보안 정보

AWS제어 카탈로그

AWS제어 카탈로그: 보안 정보

Table of Contents

AWS제어 카탈로그란 무엇입니까?

AWS제어 카탈로그 보안 정보 가이드에 오신 것을 환영합니다. 제어 카탈로그는 다음 항목의 일부입니다. AWS Control Tower에는 여러 컨트롤에 대한 목록이 나열되어 있습니다. AWS 서비스. 의 통합 카탈로그입니다. AWS 컨트롤. 설정할 필요가 없습니다. AWS Control Tower 제어 카탈로그를 사용하려면

제어 카탈로그를 사용하면 보안, 비용, 내구성, 운영 등 일반적인 사용 사례에 따른 컨트롤을 볼 수 있습니다.

이 문서에서는 AWS Control Catalog에서 제공하는 보안 및 규정 준수 정보를 사용할 때 알아야 APIs 하는 보안 및 규정 준수 정보를 찾을 수 있습니다.

컨트롤 카탈로그는 컨트롤의 표준 분류 시스템인 컨트롤 온톨로지를 구현합니다.

온톨로지 개요

AWS 컨트롤을 분류, 구성 및 매핑하는 데 도움이 되는 표준 분류 시스템을 개발했습니다. 이 온톨로지는 24개의 프레임워크를 포함한 기존 및 새로운 규제 표준뿐만 아니라, 등과 같은 규제 표준에 컨트롤을 매핑하는 데 사용할 수 있습니다. PCI HIPAA 또한ISO, NIST 및 같은 업계 표준과 Well-Architected 프레임워크를 비롯한 아마존 전용 프레임워크에도 매핑됩니다.

온톨로지에는 네 가지 핵심 측면이 있습니다.

- 통제 영역, 통제 목표 및 공통 통제별 통제 분류. 온톨로지는 관련 제어를 세 가지 수준으로 구성하고 그룹화하는 데 도움이 됩니다.
  - L1: 제어 도메인,
  - L2: 제어 목표,
  - L3: 공통 제어.

  이러한 수준에는 엄격한 계층 관계가 있습니다. 즉, 각 도메인에는 여러 제어 목표가 있지만 각 제어 목표에는 단일 부모 도메인이 있어야 합니다. 각 규제 목표에는 여러 개의 공통 통제가 있지만 각 공통 통제에는 단일 상위 목표가 있습니다.
- 규제 표준과의 매핑. 온톨로지에는 규제 또는 산업 표준 내의 특정 요구 사항을 나타내는 표준 제어(L4) 라는 개념이 있습니다. 이러한 표준 컨트롤은 이러한 특정 요구 사항을 해결하는 데 도움이 되는 공통 컨트롤에 매핑됩니다.

예: PCI- DSS v3.2.1. ID 4.1 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. NIST 800.53.r5 ID SC-16 보안 및 개인 정보 보호 속성의 전송은 두 가지 표준 제어 기능으로, 둘 다 전송 중인 데이터 암호화에 매핑됩니다. 공통 제어입니다.

- 제어 구현 및 통제 증거. 온톨로지에는 제어 구현 (L6) 이라는 개념이 있으며, 이 개념은 다음과 같은 특정 제어 구현을 나타낼 수 있습니다. AWS예를 들어, AWS Control Tower 컨트롤, AWS Security Hub 확인, 그리고 AWS Config 규칙 등, 또는 외부 비기술적 구현 AWS예: 프로세스 지침 통제 증거 (L7) 라는 별도의 개념은 다음과 같은 방법으로 규제 증거로 사용할 수 있는 데이터 소스를 나타냅니다. AWS Audit Manager, 타사 도구 또는 고객 자체 이러한 증거 출처는 다음과 같을 수 있습니다. AWS 다음과 같은 출처: AWS CloudTrail 이벤트, API 통화 기록 및 AWS Config 규칙 평가 결과. 또는 고객 문서와 같은 외부 소스일 수도 있습니다.
- 코어 컨트롤 (L5) 의 개념. 핵심 컨트롤은 모든 컨트롤 구현 (L6), 해당 증거 소스 (L7), 관련 표준 컨트롤 (L4), 공통 컨트롤 (L3) 을 하나의 전체적인 개체로 통합하는 매핑 레이어입니다. 핵심 컨트롤은 컨트롤 자체라기보다는 매핑 문서에 가깝습니다. 컨트롤 X와 관련된 모든 정보를 보여줘야 한다는 질문에 답하는 데 도움이 됩니다. 각 핵심 컨트롤에는 여러 개의 컨트롤 구현 (L6) 과 여러 증거 소스 (L7) 가 있을 수 있습니다.

요약하면 AWS 제어 카탈로그 온톨로지는 7개의 계층으로 구성되어 있습니다. 세 가지 계층적 분류 계층 (제어 도메인, 제어 목표, 공통 제어) 이 있습니다. 또 다른 계층 (표준 제어) 은 규제 또는 업계 표준 요구 사항을 설명합니다. 매핑 계층 (핵심 제어) 은 지정된 리소스 유형에 대한 제어 결과를 설명합니다. 두 계층 (제어 구현, 제어 증거) 은 특정 제어 구현 및 증거 소스를 설명합니다.

