사용자 가이드

AWS 청구 담당자

AWS 청구 담당자: 사용자 가이드

Table of Contents

AWS 빌링 컨덕터란 무엇입니까?

AWS Billing Conductor 차지백 요구 사항이 있는 AWS Marketplace 채널 파트너 (파트너) 및 조직을 위한 맞춤형 청구 서비스입니다. 파트너의 경우 지불 거절은 고객으로부터 대금을 받기 위한 전제 조건이며 청구 한도 AWS 계정 또는 청구 기준을 따릅니다. AWS Organizations 조직의 경우 차지백 활동을 통해 조직은 특정 팀 (예: 계정 모음) 의 비용을 정확한 내부 예산 또는 손익 (P&L) 명세서에 할당해야 합니다.

이러한 활동을 달성하기 위해 Billing Conductor는 고객이 비용을 두 번째로 견적 버전으로 만들어 고객 또는 계정 소유자와 공유할 수 있도록 합니다. 견적 비용은 Billing Conductor 관리 계정 (청구 그룹에 할당된 계정) 내 사용량을 Billing Conductor 내에서 정의된 가격 책정 요율로 나타냅니다 (예: 글로벌 가격 책정 규칙을 사용하여 모든 사용량에 공개 가격 적용).

> **Note**
>
> 고객은 한 달 내내 청구 가능 비용 (AWS 청구서 일치) 과 견적 비용 (청구 담당자 구성과 일치) 간의 미미한 사용량 차이를 확인할 수 있습니다. 하지만 청구서가 발행된 후 매월 말에 사용량 값이 일치합니다 AWS .

견적 비용을 정의하면 고객은 다음 사용 사례 중 하나에 맞게 비용을 균일하게 모델링할 수 있습니다.

1. 고객 계약 (파트너 사용 사례는 외부에서 협상할 수 있음) AWS
2. 내부 회계 관행 (대개 조직별 사용 사례)

Billing Conductor 구성은 크레딧 공유 또는 예약 인스턴스 AWS 또는 Savings Plans와 같은 약정 기반 할인 등 고객의 기존 청구서 또는 청구 구성 (예: 크레딧 공유) 에 영향을 주지 않습니다.

고객은 다음 작업을 수행하여 관리 계정에서 견적 비용을 분석할 수 있습니다.

- Billing Conductor 내에서 마진 (동일한 계정 세트에 대한 견적 비용과 청구 가능 비용 간의 차이) 을 분석합니다.
- 청구 세부 정보 페이지에서 월별 견적 비용을 확인하세요.
- 청구 그룹별 AWS Cost and Usage Report (CUR) 생성

Billing Conductor 관리 계정 (청구 그룹의 계정) 은 비용 및 사용 보고서 AWS Cost Explorer, 청구 대시보드 및 청구 세부 정보 페이지에서 견적 비용을 분석할 수 있습니다.

빌링 컨덕터 콘솔에서 또는 빌링 컨덕터 API를 사용하여 청구 그룹, 가격 책정 계획, 가격 책정 규칙 및 사용자 지정 항목을 구성할 수 있습니다.

AWS 청구서 서비스 할당량에 대한 자세한 내용은 을 참조하십시오. 할당량 및 제한

주제

- 빌링 컨덕터의 특징 AWS
- 관련 서비스

빌링 컨덕터의 특징 AWS

AWS 청구 담당자 기능을 사용하여 다음 작업을 수행할 수 있습니다.

그룹 계정

견적 비용을 종합적으로 볼 수 있도록 계정을 결제 그룹으로 정리하세요. 서비스 간 할인과 AWS 프리 티어 같은 개별 고객 혜택을 각 그룹별로 시뮬레이션하세요.

맞춤형 가격

글로벌 또는 특정 마크업 또는 할인을 설정하고 프리 티어 액세스를 제어하십시오.

요금 및 크레딧

일회성 또는 정기 균일 요금 또는 백분율 기반 요금이나 크레딧을 청구 그룹에 추가하세요.

견적 분석

결제 콘솔에서 가격 구성을 기반으로 비용을 분석하세요. 결제 그룹의 계정은 AWS Cost Explorer의 견적 비용을 시각화하고 예측하고 사용자 지정 보고서를 생성할 수 있습니다. 기본 계정은 결제 그룹의 계정에서 발생한 모든 비용을 교차 계정 보기로 볼 수 있는 반면, 기본 계정이 아닌 계정에는 자체 비용이 표시됩니다.

보고

각 결제 그룹에 대한 비용 및 사용 보고서를 구성하세요.

요금 분석

청구 그룹 마진 보고서를 사용하여 적용된 AWS 요율을 실제 요율과 비교하세요.

관련 서비스

AWS 결제 콘솔

AWS 빌링 콘솔은 학생, 스타트업 기업부터 대기업까지 모든 AWS 고객을 위한 포털입니다. 콘솔을 사용하여 AWS 계정에서 실행되는 리소스를 확인하고, 청구 기본 설정을 관리하고, 결제에 필요한 결제 아티팩트에 액세스할 수 있습니다. AWS또한 AWS 결제 콘솔은 계정 지출에 대한 수준 높은 설명을 제공하며 AWS Cost Management 제품에 제품을 등록하기 위한 시작점 역할을 합니다.

자세한 정보는 AWS Billing 사용 설명서를 참조하세요.

AWS Cost Explorer

Cost Explorer 인터페이스를 사용하여 시간 경과에 따른 AWS 비용 및 사용량을 시각화하고 이해하고 관리할 수 있습니다. 비용 및 사용량 데이터를 분석하는 사용자 지정 보고서를 만들어 빠르게 시작하십시오. 데이터를 높은 수준(예: 모든 계정의 총 비용 및 사용량)으로 분석하거나 비용 및 사용량 데이터를 심층적으로 분석하여 추세를 파악하고 비용 동인을 찾아내며 이상 징후를 찾아내십시오.

자세한 정보는 다음 주제를 참조하십시오.

- 견적 비용에 대한 임시 분석 수행 AWS Cost Explorer
- AWS Cost Management 사용 설명서를 사용하여 AWS Cost Explorer비용을 분석하십시오.

AWS 비용 및 사용 보고서

AWS 비용 및 사용 보고서 (AWS CUR) 에는 사용 가능한 가장 포괄적인 비용 및 사용 데이터 세트가 포함되어 있습니다. 비용 및 사용 보고서를 사용하여 소유한 Amazon Simple Storage Service (Amazon S3) 버킷에 AWS 결제 보고서를 게시할 수 있습니다. 시간이나 일, 제품이나 제품 리소스, 또는 직접 정의한 태그를 기준으로 비용을 구분한 보고서를 받을 수 있습니다.

AWS 하루에 한 번 CSV (쉼표로 구분된 값) 또는 Apache Parquet 형식으로 버킷의 보고서를 업데이트합니다. Microsoft Excel 또는 Apache OpenOffice Calc와 같은 스프레드시트 소프트웨어를 사용하여 보고서를 볼 수 있습니다. Amazon S3 또는 Amazon Athena API를 사용하여 애플리케이션에서 액세스할 수도 있습니다.

AWS 비용 및 사용 보고서는 AWS 사용량을 추적하고 계정과 관련된 예상 요금을 제공합니다. 각 보고서에는 AWS 계정에서 사용하는 AWS 제품, 사용 유형 및 운영의 고유한 조합에 대한 항목이 포함되어 있습니다.

AWS Identity and Access Management (IAM)

AWS 빌링 컨덕터 서비스는 AWS Identity and Access Management (IAM) 과 통합되었습니다. IAM과 AWS Billing Conductor를 함께 사용하면 내 계정에서 일하는 다른 사람들이 작업을 완료하는 데 필요한 만큼만 액세스할 수 있도록 할 수 있습니다.

또한 IAM을 사용하여 모든 리소스에 대한 액세스를 제어할 수 있습니다. AWS 여기에는 결제 정보가 포함되지만 이에 국한되지는 않습니다. 계정 구조를 설정하는 데 너무 깊이 들어가기 전에 IAM의 기본 개념과 모범 사례를 숙지하는 것이 중요합니다. AWS

IAM 사용 방법에 대한 자세한 내용은 IAM이란? 및 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하십시오.

AWS Organizations (통합 결제)

AWS 제품 및 서비스는 소규모 스타트업부터 대기업에 이르기까지 모든 규모의 회사를 수용할 수 있습니다. 회사 규모가 크거나 성장할 가능성이 있는 경우 통합 결제를 사용하여 회사의 구조를 반영하는 여러 AWS 계정을 설정할 수 있습니다. 예를 들어 회사 전체의 계정 하나와 개별 직원의 계정을 만들거나, 회사 전체용 계정 하나를 만들고 각 직원은 IAM 사용자로 이용할 수 있습니다. 회사 전체의 계정, 회사 내 부서별 또는 팀별 계정, 그리고 각 직원의 계정을 만들 수 있습니다.

여러 계정을 생성하는 경우 AWS Organizations 의 통합 결제 기능을 사용하여 관리 계정 아래 모든 멤버 계정을 통합하여 하나의 청구서만 받을 수 있습니다. 자세한 내용은 AWS Billing 사용자 설명서의 조직의 통합 결제를 참조하십시오.

AWS Billing Conductor 대시보드 이해하기

AWSBilling Conductor 대시보드는 사용자 지정 요금 기준이 미치는 영향을 이해하는 데 도움이 되는 주요 지표에 대한 개괄적인 요약을 제공합니다.

핵심 성능 지표

이 섹션에서는 AWS Billing Conductor 대시보드에서 사용할 수 있는 주요 성과 지표(KPI)를 정의합니다. KPI는 모두 당월 누계 수치입니다. AWS Organizations에 계정을 만들거나 계정을 추가하면 해당 계정에 이 KPI가 누적됩니다. 결제 그룹을 삭제하면 해당 결제 그룹의 계정에도 이 KPI가 누적됩니다.

- 청구 금액 – 적용된 요금제에서 정의된 사용자 지정 요금을 기준으로 모든 결제 그룹에서 누적된 사용량에 대한 누계 요금입니다. 결제 그룹 외부에서 구매한 약정 기반 할인, 비공개 가격 또는 청구 가능한 도메인에서 사용한 크레딧은 계산에 반영되지 않습니다. 약정 기반 할인의 예로는 예약 인스턴스 및 절감형 플랜 등이 있습니다.
- AWS비용 – AWS 청구서에 적힌 예상 요금에 따라 모든 결제 그룹에서 누적된 사용량에 대한 월간 누계 요금입니다. 계산에는 결제 그룹 외부에서 구매한 약정 기반 할인(해당 혜택이 청구 가능한 도메인에 적용된 경우), 모든 비공개 가격, 대량 구매 할인, 크레딧이 포함됩니다. 약정 기반 할인의 예로는 예약 인스턴스 및 절감형 플랜 등이 있습니다.
- 마진 – 모든 결제 그룹에 의해 누적 집계된 월간 마진입니다. 마진은 청구 금액에서 AWS 비용을 빼서 계산됩니다. 요금제, 적용된 사용자 지정 품목과 같은 요소에 따라 마진은 음수가 될 수도 있습니다.

