인가요?

AWS Management Console에서 통합 검색을 사용하면 보안 주체가 AWS Management Console의 모든 페이지에서 검색할 수 있습니다. Resource Explorer가 활성화되어 있고 통합 검색을 지원하도록 구성된 경우 결과에 보안 주체 계정의 리소스가 포함될 수 있습니다. 통합 검색 창에 입력을 시작할 때마다 통합 검색은 결과에 사용자 계정의 리소스를 포함할 수 있는지 확인하기 위해 `resource-explorer-2:ListIndexes` 작업을 호출려고 시도합니다.

통합 검색은 현재 로그인한 사용자의 권한을 사용하여 이 확인을 수행합니다. 해당 사용자에게 연결된 AWS Identity and Access Management(IAM) 권한 정책에서 부여된 `resource-explorer-2:ListIndexes` 호출 권한이 없는 경우 확인이 실패합니다. 해당 실패는 CloudTrail 로그에 `Access denied` 항목으로 추가됩니다.

이 CloudTrail 로그 항목에는 다음과 같은 특성이 있습니다.

- 이벤트 소스: `resource-explorer-2.amazonaws.com`
- 이벤트 이름: `ListIndexes`
- 오류 코드: `403`(액세스 거부됨)

다음 AWS 관리형 정책에는 `resource-explorer-2:ListIndexes`를 호출할 수 있는 권한이 포함되어 있습니다. 보안 주체 또는 이 권한을 포함하는 다른 정책에 이들 중 하나를 할당하는 경우 이 오류는 발생하지 않습니다.

- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

Resource Explorer 설정 및 구성 문제 해결

이 문서의 정보를 사용하여 AWS 리소스 탐색기을 처음 설정하거나 구성할 때 발생할 수 있는 문제를 진단하고 수정할 수 있습니다.

주제

Resource Explorer에 요청 시 '액세스 거부' 메시지가 표시됨

- 요청한 작업 및 리소스를 호출할 권한이 있는지 확인하세요. 관리자는 IAM 보안 주체(예: 역할, 그룹 또는 사용자)에게 AWS Identity and Access Management(IAM) 권한 정책을 할당하여 권한을 부여할 수 있습니다.

  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 사용자(콘솔)에 권한 추가의 지침을 따르세요.

  정책에서 액세스하려는 `Resource`에서 요청된 `Action`을 허용해야 합니다.

  이러한 권한을 부여하는 정책 명령문에 시간이나 IP 주소 제한 정책이 포함된다면, 요청을 전송할 때 이러한 요구사항을 충족해야 합니다. IAM 보안 주체의 정책을 확인하거나 수정하는 방법은 IAM 사용 설명서의 IAM 정책 관리를 참조하세요.

- API 요청에 수동으로 서명하는 경우(AWS SDK를 사용하지 않고) 올바르게 요청에 서명했는지 확인합니다.

임시 보안 자격 증명으로 요청하면 "액세스 거부" 메시지가 표시됩니다

- 요청을 수행하는 데 사용 중인 IAM 보안 주체에 올바른 권한이 있는지 확인합니다. 임시 보안 보안 인증에 대한 권한은 IAM에서 정의된 보안 주체에서 파생되므로 해당 권한은 해당 주체에게 부여된 권한으로 제한됩니다. 임시 보안 보안 인증에 대한 권한이 결정되는 방법에 대한 자세한 내용은 IAM 사용 설명서의 임시 보안 보안 인증에 대한 권한 제어를 참조하세요.
- 요청에 올바르게 서명했고 요청이 잘 구성되었는지 확인합니다. 자세한 내용은 선택한 SDK에 대한 툴킷 설명서나 IAM 사용 설명서의 AWS 리소스에 임시 보안 인증 사용을 참조하세요.
- 임시 보안 자격 증명이 만료되지 않았는지 확인합니다. 자세한 내용은 IAM 사용 설명서의 임시 보안 보안 인증 요청을 참조하세요.

Resource Explorer 검색 문제 해결

여기에 있는 정보를 사용하면 Resource Explorer를 사용하여 리소스를 검색할 때 발생할 수 있는 일반적인 오류를 진단하고 수정할 수 있습니다.