이 온톨로지는 다음과 같이 설계되었습니다. AWS 규정 준수 감사를 위해 수백 명의 고객과 함께 일한 경험을 바탕으로 한 공인 심사원 팀 규제 도메인, 규제 목표, 공통 규제 및 표준 규제 (L1-L4) 의 개념은 업계 전반에 걸쳐 사용됩니다. 이는 일반적인 산업 패턴 및 NIST 권장 사항과 일치합니다. 나머지 3개 레이어 (L5-L7) 는 기존 레이어를 기반으로 설계되었습니다. AWS 개념 (예: 리소스 유형 및 관리형 제어)

제어 카탈로그에 대한 액세스 AWS

AWS제어 카탈로그는 콘솔과 AWS 제어 카탈로그 애플리케이션 프로그래밍 인터페이스 (API) 를 통해 사용할 수 있습니다. 이를 API 통해 사용자가 사용할 수 있는 공통 컨트롤 및 관련 메타데이터를 프로그래밍 방식으로 식별하고 필터링할 수 있습니다. AWS 고객. 자세한 내용은 AWS제어 카탈로그 API 참조를 참조하십시오.

제어 카탈로그의 AWS 보안

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

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

- 클라우드 보안 — AWS 실행 중인 인프라를 보호할 책임이 있습니다. AWS 서비스 에서 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 제3자 감사자는 보안 조치의 일환으로 당사 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS 규정 준수 프로그램 . AWS제어 카탈로그에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 다음을 참조하십시오. AWS 규정 준수 프로그램별 범위 내 서비스 .
- 클라우드에서의 보안 — 귀하의 책임은 다음에 의해 결정됩니다. AWS 서비스 사용하는 것. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS 제어 카탈로그를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목은 보안 및 규정 준수 목표를 충족하도록 AWS 제어 카탈로그를 구성하는 방법을 보여줍니다. 다른 방법을 사용하는 방법도 배웁니다. AWS 서비스 AWS제어 카탈로그 리소스를 모니터링하고 보호하는 데 도움이 됩니다.

주제

AWS제어 카탈로그의 데이터 보호

더 AWS 공동 책임 모델 AWS 제어 카탈로그의 데이터 보호에 적용됩니다. 이 모델에 설명된 바와 같이 AWS 모든 시스템을 운영하는 글로벌 인프라를 보호하는 책임이 있습니다. AWS 클라우드. 이 인프라에서 호스팅되는 콘텐츠에 대한 통제권을 유지할 책임은 귀하에게 있습니다. 또한 귀하는 에 대한 보안

구성 및 관리 작업을 담당합니다. AWS 서비스 사용하는 것. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시를 참조하십시오FAQ. 유럽의 데이터 보호에 대한 자세한 내용은 다음을 참조하십시오. AWS 공동 책임 모델 및 관련 GDPR 블로그 게시물 AWS 보안 블로그.

데이터 보호를 위해 다음을 보호하는 것이 좋습니다. AWS 계정 자격 증명 및 개별 사용자 설정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM). 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정마다 다단계 인증 (MFA) 을 사용하십시오.
- SSL/를 사용하여 다음과 TLS 통신할 수 있습니다. AWS 있습니다. TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- 다음을 사용하여 사용자 활동 API 로깅을 설정하고 사용자 활동을 기록합니다. AWS CloudTrail. CloudTrail 트레일을 사용하여 캡처하는 방법에 대한 자세한 내용은 AWS 활동에 대한 자세한 내용은 CloudTrail 트레일 사용을 참조하십시오. AWS CloudTrail 사용자 가이드.
- 사용 AWS 암호화 솔루션 및 포함된 모든 기본 보안 제어 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 액세스 시 FIPS 140-3개의 검증된 암호화 모듈이 필요한 경우 AWS 명령줄 인터페이스 또는 API an을 통해 엔드포인트를 사용하십시오. FIPS 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준 (FIPS) 140-3을 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 AWS 제어 카탈로그 또는 기타 항목을 사용하는 경우가 포함됩니다. AWS 서비스 콘솔 사용API, AWS CLI, 또는 AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 제공하는 경우 해당 서버에 대한 요청을 URL 검증하기 위해 자격 증명 정보를 에 포함하지 않는 것이 좋습니다. URL

데이터 암호화

AWS 제어 카탈로그에는 고객 데이터가 저장되지 않습니다.

저장 중 암호화

AWS 제어 카탈로그는 고객 데이터를 암호화하지 않습니다. 에 의해 유지되거나 보존되는 고객 데이터가 없기 때문입니다. AWS 제어 카탈로그에는 저장 중 암호화에 대한 구체적인 지침이 없습니다.

전송 중 암호화

AWS 제어 카탈로그는 고객 데이터를 암호화하지 않습니다. 는 민감한 데이터를 교환하거나 보관하지 않기 때문입니다. AWS 제어 카탈로그에는 전송 중 암호화에 대한 구체적인 지침이 없습니다.

키 관리

암호화 키 관리는 다음과 같은 경우에는 적용되지 않습니다. AWS 제어 카탈로그.

인터네트워크 트래픽 개인 정보 보호

네트워크 간 트래픽 개인 정보 보호는 다음 항목에는 적용되지 않습니다. AWS 제어 카탈로그.

AWS제어 카탈로그의 ID 및 액세스 관리

AWS Identity and Access Management (IAM) 는 AWS 서비스 이를 통해 관리자는 다음 항목에 대한 액세스를 안전하게 제어할 수 있습니다. AWS 있습니다. IAM관리자는 제어 카탈로그 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 AWS 제어합니다. IAM는 AWS 서비스 추가 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- AWS제어 카탈로그의 작동 방식 IAM
- 제어 카탈로그의 ID 기반 정책 예제 AWS
- AWS제어 카탈로그 ID 및 액세스 문제 해결

고객

사용 방법 AWS Identity and Access Management (IAM) 는 AWS 제어 카탈로그에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - AWS 제어 카탈로그 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS 제어 카탈로그 기능을 사용하여 작업을 수행함에 따라 추가

권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS제어 카탈로그의 기능에 액세스할 수 없는 경우 을 참조하십시오AWS제어 카탈로그 ID 및 액세스 문제 해결.