  > **Note**
  >
  > 청구 기간 이후 조정은 과거 마진에 영향을 미칩니다. 자세한 내용은 결제 그룹별 마진 분석 섹션을 참조하세요.

- 결제 그룹 – 기본 계정 및 관련 요금제를 사용하는 상호 배타적인 계정 그룹의 수입니다.
- 모니터링되는 계정 – 통합 결제 그룹 내에서 현재 결제 그룹에 할당된 계정 수입니다.
- 모니터링되지 않는 계정 – 통합 결제 그룹 내에서 결제 그룹에 할당되지 않은 계정의 수입니다.

AWS Billing Conductor에 대한 기타 정의

이 섹션에서는 서비스를 효과적으로 사용할 수 있도록 AWS Billing Conductor 전체에서 사용되는 기타 용어를 정의합니다.

- 청구 가능 – AWS 청구서 계산 시 AWS(이)가 생성하고 편향된 계산으로 사용되는 청구 결과입니다.
- 견적 – AWS Billing Conductor가 생성한 결과입니다. 이는 요율 관리 (요금 구성) 및 집계된 계정 가시성 (결제 그룹) 에서 원하는 변경 사항과 일치합니다.
- 리소스 값 – 백분율 기반 사용자 지정 품목을 계산하는 데 사용되는 입력입니다. 리소스 값에는 결제 그룹의 누적된 비용과 청구 기간 동안 지정된 결제 그룹과 연결된 모든 일반 사용자 지정 품목이 포함됩니다.

청구 금액별 상위 5개 결제 그룹 보기

시각적 보기와 테이블 보기를 참조하면 수익을 창출하는 상위 5개 결제 그룹을 이해할 수 있습니다. 기존 결제 그룹을 관리하려면 대시보드 페이지에서 결제 그룹 관리를 선택합니다.

결제 그룹, 요금 구성, 사용자 지정 품목 생성

이 섹션에서는 Billing Conductor에서 AWS 청구 그룹, 가격 구성 및 사용자 지정 품목을 생성하는 방법을 보여줍니다. 또한 각 섹션은 각 항목을 생성한 후 결제 그룹 테이블, 요금 규칙 테이블, 사용자 지정 품목 테이블을 사용하는 방법에 대한 개요를 제공합니다.

주제

결제 그룹 생성

AWS Billing Conductor를 사용하여 청구 그룹을 생성하여 계정을 구성할 수 있습니다. 기본적으로 관리자 권한이 있는 지급인 계정은 결제 그룹을 만들 수 있습니다. 각 결제 그룹은 상호 배타적입니다. 즉, 특정 청구 기간 동안 계정은 하나의 결제 그룹에만 속할 수 있습니다. 결제 그룹 분류는 즉시 확인할 수 있지만, 결제 그룹을 만든 후 그룹의 사용자 지정 요율이 반영되기까지는 최대 24시간이 걸립니다.

> **Note**
>
> 월 중순에 결제 그룹 간에 계정을 이동하면 두 결제 그룹이 청구 기간 시작 시점으로 다시 계산되기 시작합니다. 월 중순에 계정을 이전해도 이전 청구 기간에는 영향을 미치지 않습니다.

다음 단계에 따라 결제 그룹을 생성합니다.

결제 그룹 생성

1. https://console.aws.amazon.com/billingconductor/ 에서 빌링 컨덕터에 AWS Management Console 로그인하고 AWS 빌링 컨덕터를 엽니다.
2. 탐색 창에서 결제 그룹을 선택합니다.
3. 결제 그룹 생성을 선택합니다.

4. 결제 그룹 세부 정보에는 결제 그룹의 이름을 입력합니다. 이름 지정 제한에 대한 내용은 할당량 및 제한 섹션을 참조하십시오.
5. (선택 사항) 설명에 결제 그룹에 대한 설명을 입력합니다.
6. 요금제의 경우, 결제 그룹과 연결할 요금제를 선택하십시오. 요금제를 생성하려면 요금제 생성 섹션을 참조하십시오.
7. (선택 사항) 추가 설정의 경우, 결제 그룹에 대한 자동 계정 연결을 활성화할 수 있습니다.

> **참고**
>
> - 하나의 결제 그룹만 자동 계정 연결을 설정할 수 있습니다.
> - 이 기능을 활성화하면 조직에 생성되거나 추가된 계정이 자동으로 이 결제 그룹에 연결됩니다.
> - 현재 CloudTrail 로그 기록이 있는 경우 CloudTrail 로그에서 자동 계정 연결을 검토할 수 있습니다.

8. 계정에서 결제 그룹에 추가할 계정을 하나 이상 선택하거나 조직 단위 가져오기를 선택하여 조직 단위 내에 있는 계정을 자동으로 선택합니다. OU 가져오기 기능에 대한 액세스 권한을 부여하는 정책 예제는 Billing Conductor에 조직 단위 가져오기 기능에 대한 액세스 권한 부여 섹션을 참조하십시오.

   테이블 필터를 사용하면 계정 이름, 계정 ID 또는 계정과 연결된 루트 이메일 주소를 기준으로 정렬할 수 있습니다.
9. 기본 계정은 청구 그룹 전체의 견적 비용 및 사용량을 볼 수 있는 기능을 상속하며 청구 그룹에 대한 견적 비용 및 사용 보고서 (AWS CUR) 를 생성할 수 있습니다.

   이번 달에 조직에 가입한 기본 계정을 선택하면 해당 청구 그룹의 모든 계정에 대한 견적 비용에는 기본 계정이 조직에 가입한 이후 발생한 비용 및 사용량만 포함됩니다. 가입일을 확인하려면 가입일 확인을 선택합니다. 자세한 정보는 기본 계정 가입일의 중요성 이해을 참조하세요.
10. 결제 그룹 생성을 선택합니다.

> **참고**
>
> - 9단계에서 기본 계정을 선택해야 합니다. 결제 그룹을 만든 후에는 기본 계정을 변경할 수 없습니다. 새 기본 계정을 할당하려면 결제 그룹을 삭제하고 계정을 재그룹화하십시오. 지급인 계정을 결제 그룹에 포함할 수는 있지만, 지급인 계정에 기본 계정의 역할을 할당할 수는 없습니다.

- 결제 그룹의 기본 계정이 조직을 떠나고 이 결제 그룹에 자동 계정 연결이 활성화되어 있는 경우, 월말까지 계속해서 계정이 자동으로 연결됩니다. 그러면 결제 그룹이 자동으로 삭제됩니다. 기존 결제 그룹에 자동 계정 연결을 활성화하거나 다른 결제 그룹을 만들 수 있습니다.

결제 그룹 테이블

결제 그룹을 생성한 후 결제 그룹의 세부 정보를 필터링 가능한 테이블에서 볼 수 있습니다. 다음 차원을 사용하여 필터링할 수 있습니다.

- 결제 그룹 이름
- 기본 계정 이름
- 기본 계정 ID
- 계정 수
- 요금제 이름

각 결제 그룹의 세부 정보를 보려면 테이블에서 결제 그룹 이름을 선택하십시오. 자동 계정 연결 기능을 사용하도록 설정한 결제 그룹에는 결제 그룹 이름 옆에 자동 연결 아이콘이 있습니다.

요금 규칙 생성

AWS Billing Conductor에서 가격 책정 규칙을 생성하여 청구 그룹 전체의 청구 요금을 사용자 지정할 수 있습니다. 요금 규칙은 범위에 따라 글로벌, 서비스별, 청구 주체별 또는 SKU별로 다를 수 있습니다. 요금 규칙을 사용하여 할인율 또는 인상율을 적용할 수 있습니다. 범위는 겹치지 않습니다. 범위가 서로 다른 요금 규칙이 단일 요금제에 포함된 경우, 범위가 가장 세분화된 것부터 가장 세분화되지 않은 것까지 적용됩니다. 글로벌 요금 규칙의 경우 `Always Free Tier` 요금을 비활성화하거나 활성화하도록 선택할 수도 있습니다. Always Free Tier가 비활성화된 요금 규칙은 사용 유형 또는 작업에 대한 첫 번째 유료 티어로 기본 설정됩니다. 기본적으로 관리자 권한이 있는 지급인 계정은 요금 규칙을 생성할 수 있습니다. 결제 그룹에 요금 규칙을 적용한 후 결제 그룹의 사용자 지정 요금이 반영되었는지 확인하는 데 최대 24시간이 걸립니다.

단일 요금제를 여러 결제 그룹에 적용할 수 있습니다.

다음 단계에 따라 요금 규칙을 생성합니다.

요금 규칙 생성

1. https://console.aws.amazon.com/billingconductor/ 에서 AWS 빌링 컨덕터를 엽니다.
2. 탐색 창에서 요금 구성을 선택합니다.
3. 요금 규칙 탭을 선택합니다.
4. 요금 규칙 생성을 선택합니다.
5. 요금 규칙 세부 정보를 보려면 요금 규칙의 이름을 입력합니다. 이름 지정 제한에 대한 내용은 할당량 및 제한 섹션을 참조하십시오.
6. (선택 사항) 설명에 요금 규칙에 대한 설명을 입력합니다.
7. 범위에서,`Global`, `Service`, `Billing entity` 또는 SKU을(를) 선택합니다.
   - 글로벌 - 모든 사용에 적용됩니다.
   - 서비스 - 특정 서비스에만 적용됩니다. 서비스를 선택할 때는 요금을 구성할 서비스 코드를 선택하십시오. 서비스를 선택할 때는 Price List Query API에서 조정하려는 서비스 코드를 선택합니다.
   - 청구 주체 - 특정 청구 주체에만 적용됩니다. 청구 주체란 서비스를 판매하는 업체 AWS, 계열사 또는 서비스를 판매하는 타사 제공업체에서 제공하는 서비스를 판매하는 업체를 말합니다. AWS Marketplace
   - SKU - 서비스 (제품) 코드, 사용 유형 및/또는 운영의 고유한 조합에만 적용됩니다.
8. 유형에서 할인, 마크업 또는 계층화를 선택합니다.

   > **Note**
   >
   > 계층화는 글로벌 및 서비스 범위 요금 규칙에만 사용할 수 있습니다.

9. 백분율에는 백분율 금액을 입력합니다.

   0 백분율로 입력하면 요금제는 AWS 온디맨드 요금을 기본값으로 사용합니다. 10진수 값을 입력하면 가장 가까운 소수점 두 자리로 반올림됩니다.
10. 계층화 유형의 경우 계층화 구성 아래의 확인란을 선택하여 Always Free Tier를 비활성화하거나 활성화된 상태로 둘 수 있습니다. 명시적으로 비활성화하지 않는 한 Always Free Tier는 활성화됩니다.
11. (선택 사항) 동일한 워크플로에서 다른 요금 규칙을 만들려면 요금 규칙 추가를 선택합니다.
12. 요금 규칙 생성을 선택합니다.

요금 규칙 테이블

요금 규칙을 생성한 후 필터링 가능한 테이블에서 요금 규칙의 세부 정보를 볼 수 있습니다. 다음 차원으로 필터링할 수 있습니다.