주제

- Resource Explorer 검색 결과에서 일부 리소스가 누락되는 이유는 무엇인가요?
- 리소스가 콘솔의 통합 검색 결과에 표시되지 않는 이유는 무엇인가요?
- 콘솔과 Resource Explorer의 통합 검색에서 가끔 다른 결과가 나오는 이유는 무엇인가요?
- 리소스를 검색하려면 어떤 권한이 필요한가요?

Resource Explorer 검색 결과에서 일부 리소스가 누락되는 이유는 무엇인가요?

다음 목록은 일부 리소스가 예상대로 검색 결과에 나타나지 않을 수 있는 이유를 제공합니다.

초기 인덱싱 생성이 완료되지 않음

에서 리소스 탐색기를 처음 켠 후 인덱싱 및 애그리게이터 인덱스로의 복제를 완료하는 데 최대 36시간이 걸릴 수 있습니다. AWS 리전나중에 다시 검색해 보세요.

새 리소스일 경우

Resource Explorer에서 새 리소스를 검색하고 로컬 인덱스에 추가하는 데 몇 분 정도 걸릴 수 있습니다. 몇 분 후에 다시 시도하세요.

한 리전의 새 리소스에 대한 정보가 아직 애그리게이터 인덱스에 전파되지 않음

한 지역에서 검색된 새 리소스에 대한 세부 정보가 해당 지역에서 인덱싱된 다음 해당 계정의 애그리게이터 인덱스로 복제되는 데 시간이 걸릴 수 있습니다. 새 리소스는 복제가 완료된 후에만 리전 간 검색 결과에 표시될 수 있습니다. 나중에 다시 검색해 보세요.

리소스가 있는 리전에 Resource Explorer가 활성화되어 있지 않음

리소스 탐색기가 어느 위치에서 작동할 수 AWS 리전 있는지는 관리자가 결정합니다. 설정 페이지에는 Resource Explorer가 활성화되어 있고 인덱스가 포함된 리전이 표시됩니다. 리소스가 있는 리전이 활성화되어 있지 않은 경우 관리자에게 해당 리전의 Resource Explorer를 활성화하도록 요청하세요.

리소스가 다른 리전에 있고 검색된 리전에 애그리게이터 인덱스가 포함되어 있지 않음

애그리게이터 인덱스가 포함된 리전의 뷰를 사용해야만 계정에 있는 모든 리전에 걸쳐 리소스를 검색할 수 있습니다. 다른 리전에서 검색하면 검색을 수행하는 리전의 리소스만 반환됩니다.

뷰의 필터에서 해당 리소스가 제외됨

모든 뷰에는 해당 뷰로 작성된 검색 결과에 포함할 수 있는 결과를 제한하는 필터를 구성에 포함할 수 있습니다. 찾고 있는 리소스가 검색에 사용하는 뷰의 필터와 일치하는지 확인하세요. 필터에 대한 자세한 내용은 을 참조하십시오필터.

리소스 유형은 리소스 탐색기에서 지원되지 않습니다.

일부 리소스 유형은 Resource Explorer에서 지원되지 않습니다. 자세한 내용은 Resource Explorer로 검색할 수 있는 리소스 유형 단원을 참조하십시오.

인덱스 또는 뷰는 콘솔 영역에 구성되어 있지 않습니다.

콘솔에서 위젯을 사용하는 데 필요한 지역에 인덱스 또는 뷰가 구성되지 않으면 예상한 결과가 표시되지 않습니다. 자세한 내용은 애그리게이터 인덱스를 생성하여 리전 간 검색 활성화 단원을 참조하십시오.

뷰에는 태그가 포함되지 않습니다.

리소스 탐색기 위젯에는 태그가 필요합니다. 뷰에 태그가 포함되지 않은 경우 리소스는 결과에 포함되지 않습니다. 자세한 내용은 뷰에 태그 추가 단원을 참조하십시오.

검색에서 잘못된 검색어 구문을 사용합니다.

리소스 탐색기에서의 검색은 이 서비스에만 있습니다. 구문이 올바르지 않으면 원하는 리소스를 찾을 수 없습니다. 자세한 내용은 Resource Explorer에 대한 검색 쿼리 구문 참조 단원을 참조하십시오.