서비스 관리자 — 회사에서 AWS 제어 카탈로그 리소스를 담당하는 경우 제어 카탈로그에 AWS 대한 전체 액세스 권한이 있을 것입니다. 서비스 사용자가 액세스해야 하는 AWS 제어 카탈로그 기능 및 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음 IAM 관리자에게 서비스 사용자의 권한을 변경해 달라는 요청을 제출해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 IAM 이해하십시오. 회사에서 AWS 제어 카탈로그를 사용하는 IAM 방법에 대한 자세한 내용은 을 참조하십시오AWS제어 카탈로그의 작동 방식 IAM.

IAM관리자 - IAM 관리자인 경우 AWS 제어 카탈로그에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알아보는 것이 좋습니다. 에서 IAM 사용할 수 있는 AWS 제어 카탈로그 ID 기반 정책의 예를 보려면 을 참조하십시오. 제어 카탈로그의 ID 기반 정책 예제 AWS

ID를 통한 인증

인증은 로그인하는 방법입니다. AWS ID 자격 증명 사용. 인증 (로그인) 을 받아야 합니다. AWS다음과 같이) AWS 계정 루트 사용자 IAM사용자로서, 또는 IAM 역할을 맡아서.

에 로그인할 수 있습니다. AWS ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 사용할 수 있습니다. AWS IAM Identity Center 페더레이션 ID의 예로는 (IAMID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 있습니다. 페더레이션 ID로 로그인하는 경우 관리자는 이전에 역할을 사용하여 ID 페더레이션을 설정했습니다. IAM 액세스하는 경우 AWS 페더레이션을 사용하면 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 로그인할 수 있습니다. AWS Management Console 또는 AWS 액세스 포털. 로그인에 대한 자세한 내용은 AWS로그인하는 방법을 참조하십시오. AWS 계정의 AWS 로그인 사용자 가이드.

액세스하는 경우 AWS 프로그래밍 방식으로 AWS 자격 증명을 사용하여 요청에 암호로 서명할 수 있는 소프트웨어 개발 키트 (SDKCLI) 와 명령줄 인터페이스 () 를 제공합니다. 사용하지 않는 경우 AWS 도구를 사용하려면 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 서명을 참조하십시오. AWS APIIAM사용 설명서의 요청.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예: AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 의 다단계 인증을 참조하십시오. AWS IAM Identity Center 사용 설명서 및 다단계 인증 사용 () MFA AWS(출처: IAM 사용 설명서).

AWS 계정 루트 사용자

를 생성할 때 AWS 계정모든 계정에 완전히 액세스할 수 있는 하나의 로그인 ID로 시작합니다. AWS 서비스 및 계정 내 리소스 이 ID를 다음과 같이 부릅니다. AWS 계정 루트 사용자는 계정을 만들 때 사용한 이메일 주소와 암호로 로그인하여 액세스할 수 있습니다. 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 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오. IAM

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 사용자가 ID 공급자와의 페더레이션을 사용하여 액세스하도록 하는 것입니다. AWS 서비스 임시 자격 증명을 사용하여

페더레이션 ID는 기업 사용자 디렉토리의 사용자, 웹 ID 제공업체, AWS Directory Service, ID 센터 디렉터리 또는 액세스하는 모든 사용자 AWS 서비스 ID 소스를 통해 제공된 자격 증명을 사용합니다. 페더레이션된 ID가 액세스하는 경우 AWS 계정역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해서는 다음을 사용하는 것이 좋습니다. AWS IAM Identity Center. IAMIdentity Center에서 사용자 및 그룹을 만들거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 위치에서 사용할 수 있습니다. AWS 계정 및 애플리케이션. ID 센터에 대한 자세한 내용은 IAM ID 센터란 IAM 무엇입니까? 를 참조하십시오. ... 에서 AWS IAM Identity Center 사용자 가이드.

IAM 사용자 및 그룹

IAM사용자는 내 정체성에 속해 있습니다. AWS 계정 이는 한 사람이나 애플리케이션에 대한 특정 권한을 가지고 있습니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명을 가진 IAM 사용자를 만드는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 특정 사용 사례에서 IAM 사용자의 장기 자격 증명이 필요한 경우에는 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 사용 설명서의 장기 자격 증명이 필요한 사용 사례에 대한 정기적인 액세스 키 IAM 교체를 참조하십시오.

IAM그룹은 IAM 사용자 컬렉션을 지정하는 ID입니다. 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 이름을 지정한 IAMAdmins그룹을 만들고 해당 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세히 알아보려면 사용 설명서의 역할 대신 IAM 사용자를 만드는 시기를 참조하십시오. IAM

IAM역할

IAM역할은 내 안의 정체성입니다. AWS 계정 여기에는 특정 권한이 있습니다. 사용자와 비슷하지만 특정 IAM 사용자와는 관련이 없습니다. 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS Management Console 역할을 바꿔서 말이죠. 를 호출하여 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API오퍼레이션을 사용하거나 사용자 지정을 사용합니다URL. 역할 사용 방법에 대한 자세한 내용은 사용 IAM설명서의 IAM역할 사용을 참조하십시오.