- 요금 규칙 이름
- 범위
- 유형
- Details
- Rate

요금제 생성

AWS Billing Conductor에서 가격 책정 플랜을 생성하여 청구 그룹 전체의 청구 세부 정보 출력을 사용자 지정할 수 있습니다. 기본적으로 관리자 권한이 있는 지급인 계정은 요금제를 생성할 수 있습니다. 결제 그룹에 요금제를 적용한 후 결제 그룹의 사용자 지정 요금이 반영되기까지 최대 24시간이 소요됩니다.

단일 요금제를 여러 결제 그룹에 적용할 수 있습니다.

> **Note**
>
> 요금제 업데이트는 요금제와 연결된 각 결제 그룹의 청구서 세부 정보에도 영향을 미칩니다. 요금제가 결제 그룹 또는 결제 그룹 집합과 연결된 경우 이 변경은 현재 청구 기간에만 영향을 미칩니다. 이전 청구 기간은 동일하게 유지됩니다.

다음 단계에 따라 요금제를 생성합니다.

요금제 생성

1. https://console.aws.amazon.com/billingconductor/ 에서 AWS 빌링 컨덕터를 엽니다.
2. 탐색 창에서 요금 구성을 선택합니다.
3. 요금제 탭에서 요금제 생성을 선택합니다.
4. 요금제 세부 정보에 요금제의 이름을 입력합니다. 이름 지정 제한에 대한 내용은 할당량 및 제한 섹션을 참조하십시오.

5. (선택 사항) 설명에 요금제에 대한 설명을 입력합니다.
6. 요금 규칙 테이블에서 요금제와 연결할 요금 규칙을 선택합니다. 요금 규칙 이름, 범위, 세부 정보, 유형 또는 요율별로 요금 규칙을 필터링할 수 있습니다.
7. 요금제 생성을 선택합니다.

요금제 테이블

요금제를 생성한 후 요금제의 세부 정보를 필터링 가능한 테이블에서 볼 수 있습니다. 다음 차원으로 필터링할 수 있습니다.

- 요금제 이름
- 설명
- 요금제와 관련된 요금 규칙의 수

결제 그룹당 사용자 지정 품목 생성

개인화된 품목을 AWS Billing Conductor 생성하여 청구 그룹 AWS 계정 내 지정된 항목에 적용하는 데 사용합니다.

사용자 지정 품목을 사용하여 비용과 할인을 할당할 수 있습니다. 사용자 지정 품목은 고정 요금 또는 백분율 요금으로 계산할 수 있습니다. 리소스를 포함하거나 제외하도록 백분율 기반 사용자 지정 라인 항목을 구성하세요. 이러한 리소스에는 청구 그룹 비용 및 청구 기간 동안 청구 그룹과 연결된 기타 일반 사용자 지정 항목이 포함됩니다. 그런 다음 사용자 지정 품목이 한 달 동안 적용되거나 여러 달 동안 다시 발생하도록 설정할 수 있습니다.

사용자 지정 품목 생성의 일반적인 사용 사례에는 다음이 포함되지만 이에 국한되지는 않습니다.

- 수수료 배분 AWS Support
- 공유 서비스 비용 할당
- 관리 서비스 수수료 적용
- 세금 적용
- 크레딧 분배
- RI 및 절감형 플랜 절감액 분배 (온디맨드와 반대)
- 기관 크레딧 및 할인 행 항목 추가

정액제 사용자 지정 품목 생성

다음 단계를 사용하여 개별 결제 그룹에 크레딧 또는 수수료 항목을 적용하는 사용자 지정 품목을 생성하십시오.

사용자 지정 품목 생성

1. https://console.aws.amazon.com/billingconductor/ 에서 AWS 빌링 컨덕터를 개설하세요.
2. 탐색 창에서 사용자 지정 품목을 선택합니다.
3. 사용자 지정 품목 생성을 선택합니다.
4. 사용자 지정 품목 세부 정보에 사용자 지정 품목의 이름을 입력합니다. 이름 지정 제한에 대한 내용은 할당량 및 제한 섹션을 참조하십시오.
5. 설명에 사용자 지정 품목의 설명을 입력합니다. 글자 수 제한은 255자입니다.
6. Billing 기간의 경우 기존 청구 기간 또는 이전 청구 기간을 선택합니다.
7. 기간에서 1개월 또는 반복(정의된 종료일 없음)을 선택합니다.
8. 결제 그룹의 경우 결제 그룹을 선택합니다. 사용자 지정 요금은 한 번에 하나의 결제 그룹에만 연결할 수 있습니다.
   - (선택 사항) 할당된 계정의 경우 원하는 결제 그룹 계정에 사용자 지정 항목을 적용할 수 있습니다. 사용자 지정 품목은 기본적으로 선택한 결제 그룹의 기본 계정에 적용됩니다.
9. 사용자 지정 품목 유형에 대해 정액 청구를 선택합니다.
10. 청구 유형을 선택하고 금액을 입력합니다.

    할인 행 항목은 크레딧을 추가합니다. 이렇게 하면 선택한 결제 그룹에 청구되는 금액이 줄어듭니다. 마크업 행 항목은 요금을 추가합니다. 이렇게 하면 선택한 결제 그룹에 청구되는 금액이 늘어납니다. 모든 사용자 지정 품목은 USD 기준입니다.
11. 생성을 선택하세요.

백분율 요금 사용자 지정 품목 생성

다음 단계를 사용하여 개별 결제 그룹에 크레딧 또는 수수료 항목을 적용하는 사용자 지정 품목을 생성하십시오.

사용자 지정 품목 생성

1. https://console.aws.amazon.com/billingconductor/ 에서 AWS 빌링 컨덕터를 엽니다.

2. 탐색 창에서 사용자 지정 품목을 선택합니다.
3. 사용자 지정 품목 생성을 선택합니다.
4. 사용자 지정 품목 세부 정보에 사용자 지정 품목의 이름을 입력합니다. 이름 지정 제한에 대한 내용은 할당량 및 제한 섹션을 참조하십시오.
5. 설명에 사용자 지정 품목의 설명을 입력합니다. 글자 수 제한은 255자입니다.
6. Billing 기간의 경우 기존 청구 기간 또는 이전 청구 기간을 선택합니다.
7. 기간에서 1개월 또는 반복(정의된 종료일 없음)을 선택합니다.
8. 결제 그룹의 경우 결제 그룹을 선택합니다. 사용자 지정 요금은 한 번에 하나의 결제 그룹에만 연결할 수 있습니다.

    - (선택 사항) 할당된 계정의 경우 원하는 결제 그룹 계정에 사용자 지정 항목을 적용할 수 있습니다. 사용자 지정 품목은 기본적으로 선택한 결제 그룹의 기본 계정에 적용됩니다.
9. 사용자 지정 품목 유형에 대한 요금 비율을 선택하세요.
10. 청구 유형을 선택하고 금액을 입력합니다.

    할인 행 항목은 크레딧을 추가합니다. 이렇게 하면 선택한 결제 그룹에 청구되는 금액이 줄어듭니다. 마크업 행 항목은 요금을 추가합니다. 이렇게 하면 선택한 결제 그룹에 청구되는 금액이 늘어납니다. 모든 사용자 지정 품목은 USD 기준입니다.
11. (선택 사항) 리소스 값의 경우 계산에 포함할 값을 선택합니다. 기본적으로 결제 그룹 총 비용이 리소스로 선택됩니다. 여기에는 모든 플랫 사용자 지정 품목이 제외됩니다.

    - (선택 사항) 기본적으로 절감형 플랜 할인이 포함됩니다. 계산에서 제외하려면 절감형 플랜 할인 제외 확인란을 선택합니다.
12. (선택 사항) 하나 이상의 플랫 커스텀 라인 항목을 포함하세요. 테이블에서 백분율 기반 계산에 포함하려는 해당 플랫 사용자 지정 라인 항목을 각각 선택합니다.

    > **Note**
    >
    > 연결된 리소스 없이 백분율 사용자 지정 품목을 만들 수 있습니다. 이러한 사용자 지정 품목은 청구 데이터의 `$0.00` 값을 보여줍니다.
13. 생성을 선택하세요.

사용자 지정 품목 테이블

사용자 지정 품목을 만든 후 필터링 가능한 표에서 지정 품목의 세부 정보를 볼 수 있습니다. 다음 차원으로 필터링할 수 있습니다.

- 행 항목 이름
- 행 항목 설명
- 해당 청구 금액
- 해당 행 항목이 속하는 결제 그룹
- 해당 행 항목이 생성된 날짜

이전 청구 기간에 생성한 사용자 지정 품목을 보려면 날짜 선택기 드롭다운 목록을 사용하십시오.

사용자 지정 품목 편집

다음 단계에 따라 사용자 지정 품목을 편집할 수 있습니다.

사용자 지정 품목을 편집하려면

1. https://console.aws.amazon.com/billingconductor/ 에서 AWS 빌링 컨덕터를 엽니다.
2. 탐색 창에서 사용자 지정 품목을 선택합니다.
3. 사용자 지정 품목 생성을 선택합니다.
4. 편집할 사용자 지정 품목을 선택합니다.
5. 편집을 선택합니다.
6. 편집하려는 파라미터를 변경합니다.

> **Note**
>
> 청구 기간, 청구 그룹, 할당된 계정, 청구 유형 (고정 또는 백분율) 또는 청구 금액 유형 (크레딧 또는 수수료) 은 변경할 수 없습니다.

7. 변경 사항 저장를 선택합니다.

사용자 지정 품목 삭제

다음 단계에 따라 사용자 지정 품목을 삭제합니다.

사용자 지정 품목을 편집하려면

1. https://console.aws.amazon.com/billingconductor/ 에서 AWS 빌링 컨덕터를 엽니다.
2. 탐색 창에서 사용자 지정 품목을 선택합니다.
3. 사용자 지정 품목 생성을 선택합니다.
4. 삭제할 사용자 지정 품목을 선택합니다.
5. 삭제를 선택합니다.
6. 사용자 지정 품목 삭제가 미치는 영향을 읽은 다음 사용자 지정 품목 삭제를 선택합니다.

AWS 빌링 컨덕터 모범 사례

이 섹션에서는 AWS 빌링 컨덕터와 협력할 때 사용할 수 있는 몇 가지 모범 사례를 중점적으로 설명합니다.

주제

기본 계정 가입일의 중요성 이해

기본 계정이 조직에 가입한 날짜에 따라 해당 청구 그룹의 견적 비용의 역사적 기준이 정해집니다. 월 중에 생성되거나 관리 계정에 연결된 기본 계정을 선택하는 경우 기본 계정이 가입되기 전에 조직에 속했던 계정을 포함하여 청구 그룹의 다른 계정에서 발생한 비용은 견적 비용에 포함되지 않습니다.