최근에 리소스에 태그를 지정했습니다.

리소스에 태그를 지정한 후 해당 리소스가 검색 결과에 표시되기까지 30초 정도 지연됩니다.

리소스 유형은 태그 필터를 지원하지 않습니다.

리소스 유형에서 태그 필터를 지원하지 않는 경우 리소스 탐색기 위젯에 표시되지 않습니다. 태그 필터를 지원하지 않는 리소스 유형은 다음과 같습니다.

- `cloudfront:cache-policy`
- `cloudfront:origin-access-identity`
- `cloudfront:function`
- `cloudfront:origin-request-policy`
- `cloudfront:realtime-log-config`
- `cloudfront:response-headers-policy`
- `cloudwatch:dashboard`
- `docdb:globalcluster`
- `elasticache:globalreplicationgroup`
- `iam:group`
- `lambda:code-signing-config`
- `lambda:event-source-mapping`

- ssm:windowtarget
- ssm:windowtask
- rds:auto-backup
- rds:global-cluster
- s3:accesspoint

리소스가 콘솔의 통합 검색 결과에 표시되지 않는 이유는 무엇인가요?

통합 검색 결과는 모든 AWS Management Console 페이지 상단의 검색 창에서 확인할 수 있습니다. 하지만 검색에서는 다음 구성 옵션이 완료된 후에만 검색 결과에서 쿼리와 일치하는 리소스를 반환할 수 있습니다.

- 계정에 있는 리전 중 하나에 애그리게이터 인덱스가 있어야 합니다.
- 리전에 애그리게이터 인덱스가 포함된 기본 뷰가 있어야 합니다.
- 모든 주도자 (IAM역할 및 사용자) 에게는 해당 기본 보기를 사용하여 검색할 수 있는 권한이 있어야 합니다.

콘솔과 Resource Explorer의 통합 검색에서 가끔 다른 결과가 나오는 이유는 무엇인가요?

통합 검색 결과는 모든 AWS Management Console 페이지 상단의 검색 창에서 확인할 수 있습니다. 통합 검색을 사용하는 경우 통합 검색 프로세스에서는 쿼리 문자열에 입력하는 첫 번째 용어 끝에 와일드카드 문자(*)를 자동으로 삽입합니다. 이 와일드카드 문자는 통합 검색 창에 표시되지 않지만 결과에는 영향을 미칩니다.

> **Important**
>
> 통합 검색은 문자열의 첫 번째 키워드 끝에 와일드카드 문자(*) 연산자를 자동으로 삽입합니다. 즉, 통합 검색 결과에는 지정된 키워드로 시작하는 모든 문자열과 일치하는 리소스가 포함됩니다.
>
> Resource Explorer 콘솔의 리소스 검색 페이지에 있는 쿼리 텍스트 상자에서 수행되는 검색에는 와일드카드 문자가 자동으로 추가되지 않습니다. 검색 문자열에서 용어 뒤에 *를 수동으로 삽입할 수 있습니다.

리소스를 검색하려면 어떤 권한이 필요한가요?

검색하려면 작업을 호출한 리전에 있는 뷰에서 다음 작업을 모두 수행할 수 있는 권한이 있어야 합니다.

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

보안 주체에 할당된 정책에 다음 예와 비슷한 설명을 추가하여 이 작업을 수행할 수 있습니다IAM.

```
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-
View-Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
```

특정 뷰의 Amazon 리소스 번호 (ARN) 를 와일드카드 (*) ARN 가 포함된 것으로 대체하여 일치하는 모든 뷰에 권한을 부여할 수 있습니다.

요청에서 뷰를 지정하지 않으면 Resource Explorer는 요청한 리전의 기본 뷰를 자동으로 사용합니다. 기본 뷰를 사용할 권한이 없는 경우 관리자에게 문의하세요.

> **Note**
>
> Resource Explorer 검색 쿼리 결과에 리소스가 표시되더라도 해당 리소스와 상호 작용하려면 리소스 자체에 대한 권한이 필요합니다.