IAM임시 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. 페더레이션을 위한 역할에 대한 자세한 내용은 IAM사용 설명서의 타사 ID 제공자를 위한 역할 생성을 참조하십시오. IAMIdentity Center를 사용하는 경우 권한 집합을 구성합니다. ID가 인증된 후 액세스할 수 있는 대상을 제어하기 위해 IAM Identity Center는 권한 집합을 역할의 상관 관계와 연결합니다. IAM 권한 집합에 대한 자세한 내용은 권한 집합의 사용 권한 집합을 참조하십시오. AWS IAM Identity Center 사용 설명서.
- 임시 IAM 사용자 권한 — IAM 사용자 또는 역할은 역할을 맡아 특정 작업에 대해 일시적으로 다른 권한을 부여받을 수 있습니다. IAM
- 계정 간 액세스 - IAM 역할을 사용하여 다른 계정의 사용자 (신뢰할 수 있는 사용자) 가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 하지만 일부 경우에는 AWS 서비스역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 IAM 계정 간 리소스 액세스를 참조하십시오. IAM
- 서비스 간 액세스 — 일부 AWS 서비스 다른 기능 사용 AWS 서비스. 예를 들어, 서비스를 호출하면 해당 서비스가 Amazon에서 애플리케이션을 EC2 실행하거나 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 작업을 수행하는 경우 AWS, 귀하는 주도자로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS전화를 건 주체의 권한을 사용합니다. AWS 서비스, 요청과 결합 AWS 서비스 다운스트림 서비스에 요청하기. FAS요청은 서비스가 다른 서비스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. AWS 서비스 또는 완료해야 할 리소스. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM 역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다. 자

세한 내용은 권한을 위임하기 위한 역할 만들기를 참조하십시오. AWS 서비스(출처: IAM 사용 설명서).

- 서비스 연결 역할 - 서비스 연결 역할은 다음과 연결된 서비스 역할 유형입니다. AWS 서비스. 서비스가 사용자를 대신하여 작업을 수행하는 역할을 맡을 수 있습니다. 서비스 연결 역할은 다음과 같습니다. AWS 계정 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

- Amazon에서 실행되는 애플리케이션 EC2 — IAM 역할을 사용하여 EC2 인스턴스에서 실행 중이고 다음을 생성하는 애플리케이션에 대한 임시 자격 증명을 관리할 수 있습니다. AWS CLI 또는 AWS API요청. EC2인스턴스 내에 액세스 키를 저장하는 것보다 이 방법이 더 좋습니다. 할당하려면 AWS EC2인스턴스에 역할을 부여하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며, 이를 통해 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 사용 설명서의 IAM역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 IAM 참조하십시오.

IAM역할을 사용할지 IAM 사용자를 사용할지 알아보려면 사용 설명서의 IAM 역할 생성 시기 (사용자 대신) 를 IAM참조하십시오.

정책을 사용한 액세스 관리

에서 액세스를 제어할 수 있습니다. AWS 정책을 생성하여 정책에 연결하면 됩니다. AWS ID 또는 리소스. 정책은 다음의 객체입니다. AWS 이는 ID 또는 리소스와 연결될 경우 해당 권한을 정의합니다. AWS 보안 주체 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 다음 위치에 저장됩니다. AWS JSON문서로. JSON정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 다음을 사용할 수 있습니다. AWS JSON정책을 통해 누가 무엇에 액세스할 수 있는지 지정합니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

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

보안 인증 기반 정책

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

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 조직의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정. 관리형 정책에는 다음이 포함됩니다. AWS 관리형 정책 및 고객 관리형 정책. 관리형 정책과 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM사용 설명서의 관리형 정책과 인라인 정책 중 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 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, 연동 사용자 또는 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 사용할 수 없습니다. AWS 리소스 기반 정책의 관리형 정책. IAM

액세스 제어 목록 () ACLs

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지는 않지만 리소스 기반 정책과 JSON 비슷합니다.

아마존 S3, AWS WAF, VPC Amazon은 지원하는 서비스의 예입니다ACLs. 자세한 내용은 Amazon 심플 스토리지 서비스 개발자 안내서의 액세스 제어 목록 (ACL) 개요를 참조하십시오. ACLs

기타 정책 타입

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

- 권한 경계 - 권한 경계는 ID 기반 정책이 IAM 엔티티 (IAM사용자 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 사용 IAM설명서의 IAM 엔티티의 권한 경계를 참조하십시오.

- 서비스 제어 정책 (SCPs) — SCPs 조직 또는 OU (조직 구성 단위) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations. AWS Organizations 여러 개를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. AWS 계정 귀사가 소유한 것입니다. 조직의 모든 기능을 사용하도록 설정하면 일부 또는 모든 계정에 서비스 제어 정책 (SCPs) 을 적용할 수 있습니다. 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 SCP 제한합니다. AWS 계정 루트 사용자. Organizations 및 SCPs 에 대한 자세한 내용은 의 서비스 제어 정책을 참조하십시오. AWS Organizations 사용 설명서.
- 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 IAM사용 설명서의 세션 정책을 참조하십시오.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 방법을 알아보려면 AWS 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 결정하려면 IAM사용 설명서의 정책 평가 로직을 참조하십시오.

AWS제어 카탈로그의 작동 방식 IAM

제어 카탈로그에 대한 액세스를 관리하는 IAM 데 사용하기 전에 AWS 제어 카탈로그와 함께 AWS 사용할 수 있는 IAM 기능에 대해 알아보십시오.

IAMAWS제어 카탈로그와 함께 사용할 수 있는 기능

IAM기능	AWS제어 카탈로그 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예

IAM기능	AWS제어 카탈로그 지원
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책의 태그)	아니요
임시 보안 인증	예
보안 주체 권한	아니요
서비스 역할	아니요
서비스 연결 역할	아니요

AWS제어 카탈로그 및 기타 방법을 개괄적으로 파악하려면 AWS 서비스는 대부분의 IAM 기능과 함께 작동합니다. AWSIAM사용 IAM 설명서에서 함께 작동하는 서비스.

제어 카탈로그의 ID 기반 정책 AWS

ID 기반 정책 지원: 예

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

IAMID 기반 정책을 사용하면 허용 또는 거부된 작업 및 리소스는 물론 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 사용 IAM설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

제어 카탈로그의 ID 기반 정책 예제 AWS

AWS제어 카탈로그 ID 기반 정책의 예를 보려면 을 참조하십시오. 제어 카탈로그의 ID 기반 정책 예제 AWS

제어 카탈로그 내의 리소스 기반 정책 AWS

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 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, 연동 사용자 또는 AWS 서비스.