예를 들어, 기본 계정이 10월 15일에 조직에 가입했다고 가정해 보겠습니다. 결제 그룹의 모든 계정에 대한 견적 청구서에는 해당 날짜부터 시작되는 비용 및 사용량만 포함됩니다. 견적 청구서는 10월 15일에 시작됩니다. 청구 그룹의 다른 계정이 이번 달 이전에 조직의 구성원이었더라도 마찬가지입니다.

청구 그룹의 첫 달에는 청구 가능 도메인과 견적 청구 도메인 간에 차이가 있을 수 있습니다. 프로포마 도메인에는 10월 15일 이전에 누적된 사용량이 포함되지 않습니다. 첫 달 이후에는 모든 사용량이 견적 비용에 포함됩니다.

결제 그룹의 첫 번째 청구서에서 청구 가능 데이터와 견적 데이터 간의 초기 불일치를 방지하려면 한 달 전체 또는 그 이전에 관리 계정에 연결된 기본 계정을 선택하세요.

빌링 컨덕터에 대한 액세스 제어 AWS

과금 정보 및 비용 관리는 지급인 또는 관리 계정에 액세스할 수 있는 사용자만 액세스할 수 있습니다. IAM 사용자에게 결제 그룹을 생성하고 Billing and Cost Management 콘솔에서 AWS 결제 담당자 주요 성과 지표 (KPI) 를 볼 수 있는 권한을 부여하려면 IAM 사용자에게 다음 권한도 부여해야 합니다.

- Organizations 내 계정 목록

Billing Conductor 콘솔에서 사용자에게 결제 그룹 및 가격 책정 계획을 생성할 수 있는 권한을 부여하는 방법에 대한 자세한 내용은 을 AWS 참조하십시오. ID 및 액세스 관리 대상: AWS Billing Conductor

청구 담당자 API를 사용하여 AWS 청구 담당자 리소스를 프로그래밍 방식으로 만들 수도 있습니다 AWS . AWS 청구서 API에 대한 액세스를 구성할 때는 프로그래밍 방식의 액세스를 허용하는 고유한 IAM 사용자를 생성하는 것이 좋습니다. 이렇게 하면 조직 내에서 AWS 청구 지휘자 콘솔과 API에 액세스할 수 있는 사용자 간에 보다 정확한 액세스 제어를 정의할 수 있습니다. 여러 IAM 사용자에게 AWS 요금 청구 안내자 API에 대한 쿼리 액세스 권한을 부여하려면 각 사용자에게 프로그래밍 방식 액세스 IAM 역할을 생성하는 것이 좋습니다.

빌링 컨덕터 데이터 세트에 AWS 대한 이해

AWS 청구 담당자 데이터 모델은 표준 AWS 청구 데이터 모델과 많은 유사점을 공유하지만 몇 가지 차이점이 있습니다.

AWS 청구 대리인에는 다음이 포함되지 않습니다.

- 크레딧 (지급인 또는 연결 계정 수준에서 사용)
- 세금
- AWS Support 요금

또한 AWS Billing Conductor는 표준 결제 도메인의 공유 기본 설정에 관계없이 예약 인스턴스 및 Savings Plans를 동일한 결제 그룹에 속한 계정과 공유합니다.

AWS 빌링 컨덕터 계산 논리에 대한 이해

AWS 청구 담당자 계산은 이전 기간의 청구 데이터의 과거 무결성을 유지하면서 해당 월의 변경 사항에 맞게 유연하게 조정할 수 있습니다. 이는 예를 들어 설명하는 것이 가장 좋습니다.

이 예제에는 두 개의 결제 그룹 A 및 B(이)가 이습니다. 결제 그룹 A은(는) 그룹의 계정 1~3으로 청구 기간을 시작합니다. 월 중순이 되면 지급인 계정이 Account 3에서 Billing Group B(으)로 이동합니다. 이때 최신 변경 사항을 정확하게 모델링하려면 결제 그룹 A 및 B은(는) 비용을 다시 계산해야 합니다. Account 3 이동 시 현재 청구 기간 동안 Account 3이(가) 결제 그룹에 속하지 않은 것처럼 Billing Group A의 사용량이 모델링됩니다. 또한 Billing Group B의 사용량은 Account 3이

(가) 청구 기간이 시작된 이후부터 Billing Group B의 일부인 것처럼 모델링됩니다. 이 접근 방식을 사용하면 청구 기간 내에 여러 그룹으로 계정을 이동할 때 복잡한 요금 및 차지백 모델을 계산할 필요가 없습니다.

결제 그룹 A	소요일: 1~15일	소요일: 16~30일	월말
계정 1	100달러	100달러	200달러
계정 2	100달러	100달러	200달러
계정 3	100달러	N/A	N/A
합계	300달러	200달러	400달러

결제 그룹 B	소요일: 1~15일	소요일: 16~30일	월말
계정 4	100달러	100달러	200달러
계정 5	100달러	100달러	200달러
계정 6	100달러	100달러	200달러
계정 3	100달러	100달러	200달러
합계	400달러	400달러	800달러

AWS 빌링 컨덕터 업데이트 빈도 이해

AWS 청구 데이터는 하루에 한 번 이상 업데이트됩니다. AWS 청구 담당자는 이 데이터를 사용하여 견적 청구 데이터를 계산합니다. 이번 달에 적용하기 위해 생성된 사용자 지정 품목은 24시간 이내에 반영됩니다. 이전 청구 기간에 적용하기 위해 생성된 사용자 지정 항목이 청구 그룹 AWS 비용 및 사용 보고서 또는 특정 청구 그룹의 청구서 페이지에 반영되는 데 최대 48시간이 걸릴 수 있습니다.

AWS 청구 담당자 AWS CUR과 표준 CUR의 차이점 이해 AWS

표준 비용 및 사용 보고서와 청구 담당자 구성을 사용하여 만든 견적 AWS CUR 간에는 몇 가지 차이점이 있습니다. AWS

- 표준 AWS CUR은 통합 결제 패밀리의 각 계정에 대한 비용 및 사용량을 계산합니다. 청구 그룹별 견적 AWS CUR에는 계산 당시 결제 그룹에 속한 계정만 포함됩니다.
- 표준 AWS CUR은 인보이스 열을 한 번 채우고 인보이스는 에서 생성합니다. AWS견적 AWS CUR은 청구서 열을 채우지 않습니다. 현재는 견적 청구 데이터를 AWS 기반으로 생성되거나 발행된 청구서가 없습니다.

결제 그룹별 마진 분석

Billing Conductor의 마진 요약 및 마진 세부 정보를 사용하여 집계 및 특정 AWS 청구 그룹 모두에서 마진을 분석할 수 있습니다.

다음 단계를 사용하여 개별 결제 그룹 또는 결제 그룹 집합의 마진을 확인하십시오.

주제

마진 요약을 사용하여 마진을 집계하여 볼 수 있습니다.

청구 그룹 마진 요약을 보려면

1. https://console.aws.amazon.com/billingconductor/ 에서 AWS 빌링 컨덕터를 엽니다.
2. 탐색 창의 애널리틱스에서 마진 요약을 선택합니다.
3. 보고서 유형에서 모든 결제 그룹 또는 결제 그룹 선택을 선택합니다.
4. 청구 그룹 선택을 선택한 경우 청구 기간과 하나 이상의 청구 그룹을 선택합니다.
5. M onth-to-date 개요 섹션에서 청구 금액, AWS 비용, 마진을 확인할 수 있습니다.
6. 다음 두 가지 방법으로 마진 분석을 볼 수 있습니다.
   - 퍼포먼스 (최근 13개월까지) 섹션의 막대형 차트로 표시합니다.
   - 마진 분석 표의 표 참조

   그래프에서 마이너스 마진은 빨간색으로 표시되며, 금액은 마이너스이고 백분율은 마이너스입니다.

마진 분석 표의 이해

빌링 그룹 마진 분석표는 기본적으로 시간 역순으로 정렬됩니다. 다음을 포함한 모든 열을 기준으로 테이블을 정렬할 수 있습니다.

- 월
- 청구 금액
- AWS 비용

- 마진 금액
- 마진 백분율

그래프와 표는 선택한 결제 그룹의 지난 13개월 동안의 값을 반환합니다. 결제 그룹이 서로 다른 시간에 생성된 경우 선택한 가장 오래된 결제 그룹의 시간 범위를 가정합니다.

마진 분석표를 다운로드 가능한 CSV 파일로 내보낼 수 있습니다. 마진 분석표 옆의 CSV 다운로드를 선택합니다. 다운로드가 자동으로 시작됩니다.

> **Note**
>
> 결제 그룹 마진 분석이 포함된 CSV 파일을 다운로드하려면 IAM 정책에 `billingconductor:ListBillingGroupCostReport` 권한이 추가되어야 합니다.

마진 세부 정보를 사용하여 AWS 서비스 마진별 보기

서비스별 청구 그룹 마진을 보려면

1. https://console.aws.amazon.com/billingconductor/ 에서 AWS 빌링 컨덕터를 엽니다.
2. 탐색 창의 애널리틱스에서 마진 세부 정보를 선택합니다.
3. 보고서 매개변수에서 청구 기간 및 청구 그룹을 선택합니다.
4. 다음 두 가지 방법으로 마진 분석을 볼 수 있습니다.
    - 상위 5개 서비스별 마진 추이 섹션의 선형 차트로
    - 마진 분석 표의 표 참조.

마진 트렌드 차트 이해하기

마진 세부 정보에는 선택한 청구 기간 동안 마진별로 상위 5개 서비스를 마진별로 표시하는 선형 차트가 표시됩니다. 라인 차트에는 비교를 위해 지난 3개월 동안의 각 서비스의 마진이 표시됩니다.

또한 차트에는 선택한 청구 기간 동안 각 서비스의 마진을 보여 주는 표도 포함됩니다. 이 표에는 지난 3개월 동안 계산된 평균 마진이 표시되며, 여기에는 다음 열이 포함됩니다.

- 서비스 이름
- 평균

- 마진

지난 3개월 동안 결제 그룹이 활성화되지 않은 경우 차트에는 사용 가능한 비용 보고서 데이터만 표시됩니다.

마진 분석표 이해하기

빌링 그룹 마진 분석 표에는 다음 열이 포함됩니다.

- 서비스 이름
- 청구 금액
- AWS 비용
- 마진 금액
- 마진 백분율

마진 분석표를 다운로드 가능한 CSV 파일로 내보낼 수 있습니다. 마진 분석표 옆의 CSV 다운로드를 선택합니다. 다운로드가 자동으로 시작됩니다.

> **Note**
>
> 결제 그룹 마진 분석이 포함된 CSV 파일을 다운로드하려면 IAM 정책에 `billingconductor:GetBillingGroupCostReport` 권한이 추가되어야 합니다.

결제 그룹 세부 정보 보기

결제 그룹 세부 정보를 사용하여 AWS Billing Conductor에서 결제 그룹을 모니터링, 분석 및 편집할 수 있습니다. 결제 그룹 세부 정보는 월별 마진 분석, 적용된 사용자 지정 품목 내역, 필요에 따라 결제 그룹을 편집 및 삭제할 수 있는 기능을 제공합니다.