Resource Explorer 할당량

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량이 있습니다. 달리 언급하지 않는 한, 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

AWS 리소스 탐색기에 대한 할당량을 보려면 Service Quotas 콘솔을 엽니다. 탐색 창에서 AWS 서비스를 선택하고 Resource Explorer를 선택합니다.

할당량 증가을 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 한도 증가 양식을 사용합니다.

다음 할당량은 Resource Explorer의 기본값입니다.

최대값 할당량	기본값
한 AWS 리전의 조회수	10

작업에 대한 속도 제한	기본값
초당 최대 검색 작업 수	5
초당 최대 비검색 작업 수	3
애그리게이터 리전의 월별 최대 검색 작업 수	10,000
로컬 리전의 월별 최대 검색 작업 수	500

와 AWS 리소스 탐색기 함께 사용 AWS SDK

AWS 소프트웨어 개발 키트(SDKs)는 많은 인기 프로그래밍 언어에 사용할 수 있습니다. 각 는 개발자가 원하는 언어로 애플리케이션을 더 쉽게 빌드할 수 있도록 API, 코드 예제 및 설명서를 SDK 제공합니다.

SDK 설명서	코드 예시
AWS SDK for C++	AWS SDK for C++ 코드 예제
AWS CLI	AWS CLI 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 Kotlin	AWS SDK for Kotlin 코드 예제
AWS SDK for .NET	AWS SDK for .NET 코드 예제
AWS SDK for PHP	AWS SDK for PHP 코드 예제
AWS Tools for PowerShell	PowerShell 코드 예제용 도구
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 코드 예제
AWS SDK for Ruby	AWS SDK for Ruby 코드 예제
AWS SDK for Rust	AWS SDK for Rust 코드 예제
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP 코드 예제
AWS SDK for Swift	AWS SDK for Swift 코드 예제

가용성 예제

필요한 예제를 찾을 수 없습니까? 이 페이지 하단의 피드백 제공 링크를 사용하여 코드 예시를 요청하세요.

Resource Explorer 사용 설명서의 문서 기록

다음 표에서는 에 대한 설명서 릴리스를 설명합니다 AWS 리소스 탐색기. 이 설명서의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
새 검색 필터 추가됨	Resource Explorer는 리소스 유형이 Resource Explorer에서 지원되지 않더라도 하나 이상의 사용자 생성 태그가 연결된 리소스를 검색할 수 있도록 새 `tag:all` 검색 쿼리 필터를 추가했습니다.	2024년 9월 6일
콘텐츠 조직 개선 사항	주제 제목을 업데이트하고 콘텐츠를 재구성하여 가독성과 검색 가능성을 개선했습니다.	2024년 8월 29일
IAM 정책 업그레이드 알림 IPv6	ASPEN 정책이 포함된 이중 주소 지정을 사용하는 고객은 이 업그레이드의 `aws:sourceIp` 영향을 받습니다. 이중 주소 지정은 네트워크가 IPv4 및 를 모두 지원한다는 의미입니다IPv6.	2024년 7월 15일
세 가지 리소스 유형에 대한 지원 중단	Resource Explorer는 `ecs:task`, `ssm:automation-execution` 및 의 세 가지 리소스 유형에 대한 지원을 중단했습니다`ssm:patchbaseline` .	2024년 7월 9일
새 리소스 유형에 대한 지원이 추가됨	Resource Explorer는 AWS Key Management Service, Amazon Route 53 및 Amazon	2024년 2월 20일

	Fraud Detector를 AWS 서비스 포함하여 의 65개 새 리소스에 대한 지원을 추가했습니다.	
업데이트된 관리형 정책	Resource Explorer에서 추가 리소스 유형을 보기 위한 지원을 추가했습니다. AWSResourceExplorerServiceRolePolicy AWS 관리형 정책은 Resource Explorer에 추가 리소스 유형을 볼 수 있는 액세스 권한을 부여하도록 업데이트되었습니다.	2023년 12월 12일
새 검색 필터 추가됨	Resource Explorer는 이제 애플리케이션별 리소스 검색을 지원합니다.	2023년 11월 16일
새 리소스 유형에 대한 지원이 추가됨	Resource Explorer는 AWS CloudFormation, 및 Amazon AWS Glue를 AWS 서비스 포함하여 의 86개 새 리소스에 대한 지원을 추가했습니다 SageMaker.	2023년 11월 15일
Resource Explorer에서 다중 계정 검색 지원	이제 Resource Explorer를 사용하여 조직 또는 조직 단위 내의 AWS 계정 전반에 걸쳐 리소스를 검색하고 발견할 수 있습니다. 자세한 내용은 다중 계정 검색 활성화를 참조하세요.	2023년 11월 14일