계정 간 액세스를 활성화하려면 다른 계정의 전체 계정 또는 IAM 엔티티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 경우 AWS 계정신뢰할 수 있는 계정의 IAM 관리자는 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM

AWS제어 카탈로그에 대한 정책 조치

정책 작업 지원: 예

관리자는 다음을 사용할 수 있습니다. AWS JSON정책을 통해 누가 무엇에 액세스할 수 있는지 지정합니다. 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. 일반적으로 정책 조치의 이름은 관련 조치와 동일합니다. AWS API오퍼레이션. 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.

AWS제어 카탈로그 작업 목록을 보려면 서비스 권한 부여 참조의 AWS제어 카탈로그에 정의된 작업을 참조하십시오.

AWS제어 카탈로그의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
controlcatalog
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "controlcatalog:ListCommonControls",
      "controlcatalog:ListDomains"
         ]
```

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

```
"Action": "controlcatalog:List*"
```

AWS제어 카탈로그 ID 기반 정책의 예를 보려면 을 참조하십시오. 제어 카탈로그의 ID 기반 정책 예제 AWS

제어 카탈로그의 정책 리소스 AWS

정책 리소스 지원: 예

관리자는 다음을 사용할 수 있습니다. AWS JSON정책을 통해 누가 무엇에 액세스할 수 있는지 지정합니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

ResourceJSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 Resource또는 NotResource요소가 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": "*"
```

AWS제어 카탈로그 리소스 유형 및 해당 ARNs 유형의 목록을 보려면 서비스 권한 부여 참조의 AWS 제어 카탈로그에서 정의된 리소스를 참조하십시오. 각 리소스의 어떤 작업을 지정할 수 있는지 알아보려면 AWS제어 카탈로그에서 정의한 작업을 참조하십시오. ARN

AWS제어 카탈로그 도메인의 Amazon 리소스 이름 (ARN) 형식은 다음과 같습니다.

```
arn:${Partition}:controlcatalog:::domain/${domainId}
```

AWS제어 카탈로그 목표의 ARN 형식은 다음과 같습니다.

```
arn:${Partition}:controlcatalog:::objective/${objectiveId}
```

AWS제어 카탈로그 공통 컨트롤의 ARN 형식은 다음과 같습니다.

```
arn:${Partition}:controlcatalog:::commonControl/${commonControlId}
```

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

예를 들어 명세서에서 `i-1234567890abcdef0` 도메인을 지정하려면 다음을 사용하십시오ARN.

```
"Resource": "arn:aws:controlcatalog:::domain/i-1234567890abcdef0"
```

특정 계정에 속하는 모든 인스턴스를 지정하려면 와일드카드(*)를 사용합니다.

```
"Resource": "arn:aws:controlcatalog:::domain/*"
```

리소스 생성 작업과 같은 일부 AWS 제어 카탈로그 작업은 특정 리소스에서 수행할 수 없습니다. 이러한 경우, 와일드카드(*)를 사용해야 합니다.

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

일부 AWS 제어 카탈로그 API 작업은 여러 리소스를 지원합니다. 예를 들어 공통 컨트롤, 목표 및 `ListCommonControls` 도메인에 액세스하므로 보안 주체는 이러한 각 리소스에 액세스할 수 있는 권한을 가져야 합니다. 명령문 하나에 여러 리소스를 지정하려면 ARNs 쉼표로 구분하십시오.

```
"Resource": [
      "commonControl",
      "objective",
      "domain"
```

AWS제어 카탈로그 ID 기반 정책의 예를 보려면 을 참조하십시오. 제어 카탈로그의 ID 기반 정책 예제 AWS

제어 카탈로그의 정책 조건 키 AWS

서비스별 정책 조건 키 지원: 예

관리자는 다음을 사용할 수 있습니다. AWS JSON정책을 통해 누가 무엇에 액세스할 수 있는지 지정합니다. 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.

명령문에 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에 여러 키를 지정하는 경우 AWS 논리 `AND` 연산을 사용하여 요소를 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 AWS 논리 `OR` 연산을 사용하여 조건을 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 액세스할 수 있는 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. 모두 보려면 AWS 글로벌 조건 키는 다음을 참조하십시오. AWSIAM사용 설명서의 글로벌 조건 컨텍스트 키.

AWS제어 카탈로그 조건 키 목록을 보려면 서비스 권한 부여 참조의 AWS 제어 카탈로그의 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 AWS제어 카탈로그에서 정의한 작업을 참조하십시오.

AWS제어 카탈로그 ID 기반 정책의 예를 보려면 을 참조하십시오. 제어 카탈로그의 ID 기반 정책 예제 AWS

ACLs제어 카탈로그에서 AWS

지원ACLs: 아니요

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지는 않지만 리소스 기반 정책과 JSON 비슷합니다.

ABAC제어 카탈로그 포함 AWS

지원 ABAC (정책의 태그): 아니요

속성 기반 액세스 제어 (ABAC) 는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. In AWS, 이러한 속성을 태그라고 합니다. IAM엔티티 (사용자 또는 역할) 및 여러 엔티티에 태그를 첨부할 수 있습니다. AWS 있습니다. 의 ABAC 첫 번째 단계는 엔티티와 리소스에 태그를 지정하는 것입니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC빠르게 성장하는 환경에서 유용하며 정책 관리가 복잡해지는 상황에도 도움이 됩니다.

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

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

에 대한 자세한 내용은 What is ABAC? 를 참조하십시오. ABAC IAM사용 설명서에서. 설정 ABAC 단계가 포함된 자습서를 보려면 사용 IAM설명서의 속성 기반 액세스 제어 사용 (ABAC) 을 참조하십시오.