사용자 지정 요금 기준별 청구서 세부 정보 보기

결제 그룹과 요금제를 생성하고 할당한 후에는 관리 중인 각 결제 그룹에 대한 사용 유형 세분화를 통해 사용자 지정 결제 규모를 확인할 수 있습니다.

다음 단계에 따라 견적 도메인에서 청구서 세부 정보를 확인합니다.

견적 청구서 세부 정보를 보려면

1. https://console.aws.amazon.com/billing/에서 AWS Billing 콘솔을 엽니다.
2. 탐색 창에서 청구서(Bills)를 선택합니다.
3. 청구서 세부 정보의 오른쪽 상단에서 설정을 선택합니다.
4. 견적 데이터 보기를 활성화합니다.
5. 결제 그룹에서 분석할 결제를 선택합니다.

서비스 및 AWS 리전 결제 그룹 사용량을 분석하여 AWS Billing Conductor에 정의된 요금과 일치하는 해당 사용 비용을 확인할 수 있습니다.

청구서 세부 정보 페이지의 서비스 AWS Billing Conductor에서 사용자 지정 품목을 찾을 수 있습니다.

결제 그룹별 Cost and Usage Reports 구성

생성한 각 결제 그룹에 대해 견적 AWS Cost and Usage Reports (AWS CUR) 를 생성할 수 있습니다. 견적 AWS CUR은 표준 AWS CUR과 동일한 파일 형식, 세분성 및 열을 가지며 지정된 기간 동안 사용할 수 있는 가장 포괄적인 비용 및 사용 데이터 세트를 포함합니다.

본인 소유의 Amazon Simple Storage Service (S3) 버킷에 견적 AWS CUR을 게시할 수 있습니다.

AWS은(는) 하루에 한 번 CSV (쉼표로 구분된 값) 또는 Apache Parquet 형식으로 버킷의 보고서를 업데이트합니다. Microsoft Excel 및 Apache OpenOffice Calc와 같은 스프레드시트 소프트웨어를 사용하여 보고서를 볼 수 있습니다. Amazon S3 또는 Amazon Athena API를 사용하여 애플리케이션에서 액세스할 수도 있습니다. 표준 AWS CUR에 대한 자세한 내용은 AWS Cost and Usage Reports 사용 설명서를 참조하세요.

다음 단계를 사용하여 결제 그룹에 대한 견적 AWS CUR을 생성하세요.

결제 그룹을 위한 견적 Cost and Usage Reports 생성

1. https://console.aws.amazon.com/billing/에서 AWS Billing 콘솔을 엽니다.
2. 탐색 창에서 Cost & usage reports를 선택합니다.
3. 보고서 테이블 오른쪽 상단에서 설정을 선택합니다.
4. 견적 데이터 보기를 활성화합니다.
5. 활성화를 선택합니다.
6. 보고서 생성(Create report)을 선택합니다.
7. 보고서 이름에 보고서 이름을 입력합니다.
8. 데이터 보기의 경우 견적을 선택합니다.
9. 결제 그룹의 경우 결제 그룹을 선택합니다.
10. 추가 보고서 세부 정보에서 각 개별 리소스의 ID를 보고서에 포함하려면 리소스 ID 포함을 선택합니다.
11. 데이터 새로고침 설정의 경우 청구서를 확정한 후 AWS 비용 및 사용량 데이터에 대한 새로운 변경 내용을 적용하여 Cost and Usage Reports를 새로 고칠지 여부를 선택합니다. 보고서가 새로 고침 되면 새 보고서가 Amazon S3에 업로드됩니다.

> **Note**
>
> 결제 그룹 Cost and Usage Reports에는 크레딧, 세금 또는 지원 요금이 포함되지 않습니다.

12. 다음(Next)을 선택합니다.
13. S3 버킷에서 구성을 선택합니다.
14. S3 버킷 구성 대화 상자에서 다음 중 하나를 수행합니다.
    - 드롭다운 목록에서 기존 버킷을 선택하고 다음을 선택합니다.
    - 버킷 이름과 새 버킷을 생성할 AWS 리전을 입력하고 다음을 선택합니다.
15. 이 정책이 정확함을 확인함를 선택하고 저장을 선택합니다.
16. 보고서 경로 접두사에 보고서 이름의 접두어가 되는 보고서 경로 접두사를 입력합니다.

    이 단계는 Amazon Redshift 또는 Amazon QuickSight에서는 선택 사항이지만 Amazon Athena에서는 필수입니다.

    접두사를 지정하지 않을 경우 기본 접두사는 4단계에서 보고서에 지정한 이름과 보고서 날짜 범위이고 형식은 다음과 같습니다.

    ```
    /report-name/date-range/
    ```
17. 시간 세부 수준에 대해 다음 중 하나를 선택합니다.
    - 시간별: 보고서의 행 항목을 시간별로 집계하려면 선택합니다.
    - 일별: 보고서의 행 항목을 일별로 집계하려면 선택합니다.
18. 보고서 버전 관리에서, 보고서의 각 버전을 이전 버전을 겹쳐쓸지 또는 이전 버전과 별도로 추가 제공할지를 선택합니다.
19. 보고서 데이터 통합 활성화에서 Cost and Usage Reports를 Amazon Athena, Amazon Redshift 또는 Amazon QuickSight에 업로드할지 여부를 선택합니다. 보고서는 다음 형식으로 압축됩니다.
    - Athena: 파케이 압축
    - Amazon Redshift 또는 Amazon QuickSight: .gz 압축
20. 다음(Next)을 선택합니다.
21. 보고서 설정 검토 후 Review and Complete를 선택합니다.

견적 비용에 대한 임시 분석 수행 AWS Cost Explorer

AWS 계정빌링 컨덕터에서 결제 그룹은 Cost Explorer에서 견적 비용을 분석, 예측 및 보고할 수 있습니다. 결제 그룹의 기본 계정은 그룹 내 모든 계정에 대해 이러한 활동을 수행할 수 있습니다. 를 사용하는 AWS Organizations 경우 관리 계정은 Cost Explorer에서 견적 비용을 분석, 예측 또는 보고할 수 없습니다.

결제 그룹 관리 계정 (결제 그룹 구성원) 은 자신이 청구 그룹에 속했던 청구 기간의 비용 및 사용량 데이터를 볼 수 있으며 견적 데이터도 사용할 수 있습니다. 청구 가능한 과거 비용 및 사용량 데이터는 볼 수 없습니다.

참고

- 빌링 컨덕터 관리 계정 (결제 그룹 구성원) 은 Cost Explorer에서 견적 비용을 볼 수 있습니다.
- Cost Explorer에서는 시간별 세부 수준 데이터가 비용 기준으로 지원되지 않습니다.
- Cost Explorer가 지원하는 핵심 워크플로에 대해 자세히 알아보려면 AWS Cost Management 사용 설명서의 Cost Explorer를 사용한 데이터 탐색을 참조하세요.

견적 비용을 AWS 서비스 지원하는 목록은 을 참조하십시오. AWS 서비스 견적 비용을 지원하는

AWS 서비스 견적 비용을 지원하는

다음 클라우드 재무 관리 서비스 및 해당 기능은 견적 비용을 지원합니다.

서비스 및 기능	AWS 계정 유형별 지원 수준		
	지급인 (관리 계정)	기본 계정	연결 (회원 계정)
AWS Cost and Usage Report	예	예	예
분할 비용 할당	아니요	아니요	아니요
AWS Billing	아니요	예	예
대시보드	아니요	예	예
청구서 세부 정보	예	예	예
CSV 다운로드	아니요	아니요	아니요
AWS Cost Explorer	아니요	예	예
예상	아니요	예	예
보고서 저장	아니요	예	예
규모 조정 권장 사항	아니요	아니요	아니요
비용 이상 모니터	아니요	아니요	아니요
절감형 플랜 권장 사항	아니요	아니요	아니요
절감형 플랜 이용 보고서	아니요	아니요	아니요
절감형 플랜 적용 범위 보고서	아니요	아니요	아니요
예약 권장 사항	아니요	아니요	아니요

서비스 및 기능	AWS 계정 유형별 지원 수준		
예약 이용 보고서	아니요	아니요	아니요
예약 적용 범위 보고서	아니요	아니요	아니요
AWS Budgets	아니요	아니요	아니요
예산 보고서	아니요	아니요	아니요

견적 비용을 지원하지 않는 서비스 및 기능의 경우 청구서와 일치하는 청구 가능 요율로 비용이 AWS 계정 표시됩니다. AWS

관련 정보

청구 가능한 환불, 크레딧 및 할인에 대한 연결 계정 액세스를 관리하려면 Cost Management Console의 기본 설정 페이지에 있는 AWS Cost Explorer 섹션을 참조하십시오.

IAM 엔터티에 이러한 서비스 및 기능에 대한 특정 청구 가능 요금이 표시되지 않도록 하려면 IAM 정책을 사용하여 액세스를 거부할 수 있습니다. IAM 정책 예제는 견적 비용을 지원하지 않는 서비스 및 기능에 대한 Billing 및 Cost Explorer 액세스 거부 섹션을 참조하세요.

특정 권한을 허용하거나 거부하도록 IAM 정책을 사용자 지정할 수도 있습니다. 과금 정보 및 비용 관리의 IAM 작업 세부 목록은 다음 주제를 참조하십시오.

- AWS Cost Management 사용 설명서의 AWS Cost Management에 대한 액세스 제어 마이그레이션
- AWS Billing 사용 설명서의 AWS Billing에 대한 액세스 제어 마이그레이션

AWS Billing Conductor API 사용

Billing Conductor API는 Java, Python, .NET 및 Go에서 사용할 수 있습니다. Billing Conductor에서 출시된 새로운 기능을 API로도 사용할 수 있습니다.

AWS Billing Conductor API에 대한 자세한 내용은 AWS Billing Conductor API 참조를 참조하세요.

AWS 빌링 컨덕터의 보안

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 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. AWS Billing Conductor에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 AWS 범위 내 서비스 규정 준수 프로그램이 참조하십시오.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS Billing Conductor를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 AWS Billing Conductor를 구성하는 방법을 보여줍니다. 또한 AWS Billing Conductor 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 배웁니다.

주제

- AWS 빌링 컨덕터의 데이터 보호
- ID 및 액세스 관리 대상: AWS Billing Conductor
- AWS 빌링 컨덕터의 로깅 및 모니터링
- AWS 청구 담당자에 대한 규정 준수 검증
- AWS 빌링 컨덕터의 탄력성
- AWS 빌링 컨덕터의 인프라 보안

AWS 빌링 컨덕터의 데이터 보호

AWS 공동 책임 모델 공동 책임 모델 이 모델에 설명된 대로 AWS 는 모든 것을 실행하는 글로벌 인프라를 보호할 책임이 있습니다. AWS 클라우드사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프

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

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

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-2를 참조하세요.