신규 및 업데이트된 관리형 정책	Resource Explorer에 AWS Organizations에 대한 지원이 추가되었습니다. 조직, 조직 구조, 계정 및 위임된 관리자에게 Resource Explorer 액세스 권한을 부여하도록 AWS 관리형 정책이 추가 및 업데이트되었습니다.	2023년 11월 14일
새 리소스 유형에 대한 지원이 추가됨	Resource Explorer에 AWS Organizations에 대한 지원이 추가되었습니다. 조직, 조직 구조, 계정 및 위임된 관리자에게 Resource Explorer 액세스 권한을 부여하도록 AWS 관리형 정책이 업데이트되었습니다.	2023년 11월 14일
새 리소스 유형에 대한 지원이 추가됨	Resource Explorer는 이제 Amazon Cognito, AWS Elastic Beanstalk및 Amazon Elastic File System을 포함한 서비스에서 12개의 새 리소스 유형을 지원합니다.	2023년 10월 18일
새 리소스 유형에 대한 지원이 추가됨	Resource Explorer에 164개 리소스에 대한 지원이 추가되었습니다. Resource Explorer에 인덱스 리소스에 대한 액세스 권한을 부여하는 AWS 관리형 정책이 이러한 새 리소스 유형을 포함하도록 업데이트되었습니다.	2023년 10월 17일
이제 Resource Explorer를 특정 옵트인 리전에서 사용 가능	BAH 및 의 고객은 이제 Resource Explorer에 옵트인할 CGK 수 있습니다.	2023년 10월 5일

새 리소스 유형에 대한 지원이 추가됨	Resource Explorer는 AWS 서비스 AWS CodeBuild , , Amazon Cognito AWS CodePipeline, Amazon Elastic Container Registry, Amazon Elastic File System AWS Elastic Beanstalk, AWS IoT및 의 리소스에 대한 지원을 추가했습니다 AWS Step Functions . Resource Explorer에 인덱스 리소스에 대한 액세스 권한을 부여하는 AWS 관리형 정책이 이러한 새 리소스 유형을 포함하도록 업데이트되었습니다.	2023년 8월 1일
이제 Resource Explorer가 로 검색 결과 내보내기를 지원합니다. CSV	이제 리소스 검색 페이지에서 검색 결과를 형식이 지정된 파일로 내보낼 수 있습니다. CSV	2023년 4월 4일
AWS Chatbot 를 사용하여 AWS 리소스를 검색하고 검색합니다.	이제 AWS Chatbot 를 사용하여 자연어 질문을 사용하여 리소스를 검색할 수 있습니다. 자세한 내용은 리소스 검색에 AWS Chatbot 사용을 참조하세요.	2023년 3월 30일
새 리소스 유형에 대한 지원이 추가됨	Resource Explorer는 Amazon ElastiCache, AWS Lambda및 AWS 서비스 Amazon Simple Queue Service(Amazon)의 리소스에 대한 지원을 추가했습니다SQS. Resource Explorer에 인덱스 리소스에 대한 액세스 권한을 부여하는 AWS 관리형 정책이 이러한 새 리소스 유형을 포함하도록 업데이트되었습니다.	2023년 3월 7일

IAM 모범 사례 업데이트	IAM 모범 사례에 맞게 가이드를 업데이트했습니다. 자세한 내용은 의 보안 모범 사례를 IAM참조하세요.	2022년 12월 6일
새로운 AWS 관리형 정책	Resource Explorer는 AWSResourceExplorerFullAccess, AWSResourceExplorerReadOnlyAccess 및 AWSResourceExplorerServiceRolePolicy 관리형 정책을 추가합니다.	2022년 11월 7일
최초 릴리스	Resource Explorer 사용 설명서의 최초 릴리스	2022년 11월 7일

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