제어 카탈로그에서 임시 자격 증명 사용 AWS

임시 자격 증명 지원: 예

약간 AWS 서비스 임시 자격 증명을 사용하여 로그인하면 작동하지 않습니다. 다음을 포함한 추가 정보는 AWS 서비스 임시 자격 증명으로 작업하려면 다음을 참조하십시오. AWS 서비스IAM사용 IAM 설명서에서 함께 사용할 수 있습니다.

에 로그인하면 임시 자격 증명을 사용하는 것입니다. AWS Management Console 사용자 이름과 암호를 제외한 모든 방법을 사용합니다. 예를 들어, 액세스할 때 AWS 회사의 Single Sign-On (SSO) 링크를 사용하면 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM사용 설명서의 역할 전환 (콘솔) 을 참조하십시오.

를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. AWS CLI 또는 AWS API. 그러면 해당 임시 자격 증명을 사용하여 액세스할 수 있습니다. AWS. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 의 임시 보안 자격 증명을 참조하십시오. IAM

AWS제어 카탈로그에 대한 서비스 간 보안 주체 권한

순방향 액세스 세션 지원 (FAS): 아니요

IAM사용자 또는 역할을 사용하여 작업을 수행하는 경우 AWS, 귀하는 주도자로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS전화를 건 주체의 권한을 사용합니다. AWS 서비스, 요청과 결합 AWS 서비스 다운스트림 서비스에 요청하기. FAS요청은 서비스가 다른 서비스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. AWS 서비스 또는 완료해야 할 리소스. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

AWS제어 카탈로그의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 권한을 위임하기 위한 역할 만들기를 참조하십시오. AWS 서비스(출처: IAM 사용 설명서).

> **Warning**
>
> 서비스 역할의 권한을 변경하면 AWS 제어 카탈로그 기능이 손상될 수 있습니다. AWS제어 카탈로그에서 이에 대한 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

제어 카탈로그의 서비스 연결 역할 AWS

서비스 링크 역할 지원: 아니요

서비스 연결 역할은 다음과 연결된 서비스 역할 유형입니다. AWS 서비스. 서비스가 사용자를 대신하여 작업을 수행하는 역할을 맡을 수 있습니다. 서비스 연결 역할은 다음과 같습니다. AWS 계정 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS 함께 작동하는 서비스. IAM 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

제어 카탈로그의 ID 기반 정책 예제 AWS

기본적으로 사용자와 역할에는 AWS 제어 카탈로그 리소스를 만들거나 수정할 권한이 없습니다. 또한 다음을 사용하여 작업을 수행할 수 없습니다. AWS Management Console, AWS Command Line Interface (AWS CLI), 또는 AWS API. 사용자에게 필요한 리소스에서 작업을 수행할 수 있는 권한을 부

여하기 위해 IAM 관리자는 IAM 정책을 생성할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

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

각 리소스 유형의 형식을 포함하여 AWS Control Catalog에서 정의한 작업 및 리소스 유형에 ARNs 대한 자세한 내용은 서비스 권한 부여 참조의 AWS제어 카탈로그의 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 사용자가 AWS 제어 카탈로그의 리소스를 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책은 누군가가 사용자 계정의 AWS 제어 카탈로그 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이러한 조치로 인해 비용이 발생할 수 있습니다. AWS 계정. ID 기반 정책을 만들거나 편집할 때는 다음 지침 및 권장 사항을 따르십시오.

- 시작해 보세요. AWS 관리형 정책 및 최소 권한 권한으로의 이동 — 사용자와 워크로드에 권한 부여를 시작하려면 다음을 사용하십시오. AWS 여러 일반 사용 사례에 대한 권한을 부여하는 관리형 정책. 다음 사이트에서 사용할 수 있습니다. AWS 계정. 를 정의하여 권한을 더 줄이는 것이 좋습니다. AWS 사용 사례에 맞는 고객 관리형 정책. 자세한 내용은 단원을 참조하세요.AWS 관리형 정책 또는 AWSIAM사용자 가이드의 작업 기능에 대한 관리형 정책.
- 최소 권한 적용 — IAM 정책으로 권한을 설정하는 경우 작업 수행에 필요한 권한만 부여하십시오. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 IAM 적용하는 방법에 대한 자세한 내용은 사용 설명서의 정책 및 권한을 참조하십시오. IAM IAM
- IAM정책의 조건을 사용하여 액세스를 더욱 제한할 수 있습니다. - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, 를 사용하여 모든 요청을 전송하도록 지정하는 정책 조건을 작성할 수 SSL 있습니다. 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. AWS 서비스예: AWS CloudFormation. 자세한 내용은 IAM사용 설명서의 IAMJSON정책 요소: 조건을 참조하십시오.
- IAMAccess Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 새 정책과 기존 정책을 검증하여 정책이 IAM 정책 언어 (JSON) 및 IAM 모범 사

례를 준수하는지 확인합니다. IAMAccess Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 검사와 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 사용 설명서의 IAMAccess Analyzer 정책 검증을 참조하십시오. IAM

- 다단계 인증 필요 (MFA) - 사용자 또는 루트 IAM 사용자가 필요한 시나리오가 있는 경우 AWS 계정 보안을 강화하려면 MFA 켜십시오. API작업 호출 MFA 시기를 요구하려면 정책에 MFA 조건을 추가하십시오. 자세한 내용은 IAM사용 설명서의 MFA -보호된 API 액세스 구성을 참조하십시오.

의 모범 사례에 IAM 대한 자세한 내용은 IAM사용 설명서의 보안 모범 사례를 참조하십시오. IAM

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 하는 정책을 만드는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 다음을 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다. AWS CLI 또는 AWS API.