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

ID 및 액세스 관리 대상: AWS Billing Conductor

AWS Identity and Access Management (IAM) 은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM 관리자는 어떤 사용자가 Billing Conductor 리소스를 사용할 수 있는 인증 (로그인) 및 권한 (권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- 자격 증명을 통한 인증
- 정책을 사용한 액세스 관리

- IAM의 AWS Billing Conductor 작동 방식
- AWS Billing Conductor ID 기반 정책 예제
- AWS 빌링 컨덕터를 위한 AWS 관리형 정책
- AWS Billing Conductor 리소스 기반 정책 예제
- AWS Billing Conductor ID 및 액세스 문제 해결

고객

빌링 컨덕터에서 수행하는 작업에 따라 사용 방법 AWS Identity and Access Management (IAM) 이 다릅니다.

서비스 사용자 - Billing Conductor 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증과 권한을 관리자가 제공합니다. 더 많은 Billing Conductor 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Direct Connect의 기능에 액세스할 수 없는 경우 AWS Billing Conductor ID 및 액세스 문제 해결 섹션을 참조하십시오.

서비스 관리자 – Billing Conductor 리소스를 담당하는 경우 Billing Conductor에 대한 전체 액세스 권한이 있을 수 있습니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Billing Conductor 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해합니다. 회사가 Billing Conductor에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 IAM의 AWS Billing Conductor 작동 방식 섹션을 참조하십시오.

IAM 관리자 – IAM 관리자라면 Billing Conductor에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Billing Conductor 자격 증명 기반 정책 예제를 보려면 AWS Billing Conductor ID 기반 정책 예제 섹션을 참조하십시오.

자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

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

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

계정을 만들 때는 먼저 AWS 계정계정의 모든 AWS 서비스 리소스와 모든 리소스에 완전히 액세스할 수 있는 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

IAM 사용자 및 그룹

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

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

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증 정보만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자(역할을 대신하여)를 만들어야 하는 경우를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용자 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 연동 사용자 액세스 - 연동 자격 증명에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기 부분을 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한: IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스: IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예컨대, 어떤 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 EC2에서 애플리케이션을 실행하거나 S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
- 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

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

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용자 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용자 설명서의 JSON 정책 개요를 참조하세요.

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

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

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

ID 기반 정책

ID 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 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성 단원을 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용자 설명서의 관리형 정책과 인라인 정책 사이의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

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

액세스 제어 목록(ACLs)

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

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Simple Storage Service 개발자 안내서의 ACL(액세스 제어 목록) 개요를 참조하세요.

기타 정책 타입

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

- 권한 경계: 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는

권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용자 설명서의 IAM 엔터티에 대한 권한 경계를 참조하세요.

- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 특성을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책: 세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용자 설명서의 세션 정책을 참조하세요.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

IAM의 AWS Billing Conductor 작동 방식

IAM을 사용하여 Billing Conductor에 대한 액세스를 관리하려면 먼저 어떤 IAM 기능을 Billing Conductor에 사용할 수 있는지를 이해해야 합니다. Billing Conductor 및 기타 AWS 서비스가 IAM과 어떻게 연동되는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 연동되는AWS 서비스를 참조하십시오.

주제

- Billing Conductor 자격 증명 기반 정책
- 결제 담당자 리소스 기반 정책
- 액세스 제어 목록(ACLs)
- Billing Conductor 태그 기반 권한 부여
- Billing Conductor IAM 역할

Billing Conductor 자격 증명 기반 정책

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. Billing Conductor는 특정 작업, 리소스 및 조건 키를 지원합니다. JSON 정책에서 사용하는 모든 요소에 대해 알고 싶다면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

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 있는 지를 지정할 수 있습니다.

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

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

Billing Conductor의 정책 작업은 작업 앞에 다음 접두사 `Billing Conductor:`을(를) 사용합니다. 예를 들어 누군가에게 Amazon EC2 `RunInstances` API 작업을 통해 Amazon EC2 인스턴스를 실행할 권한을 부여하려면 해당 정책에 `ec2:RunInstances` 작업을 포함하세요. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Billing Conductor는 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 정의합니다.

명령문 하나에 여러 태스크를 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

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

```
"Action": "ec2:Describe*"
```

청구 담당자 작업 목록을 보려면 IAM 사용 AWS 설명서의 청구 담당자가 정의한 작업을 참조하십시오.

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

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

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

Amazon EC2 인스턴스 리소스에는 다음 ARN이 있습니다.

```
arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}
```

ARN 형식에 대한 자세한 내용은 Amazon 리소스 이름 (ARN) 및 AWS 서비스 네임스페이스를 참조하십시오.

예를 들어 문에서 `i-1234567890abcdef0` 인스턴스를 지정하려면 다음 ARN을 사용합니다.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

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

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

리소스를 생성하기 위한 작업과 같은 일부 Billing Conductor 작업은 특정 리소스에서 수행할 수 없습니다. 이러한 경우, 와일드카드(*)를 사용해야 합니다.

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

다양한 Amazon EC2 API 작업에는 여러 리소스가 관여합니다. 예를 들어 `AttachVolume`은 Amazon EBS 볼륨을 인스턴스에 연결하므로 IAM 사용자에게 볼륨 사용 권한과 인스턴스 사용 권한이 있어야 합니다. 단일 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
      "resource1",
      "resource2"
```

청구 담당자 리소스 유형 및 해당 ARN 목록을 보려면 IAM 사용 AWS 설명서의 청구 담당자가 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 AWS 청구 담당자가 정의한 조치를 참조하십시오.

조건 키

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, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

Billing Conductor는 자체 조건 키 집합을 정의하고 일부 전역 조건 키 사용도 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 설명서의AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

모든 Amazon EC2 작업은 `aws:RequestedRegion` 및 `ec2:Region` 조건 키를 지원합니다. 자세한 내용은 예제: 특정 리전으로 액세스 제한을 참조하세요.

결제 담당자 조건 키 목록을 보려면 IAM 사용 AWS 설명서의 청구 컨덕터 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 청구 담당자가 AWS 정의한 작업을 참조하십시오.

예제

Billing Conductor 자격 증명 기반 정책 예제를 보려면 AWS Billing Conductor ID 기반 정책 예제 섹션을 참조하십시오.

결제 담당자 리소스 기반 정책

리소스 기반 정책은 지정된 보안 주체가 Billing Conductor 리소스에 대해 수행할 수 있는 작업 및 관련 조건을 제어하는 JSON 정책 문서입니다. Amazon S3은 Amazon S3 ##에 대한 리소스 기반 권한 정책을 지원합니다. 리소스 기반 정책을 사용하여 리소스별로 다른 계정에 사용 권한을 부여할 수 있습니다. *## ### ## ### #### AWS #### Amazon S3 ### ###### ### # ####.*

크로스 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 신뢰 관계 설정의 절반밖에 되지 않습니다. 보안 주체와 리소스가 서로 다른 AWS 계정에 있는 경우 보안 주체에 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 보안 인증 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 IAM 사용자 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조합니다.

Amazon S3 서비스는 리소스 기반 정책 중 한 가지 유형만 지원하는데, 이 정책 유형은 *##* 정책이라고 하며 *##*에 연결되어 있습니다. 이 정책은 *Billing Conductor*에서 작업을 수행할 수 있는 보안 주체 엔터티(계정, 사용자, 역할 및 연동 사용자)를 정의합니다.

예제

Billing Conductor 리소스 기반 정책의 예는 AWS Billing Conductor 리소스 기반 정책 예제 섹션을 참조하십시오.

액세스 제어 목록(ACLs)

ACL(액세스 제어 목록)은 리소스에 연결할 수 있는 피부여자 목록입니다. 이 목록은 연결된 리소스에 액세스할 수 있는 권한을 계정에 부여합니다. Amazon S3 *##* 리소스에 ACL을 연결할 수 있습니다.

Amazon S3 액세스 제어 목록(ACL)을 사용하여 *##* 리소스에 대한 액세스를 관리할 수 있습니다. 각 *##*마다 하위 리소스로서 연결되어 있는 ACL이 있습니다. 액세스 권한이 부여되는 AWS 계정, IAM 사용자 또는 사용자 그룹 또는 IAM 역할과 액세스 유형을 정의합니다. 리소스에 대한 요청을 받으면 해당 ACL을 AWS 검사하여 요청자에게 필요한 액세스 권한이 있는지 확인합니다.

리소스를 생성하면 Amazon S3는 리소스에 대한 모든 권한을 리소스 소유자에게 부여하는 기본 ACL을 생성합니다. 다음 예제 ## ACL에서 John Doe는 ##의 소유자로 나열되며 해당 ##에 대한 모든 제어 권한이 부여되어 있습니다. ACL은 최대 100개의 권한을 부여할 수 있습니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://Billing Conductor.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6</ID>
    <DisplayName>john-doe</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6</ID>
        <DisplayName>john-doe</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

ACL의 ID 필드는 AWS 계정 표준 사용자 ID입니다. 소유한 계정에서 이 ID를 보는 방법을 알아보려면 계정 정식 사용자 ID 찾기를 AWS 참조하십시오.

Billing Conductor 태그 기반 권한 부여

태그를 Billing Conductor 리소스에 연결하거나 Billing Conductor에 요청을 통해 태그를 에 전달할 수 있습니다. 태그를 기반으로 액세스를 제어하려면 `Billing Conductor:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

Billing Conductor IAM 역할

IAM 역할은 AWS 계정 내에서 특정 권한을 가진 엔티티입니다.

Billing Conductor 임시 보안 인증 정보 사용

임시 보안 인증을 사용하여 연동을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole또는 GetFederationToken같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻습니다.

Billing Conductor는 임시 자격 증명 사용을 지원합니다.

서비스 연결 역할

서비스 연결 역할을 사용하면 AWS 서비스가 다른 서비스의 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 나타나고 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수 없습니다.

서비스 역할

이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 수임할 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 역할은 IAM 계정에 나타나고, 해당 계정이 소유합니다. 즉, IAM 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

Billing Conductor는 서비스 역할을 지원합니다.

Billing Conductor의 IAM 역할 선택

Billing Conductor에서 리소스를 생성할 경우, Billing Conductor가 사용자 대신해 Amazon EC2에 액세스할 수 있도록 하는 역할을 선택해야 합니다. 이전에 서비스 역할 또는 서비스 연결 역할을 생성한 경우 Billing Conductor가 선택할 수 있는 역할 목록을 제공합니다. Amazon EC2 인스턴스 시작 및 중지에 대한 액세스를 허용하는 역할을 선택하는 것이 중요합니다.

AWS Billing Conductor ID 기반 정책 예제

기본적으로 IAM 사용자 및 역할은 Billing Conductor 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI, 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. IAM 관리자는 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

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

주제

- 정책 모범 사례
- Billing Conductor 자격 증명 기반 정책 예제

정책 모범 사례

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

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용: IAM 정책을 사용하여 권한을 설정하는 경우 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 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한: 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용자 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 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

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

Billing Conductor 자격 증명 기반 정책 예제

이 항목에서는 계정의 정보와 도구에 대한 액세스를 제어하기 위해 IAM 사용자 또는 그룹에 연결할 수 있는 정책의 예를 보여 줍니다.

주제

- Billing Conductor 콘솔에 대한 전체 액세스 권한 부여
- Billing Conductor API에 대한 전체 액세스 권한 부여
- Billing Conductor 콘솔에 대한 읽기 전용 액세스 권한 부여
- Billing 콘솔을 통해 Billing Conductor에게 액세스 권한 부여
- 비용 및 사용 보고서를 통해 청구 담당자에게 액세스 권한 부여 AWS
- Billing Conductor에 조직 단위 가져오기 기능에 대한 액세스 권한 부여
- 견적 비용을 지원하지 않는 서비스 및 기능에 대한 Billing 및 Cost Explorer 액세스 거부

Billing Conductor 콘솔에 대한 전체 액세스 권한 부여

Billing Conductor 콘솔에 액세스하려면 최소한의 권한 집합이 있어야 합니다. 이러한 권한은 AWS 계정에서 Billing Conductor 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 보안 인증 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(IAM 사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

해당 엔티티가 Billing Conductor 콘솔을 계속 사용할 수 있도록 하려면 다음 AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

`billingconductor:*` 권한 외에도 `pricing:DescribeServices`은(는) 요금 규칙 생성에 필요하며 `organizations:ListAccounts`은(는) 지급인 계정에 연결된 연결 계정을 나열해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "billingconductor:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "pricing:DescribeServices",
            "Resource": "*"
        }
    ]
}
```

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

Billing Conductor API에 대한 전체 액세스 권한 부여

이 예시에서는 IAM 엔터티에 Billing Conductor API에 대한 전체 액세스 권한을 부여합니다.

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

Billing Conductor 콘솔에 대한 읽기 전용 액세스 권한 부여

이 예시에서는 IAM 엔터티에 Billing Conductor 콘솔에 대한 읽기 전용 액세스 권한을 부여합니다.

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

```
            "Effect": "Allow",
            "Action": "organizations:ListAccounts",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "pricing:DescribeServices",
            "Resource": "*"
        }
    ]
}
```

Billing 콘솔을 통해 Billing Conductor에게 액세스 권한 부여

이 예제에서 IAM 엔티티는 Billing Console의 Bills 페이지를 통해 견적 결제 데이터를 전환하고 확인할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "billing:ListBillingViews",
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        }
    ]
}
```

비용 및 사용 보고서를 통해 청구 담당자에게 액세스 권한 부여 AWS

이 예제에서 IAM 개체는 결제 콘솔의 비용 및 사용 보고서 페이지를 통해 견적 청구 데이터를 전환하고 볼 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "billing:ListBillingViews",
```

```
                "aws-portal:ViewBilling",
                "cur:DescribeReportDefinitions"
            ],
            "Resource": "*"
        }
    ]
}
```

Billing Conductor에 조직 단위 가져오기 기능에 대한 액세스 권한 부여

이 예제에서 IAM 엔티티는 결제 그룹을 생성할 때 OU (조직 구성 단위) 계정을 가져오는 데 필요한 특정 AWS Organizations API 작업에 대한 읽기 전용 액세스 권한을 가집니다. OU 가져오기 기능은 AWS 빌링 컨덕터 콘솔에 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        }
    ]
}
```

견적 비용을 지원하지 않는 서비스 및 기능에 대한 Billing 및 Cost Explorer 액세스 거부

이 예시에서는 견적 비용을 지원하지 않는 서비스 및 기능에 대한 IAM 엔티티의 액세스가 거부됩니다. 이 정책에는 관리 계정 및 개별 멤버 계정 내에서 가능한 작업 목록이 포함되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "aws-portal:ModifyAccount",
            "aws-portal:ModifyBilling",
            "aws-portal:ModifyPaymentMethods",
            "aws-portal:ViewPaymentMethods",
```

```
            "aws-portal:ViewAccount",
            "cur:GetClassic*",
            "cur:Validate*",
            "tax:List*",
            "tax:Get*",
            "tax:Put*",
            "tax:ListTaxRegistrations",
            "tax:BatchPut*",
            "tax:UpdateExemptions",
            "freetier:Get*",
            "payments:Get*",
            "payments:List*",
            "payments:Update*",
            "payments:GetPaymentInstrument",
            "payments:GetPaymentStatus",
            "purchase-orders:ListPurchaseOrders",
            "purchase-orders:ListPurchaseOrderInvoices",
            "consolidatedbilling:GetAccountBillingRole",
            "consolidatedbilling:Get*",
            "consolidatedbilling:List*",
            "invoicing:List*",
            "invoicing:Get*",
            "account:Get*",
            "account:List*",
            "account:CloseAccount",
            "account:DisableRegion",
            "account:EnableRegion",
            "account:GetContactInformation",
            "account:GetAccountInformation",
            "account:PutContactInformation",
            "billing:GetBillingPreferences",
            "billing:GetContractInformation",
            "billing:GetCredits",
            "billing:RedeemCredits",
            "billing:Update*",
            "ce:GetPreferences",
            "ce:UpdatePreferences",
            "ce:GetReservationCoverage",
            "ce:GetReservationPurchaseRecommendation",
            "ce:GetReservationUtilization",
            "ce:GetSavingsPlansCoverage",
            "ce:GetSavingsPlansPurchaseRecommendation",
            "ce:GetSavingsPlansUtilization",
            "ce:GetSavingsPlansUtilizationDetails",
```

```
            "ce:ListSavingsPlansPurchaseRecommendationGeneration",
            "ce:StartSavingsPlansPurchaseRecommendationGeneration",
            "ce:UpdateNotificationSubscription"
        ],
        "Resource": "*"
    }]
}
```

자세한 정보는 AWS 서비스 견적 비용을 지원하는을 참조하세요.

AWS 빌링 컨덕터를 위한 AWS 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 정책을 직접 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의AWS 관리형 정책을 참조하십시오.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 타입의 업데이트는 정책이 연결된 모든 보안 인증(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 새 작업 및 리소스에 대한 읽기 전용 권한이 AWS 추가됩니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSBillingConductorFullAccess

AWSBillingConductorFullAccess 관리형 정책은 AWS 빌링 컨덕터 콘솔 및 API에 대한 전체 액세스 권한을 부여합니다. 사용자는 AWS 빌링 컨덕터 리소스를 나열, 생성 및 삭제할 수 있습니다.

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

```
        {
            "Effect": "Allow",
            "Action": [
               "billingconductor:*",
               "organizations:ListAccounts",
               "pricing:DescribeServices",
             ]
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSBillingConductorReadOnlyAccess

AWSBillingConductorReadOnlyAccess 관리형 정책은 AWS 빌링 컨덕터 콘솔 및 API에 대한 읽기 전용 액세스 권한을 부여합니다. 사용자는 모든 AWS 빌링 컨덕터 리소스를 보고 나열할 수 있습니다. 사용자는 리소스를 생성하거나 삭제할 수 없습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BillingConductorReadOnly",
            "Effect": "Allow",
            "Action": [
                "billingconductor:List*",
                "organizations:ListAccounts",
                "pricing:DescribeServices",
                "billingconductor:GetBillingGroupCostReport"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책에 대한 빌링 컨덕터 업데이트 AWS

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 AWS Billing Conductor의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하세요. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS 청구 담당자 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AWSBillingConductorReadOnlyAccess	정책에 `GetBillingGroupCostReport` 추가되었습니다. `AWSBillingConductorReadOnlyAccess`	2024년 2월 8일
AWSBillingConductorFullAccess	정책 생성	2022년 3월 29일
AWSBillingConductorReadOnlyAccess	정책 생성	2022년 3월 29일
AWS 청구 담당자 변경 로그 공개	AWS 빌링 컨덕터는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2022년 3월 29일

AWS Billing Conductor 리소스 기반 정책 예제

주제

- 특정 IP 주소에 대한 Amazon S3 버킷 액세스 제한

특정 IP 주소에 대한 Amazon S3 버킷 액세스 제한

다음 예제는 모든 사용자에게 권한을 부여하여 지정된 버킷에서 객체에 대해 모든 Amazon S3 작업을 수행할 수 있도록 합니다. 하지만 조건에 지정된 IP 주소 범위에서만 요청을 허용해야 합니다.

이 문의 조건은 허용되는 IPv4(인터넷 프로토콜 버전 4) IP 주소의 54.240.143.* 범위를 식별하며 단, 한 가지 예외는 54.240.143.188입니다.

`Condition`블록은 `IpAddress` 및 `NotIpAddress` 조건과 AWS 와이드 `aws:SourceIp` 조건 키인 조건 키를 사용합니다. 이러한 조건 키에 대한 자세한 내용은 정책의 조건 지정을 참조합니다. `aws:sourceIp` IPv4 값은 표준 CIDR 표기법을 사용합니다. 자세한 내용은 IAM 사용자 설명서의 IP 주소 조건 연산자를 참조합니다.