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

사용자가 AWS 제어 카탈로그의 리소스를 볼 수 있도록 허용

다음 정책은 AWS Control Catalog의 도메인, 목표 및 공통 제어를 나열할 수 있는 권한을 부여합니다.

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageControlCatalogAccess",
            "Effect": "Allow",
            "Action": [
                "controlcatalog:ListDomains",
                "controlcatalog:ListObjectives",
                "controlcatalog:ListCommonControls"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS제어 카탈로그 ID 및 액세스 문제 해결

다음 정보를 사용하면 AWS 제어 카탈로그 및 작업 시 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 IAM 됩니다.

주제

- AWS제어 카탈로그에서 작업을 수행할 권한이 없습니다.
- 저는 iam을 수행할 권한이 없습니다. PassRole
- 제 외부에 있는 사람들을 허용하고 싶어요. AWS 계정 내 AWS 제어 카탈로그 리소스에 액세스하려면

AWS제어 카탈로그에서 작업을 수행할 권한이 없습니다.

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 권한이 없는 경우 발생합니다. controlcatalog:*GetWidget*

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 controlcatalog:GetWidget on resource: my-example-widget
```

이 경우 controlcatalog:*GetWidget*작업을 사용하여 *my-example-widget*리소스에 액세스할 수 있도록 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 다음 연락처로 문의하십시오. AWS 관리자에게 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 iam을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류가 발생하는 경우 AWS Control Catalog에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다. iam:PassRole

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

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

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

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

도움이 필요한 경우 다음 연락처로 문의하십시오. AWS 관리자에게 관리자는 로그인 자격 증명을 제공한 사람입니다.

제 외부에 있는 사람들을 허용하고 싶어요. AWS 계정 내 AWS 제어 카탈로그 리소스에 액세스하려면

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 (ACLs) 을 지원하는 서비스의 경우 해당 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- AWS제어 카탈로그가 이러한 기능을 지원하는지 여부를 알아보려면 을 참조하십시오. AWS제어 카탈로그의 작동 방식 IAM
- 여러 지역의 리소스에 대한 액세스를 제공하는 방법을 알아보려면 AWS 계정 소유한 사용자는 다른 IAM 사용자에게 액세스 권한 제공을 참조하십시오. AWS 계정IAM사용 설명서에 있는 소유권.
- 리소스에 대한 액세스 권한을 제3자에게 제공하는 방법 알아보기 AWS 계정액세스 제공을 참조하십시오. AWS 계정IAM사용 설명서의 제3자가 소유합니다.
- ID 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 사용 설명서의 외부 인증된 사용자에게 액세스 제공 (ID 페더레이션) 을 IAM 참조하십시오.
- 계정 간 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM IAM

제어 카탈로그의 규정 준수 검증 AWS

여부를 알아보려면 AWS 서비스 특정 규정 준수 프로그램의 범위에 속하는지 확인하려면 다음을 참조하십시오. AWS 서비스 규정 준수 프로그램별 범위 내 프로그램별 범위에서 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 을 참조하십시오. AWS 규정 준수 프로그램 .

다음을 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. AWS Artifact. 자세한 내용은 보고서 다운로드를 참조하십시오. AWS Artifact.

사용 시 귀하의 규정 준수 책임 AWS 서비스 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 기본 환경을 배포하기 위한 단계를 제공합니다. AWS 보안 및 규정 준수에 중점을 두고 있습니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서는 회사에서 사용할 수 있는 방법을 설명합니다. AWS 적격한 HIPAA 애플리케이션을 만들려면

> **Note**
>
> 전부는 아님 AWS 서비스 HIPAA자격이 있습니다. 자세한 내용은 HIPAA적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스 — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에는 보안 모범 사례가 요약되어 있습니다. AWS 서비스 또한 이 지침을 여러 프레임워크 (국립 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (), 국제 표준화 기구 (PCI) 포함) 전반의 보안 제어 체계에 매핑하십시오. ISO
- 다음 규칙을 사용하여 리소스를 평가합니다. AWS Config 개발자 가이드 — The AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이것은 AWS 서비스 내부 보안 상태를 포괄적으로 보여줍니다. AWS. Security Hub는 보안 제어를 사용하여 다음을 평가합니다. AWS 리소스를 제공하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- 아마존 GuardDuty — 이거 AWS 서비스 고객에 대한 잠재적 위협을 탐지합니다. AWS 계정의심스럽고 악의적인 활동이 있는지 환경을 모니터링하여 워크로드, 컨테이너 및 데이터를 모니터링합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하는 PCI DSS 등 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이것은 AWS 서비스 지속적으로 감사하는 데 도움이 됩니다. AWS 사용을 통해 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

의 탄력성 AWS 제어 카탈로그

The AWS 글로벌 인프라는 다음을 중심으로 구축됩니다. AWS 리전 및 가용 영역. AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

에 대한 자세한 내용은 AWS 리전 및 가용 영역은 다음을 참조하십시오. AWS 글로벌 인프라.

AWS제어 카탈로그의 인프라 보안

관리 서비스로서 AWS 제어 카탈로그는 다음을 통해 보호됩니다. AWS Amazon Web Services: 보안 프로세스 개요 백서에 설명된 글로벌 네트워크 보안 절차

다음을 사용합니다. AWS 네트워크를 통해 AWS 제어 카탈로그에 액세스하기 위한 API 통화를 게시했습니다. 클라이언트는 전송 계층 보안 (TLS) 1.0 이상을 지원해야 합니다. TLS1.2 이상을 권장합니다. 또한 클라이언트는 (임시 디피-헬만) 또는 (타원 곡선 임시 디피-헬만PFS) 와 같은 완벽한 순방향 비밀 DHE () 을 갖춘 암호 제품군을 지원해야 합니다. ECDHE Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID 및 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. IAM 또는 다음을 사용할 수 있습니다. AWS Security Token Service (AWS STS) 를 사용하여 요청에 서명하기 위한 임시 보안 자격 증명을 생성할 수 있습니다.

의 구성 및 취약성 분석 AWS 제어 카탈로그

구성 및 IT 제어는 두 회사 간의 공동 책임입니다. AWS 그리고 우리 고객인 당신. 자세한 내용은 다음을 참조하십시오. AWS 공동 책임 모델.

AWS 제어 카탈로그 모니터링

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

- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

를 사용하여 AWS 제어 카탈로그 API 호출 로깅 AWS CloudTrail

AWS Control Catalog는 AWS Control Catalog의 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공하는 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail AWS 제어 카탈로그에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 AWS 제어 카탈로그 콘솔에서의 호출과 AWS 제어 카탈로그 API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 AWS Control Catalog의 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 AWS Control Catalog에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

AWS 컨트롤 카탈로그 정보 CloudTrail

CloudTrail 계정을 생성할 AWS 계정 때 활성화됩니다. AWS Control Catalog에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

AWS Control Catalog의 이벤트를 AWS 계정포함하여 진행 중인 이벤트 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 AWS 제어 카탈로그 작업은 AWS 제어 카탈로그 API 참조에 의해 CloudTrail 기록되고 문서화됩니다. . 예를 들어, `ListCommonControlsListObjectives`, 및 `ListDomains` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

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

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증 정보를 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail UserIdentity 요소를 참조하십시오.

AWS 컨트롤 카탈로그 로그 파일 항목의 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `ListDomains` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
```

```
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"controlcatalog.amazonaws.com",
      eventName:"ListDomains",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters: null,
      responseElements: null,
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
}
```

인터페이스 엔드포인트를 사용한 액세스 AWS 제어 카탈로그 (AWS PrivateLink)

를 AWS PrivateLink 사용하여 제어 VPC 카탈로그와 AWS 제어 카탈로그 간에 비공개 연결을 만들 수 있습니다. 인터넷 게이트웨이, NAT 장치VPC, VPN 연결 또는 AWS Direct Connect 연결을 사용하지 않고도 마치 집에 있는 것처럼 AWS 제어 카탈로그에 액세스할 수 있습니다. 의 인스턴스는 AWS 제어 카탈로그에 액세스하는 데 퍼블릭 IP 주소가 VPC 필요하지 않습니다.

AWS PrivateLink에서 제공되는 인터페이스 엔드포인트를 생성하여 이 프라이빗 연결을 설정합니다. 인터페이스 엔드포인트에 대해 사용 설정하는 각 서브넷에서 엔드포인트 네트워크 인터페이스를 생성합니다. 제어 카탈로그로 향하는 트래픽의 진입점 역할을 하는 요청자 관리형 네트워크 인터페이스입니다. AWS

자세한 내용은 가이드의 액세스를 참조하십시오 AWS 서비스 . AWS PrivateLinkAWS PrivateLink

AWS 제어 카탈로그 고려 사항

AWS 제어 카탈로그의 인터페이스 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 고려 사항을 검토하십시오.

AWS 제어 카탈로그는 인터페이스 엔드포인트를 통해 모든 API 작업에 대한 호출을 지원합니다.

AWS 제어 카탈로그용 인터페이스 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface (AWS CLI) 를 사용하여 AWS 제어 카탈로그용 인터페이스 엔드포인트를 생성할 수 있습니다. 자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트 생성을 참조하십시오.

다음 서비스 이름을 사용하여 AWS 제어 카탈로그용 인터페이스 엔드포인트를 생성합니다.

```
com.amazonaws.region.controlcatalog
```

인터페이스 엔드포인트에 DNS 대해 비공개를 활성화하면 기본 지역 DNS 이름을 사용하여 AWS Control Catalog에 API 요청을 보낼 수 있습니다. 예: `service-name.us-east-1.amazonaws.com`.

엔드포인트의 엔드포인트 정책 생성

엔드포인트 정책은 인터페이스 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 엔드포인트를 통해 AWS Control Catalog에 대한 전체 액세스를 허용합니다. 에서 AWS 제어 카탈로그에 허용되는 액세스를 제어하려면 사용자 지정 엔드포인트 정책을 인터페이스 엔드포인트에 연결하십시오. VPC

엔드포인트 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 주체 (AWS 계정, IAM 사용자, IAM 역할)
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

자세한 내용은AWS PrivateLink 가이드의 엔드포인트 정책을 사용하여 서비스에 대한 액세스 제어를 참조하세요.

예: AWS 제어 카탈로그 작업에 대한 VPC 엔드포인트 정책

다음은 사용자 지정 엔드포인트 정책의 예입니다. 이 정책을 인터페이스 엔드포인트에 연결하면 모든 리소스의 모든 보안 주체에 대해 나열된 AWS 제어 카탈로그 작업에 대한 액세스 권한이 부여됩니다.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "controlcatalog:ListDomains",
            "controlcatalog:ListObjectives",
            "controlcatalog:ListCommonControls"
         ],
         "Resource":"*"
      }
   ]
}
```

> **Note**
>
> `GetControl`및 `ListControls` API 작업에는 다른 권한, 즉 기본 전체 권한이 필요합니다. 예를 들어, 기본 엔드포인트 정책을 참조하십시오. 다른 AWS Control Tower API 작업은 지원되지 않습니다 AWS PrivateLink.

AWS 제어 카탈로그 보안 정보 가이드의 문서 기록

다음 표에는 AWS 제어 카탈로그의 설명서 릴리스가 설명되어 있습니다.

변경 사항	설명	날짜
최초 릴리스	AWS 제어 카탈로그 API 및 보안 정보 가이드의 초기 릴리스.	2024년 4월 8일

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