```
{
```

```
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
         "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
         "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
      }
    }
  ]
}
```

AWS Billing Conductor ID 및 액세스 문제 해결

다음 정보를 사용하여 Billing Conductor 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Billing Conductor에서 작업을 수행할 권한이 없음
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 내 AWS 계정 외부의 사용자가 내 청구 담당자 리소스에 액세스할 수 있도록 허용하고 싶습니다.

Billing Conductor에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 *`Billing Conductor`*에 대한 세부 정보를 보려고 하지만 `Billing Conductor:`*`GetWidget`* 권한이 없는 경우에 발생합니다.

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

이 경우 Mateo는 *my-example-Billing Conductor* 작업을 사용하여 Billing Conductor:*GetWidget* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Billing Conductor에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

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

다음 예시 오류는 marymajor인 IAM 사용자가 콘솔을 사용하여 Billing Conductor에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우 Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사용자가 내 청구 담당자 리소스에 액세스할 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 참조하세요.

- Billing Conductor가 이러한 기능을 지원하는지 여부를 알아보려면 IAM의 AWS Billing Conductor 작동 방식 섹션을 참조하십시오.
- 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.

- 보안 인증 연동을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

AWS 빌링 컨덕터의 로깅 및 모니터링

모니터링은 AWS 계정의 안정성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS 빌링 컨덕터 사용량을 모니터링하는 데 사용할 수 있는 몇 가지 도구가 있습니다.

AWS 비용 및 사용 보고서

AWS 비용 및 사용 보고서는 AWS 사용량을 추적하고 계정과 관련된 예상 요금을 제공합니다. 각 보고서에는 AWS 계정에서 사용하는 AWS 제품, 사용 유형 및 운영의 고유한 조합에 대한 항목이 포함되어 있습니다. AWS 비용 및 사용 보고서를 사용자 지정하여 시간별 또는 일별로 정보를 집계할 수 있습니다.

AWS 비용 및 사용 보고서에 대한 자세한 내용은 비용 및 사용 보고서 가이드를 참조하십시오.

를 사용하여 AWS Billing Conductor API 호출을 로깅합니다. AWS CloudTrail

AWS Billing Conductor AWS Billing Conductor에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합되었습니다. CloudTrail AWS 빌링 컨덕터에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 청구 담당자 콘솔의 통화 및 AWS 청구 수행자 API 작업에 대한 코드 호출이 AWS 포함됩니다. 트레일을 생성하면 AWS Billing Conductor에 대한 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 Billing Conductor에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기, 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

AWS Billing Conductor CloudTrail 이벤트

이 섹션에는 Billing and Cost Management와 관련된 전체 CloudTrail 이벤트 목록이 표시됩니다.

이벤트 이름	정의
AssociateAccounts	계정과 결제 그룹의 연결을 기록합니다.
AssociatePricingRules	가격 책정 규칙과 가격 책정 계획의 연결을 기록합니다.
AutoAssociateAccount	계정과 결제 그룹의 자동 연결을 기록합니다.
AutoDisassociateAccount	다음 청구 기간에 결제 그룹과 계정의 자동 연결 해제를 기록합니다.
BatchAssociateResourcesToCustomLineItem	백분율 사용자 지정 라인 항목에 대한 리소스의 일괄 연결을 기록합니다.
BatchDisassociateResourcesFromCustomLineItem	백분율 사용자 지정 라인 항목에서 리소스의 일괄 연결 해제를 기록합니다.
CreateBillingGroup	결제 그룹 생성을 기록합니다.
CreateCustomLineItem	사용자 지정 품목의 생성을 기록합니다.
CreatePricingPlan	요금제 생성을 기록합니다.
CreatePricingRule	가격 책정 규칙 생성을 기록합니다.
DeleteBillingGroup	결제 그룹 삭제를 기록합니다.
DeleteCustomLineItem	사용자 지정 품목의 삭제를 기록합니다.

이벤트 이름	정의
DeletePricingPlan	요금제 삭제를 기록합니다.
DeletePricingRule	가격 책정 규칙 삭제를 기록합니다.
DisassociateAccounts	결제 그룹과의 계정 연결 해제를 기록합니다.
DisassociatePricingRules	가격 책정 규칙과 가격 책정 규칙의 연결 해제를 기록합니다.
ListAccountAssociations	결제 그룹의 계정 ID에 대한 액세스를 기록합니다.
ListBillingGroupCostReports	결제 그룹의 실제 AWS 요금에 대한 액세스를 기록합니다.
ListBillingGroups	결제 기간 내 결제 그룹에 대한 액세스를 기록합니다.
ListCustomLineItems	청구 기간 내 사용자 지정 품목에 대한 액세스를 기록합니다.
ListCustomLineItemVersions	사용자 지정 품목의 버전에 대한 액세스를 기록합니다.
ListPricingPlans	청구 기간에 가격 책정 플랜에 대한 액세스를 기록합니다.
ListPricingPlansAssociatedWithPricingRule	가격 책정 규칙과 관련된 가격 책정 플랜에 대한 액세스를 기록합니다.
ListPricingRules	청구 기간에 가격 책정 규칙에 대한 액세스를 기록합니다.

이벤트 이름	정의
ListPricingRulesAssociatedToPricingPlan	요금제와 관련된 가격 책정 규칙에 대한 액세스를 기록합니다.
ListResourcesAssociatedToCustomLineItem	사용자 지정 품목과 관련된 리소스에 대한 액세스를 기록합니다.
ListTagsForResource	리소스의 태그에 대한 액세스를 기록합니다.
TagResource	리소스의 태그 연결을 기록합니다.
UpdateBillingGroup	결제 그룹의 업데이트를 기록합니다.
UpdateCustomLineItem	사용자 지정 품목의 업데이트를 기록합니다.
UpdatePricingPlan	요금제 업데이트를 기록합니다.
UpdatePricingRule	가격 책정 규칙 업데이트를 기록합니다.

AWS 청구 담당자 정보는 다음과 같습니다. CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. AWS Billing Conductor에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 내 사이트에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. AWS 계정자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

AWS Billing Conductor의 이벤트를 AWS 계정포함하여 내 이벤트의 진행 중인 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 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 청구 담당자 활동은 AWS 청구 담당자 CloudTrail API 참조에 의해 기록되고 문서화됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail 사용자 ID 요소를 참조하십시오.

AWS 청구 담당자 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일은 하나 이상의 로그 항목을 포함합니다. 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.

주제

- AutoAssociateAccount
- CreateBillingGroup

AutoAssociateAccount

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

```
{
```

```
    "eventVersion": "1.09",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "billingconductor.amazonaws.com"
    },
    "eventTime": "2024-02-23T00:22:08Z",
    "eventSource": "billingconductor.amazonaws.com",
    "eventName": "AutoAssociateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "billingconductor.amazonaws.com",
    "userAgent": "billingconductor.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "1v14d239-fe63-4d2b-b3cd-450905b6c33",
    "eventID": "14536982-geff-4fe8-bh18-f18jde35218d0",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "requestParameters": {
            "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666",
            "AccountIds": [
                "333333333333"
            ]
        },
        "responseElements": {
            "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666"
        }
    },
    "eventCategory": "Management"
}
```


CreateBillingGroup

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId":"111122223333",
        "accessKeyId":"ASIAIOSFODNN7EXAMPLE"
    },
    "eventTime": "2024-01-24T20:30:03Z",
```

```
    "eventSource": "billingconductor.amazonaws.com",
    "eventName": "CreateBillingGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "100.100.10.10",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "PrimaryAccountId": "444455556666",
        "ComputationPreference": {
            "PricingPlanArn": "arn:aws:billingconductor::111122223333:pricingplan/
TqeITi5Bgh"
        },
        "X-Amzn-Client-Token": "32aafb5s-e5b6-47f5-9795-3a69935e9da4",
        "AccountGrouping": {
            "LinkedAccountIds": [
                "444455556666",
                "111122223333"
            ]
        },
        "Name": "***"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "Arn": "arn:aws:billingconductor::111122223333:billinggroup/444455556666"
    },
    "requestID": "fb26ae47-3510-a833-98fe-3dc0f602gb49",
    "eventID": "3ab70d86-c63e-46fd8d-a33s-ce2970441a8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


AWS 청구 담당자에 대한 규정 준수 검증

제3자 감사자는 여러 규정 AWS 준수 프로그램의 일환으로 AWS 서비스의 보안 및 규정 준수를 평가합니다. AWS 빌링 컨덕터는 AWS 규정 준수 프로그램의 범위에 포함되지 않습니다.

특정 규정 준수 프로그램 범위 내 AWS 서비스 목록은 규정 준수 프로그램별 AWS 범위 내 서비스 규정 준수 프로그램별 참조하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact에서 보고서 다운로드를 참조하세요.

AWS Billing Conductor를 사용할 때의 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 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.
- AWS 규정AWS 준수 리소스 — 이 통합 문서 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS Config 개발자 안내서의 규칙을 통한 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이 AWS 서비스는 보안 업계 표준 및 모범 사례를 준수하는지 확인하는 데 도움이 AWS 되는 내부 보안 상태를 종합적으로 보여줍니다.

AWS 빌링 컨덕터의 탄력성

AWS 글로벌 인프라는 지역 및 가용 AWS 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 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.

AWS 지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS 빌링 컨덕터의 인프라 보안

관리형 서비스로서 AWS 글로벌 네트워크 보안으로 AWS Billing Conductor 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 빌링 컨덕터에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

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

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

할당량 및 제한

다음 테이블에서는 AWS Billing Conductor 내 할당량 및 제한에 대해 설명합니다.

할당량

지급인 계정당 결제 그룹 수	5,000
결제 그룹별 계정 수	1,000
요금제 수	5,000
요금 규칙 수	50,000
요금제에 연결할 수 있는 요금 규칙의 수	500
요금 규칙과 연결할 수 있는 요금제 수	1,000
사용자 지정 품목 수	50,000
백분율 사용자 지정 품목에 연결할 수 있는 소스 값 수	100
플랫 사용자 지정 품목에 연결할 수 있는 백분율 사용자 수	100

제한 사항

다음 테이블의 기타 제한 사항은 늘릴 수 없습니다.

결제 그룹별 결제 그룹 Cost and Usage Reports 수	10
결제 그룹 이름	• 128자 이내여야 합니다 • space을(를) 포함할 수 없습니다 • 특수 문자를 포함할 수 없습니다

결제 그룹 설명	1,024자 이내여야 합니다
요금제 이름	• 128자 이내여야 합니다 • space을(를) 포함할 수 없습니다 • 특수 문자를 포함할 수 없습니다
요금제 설명	1,024자 이내여야 합니다
사용자 지정 품목 이름	• 128자 이내여야 합니다 • space을(를) 포함할 수 없습니다 • 특수 문자를 포함할 수 없습니다

문서 이력

다음 표에서는 이번 AWS 빌링 컨덕터 릴리스에 대한 설명서를 설명합니다.

변경 사항	설명	날짜
업데이트된 설명서	What is AWS Billing Conductor? 를 업데이트했습니다. 주제.	2024년 3월 7일
AWS 관리형 정책에 대한 설명서가 업데이트되었습니다.	`GetBillingGroupCostReport` `AWSBillingConductorReadOnlyAccess` 정책에 추가되었습니다. 에 대한AWS 관리형 정책을 참조하십시오 AWS Billing Conductor.	2024년 2월 8일
마진 요약에 대한 문서 추가	청구 AWS 서비스 그룹별로 마진 세부 정보를 볼 수 있습니다. 청구 그룹별 마진 분석을 참조하십시오.	2023년 12월 14일
사용자 지정 품목에 대한 설명서가 추가되었습니다.	결제 그룹의 특정 연결 계정에 사용자 지정 항목을 적용할 수 있습니다. 청구 그룹별 사용자 지정 항목 만들기를 참조하십시오.	2023년 12월 4일
기본 계정에 대한 설명서 추가	기본 계정을 선택하는 것이 결제 그룹의 견적 비용에 어떤 영향을 미칠 수 있는지 알아보세요. 기본 계정 가입일의 중요성 이해를 참조하십시오.	2023년 10월 26일
사용자 지정 품목 필터에 대한 지원 추가	이제 사용자 지정 품목에 행 항목 필터를 지정할 수 있습니다. 자세한 내용은 백분율 요금 사	2023년 9월 5일

	용자 지정 품목 생성을 참조하십시오.	
견적 비용에 대한 문서가 추가되었습니다.	다음 주제를 참조하십시오. • 견적 비용에 대한 임시 분석 수행 AWS Cost Explorer • AWS 서비스 견적 비용 지원 • IAM 정책 예제: 견적 비용에 대한 액세스 거부	2023년 8월 22일
자동 계정 연결에 대한 지원 추가	이제 자동 계정 연결을 위해 결제 그룹을 활성화할 수 있습니다. 자세한 내용은 결제 그룹 생성, 가격 구성, 사용자 지정 품목을 참조하십시오.	2023년 7월 26일
CSV 다운로드 지원 추가	이제 결제 그룹 마진 분석표에 사용할 CSV 파일을 다운로드할 수 있습니다. 자세한 내용은 결제 그룹별 마진 분석을 참조하십시오.	2023년 6월 6일
최초 릴리스	AWS 빌링 컨덕터 사용 설명서 및 API 참조의 최초 릴리스.	2022년 3월 16일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 AWS 용어집을 참조하세요.

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