aws

사용자 가이드

Application Cost Profiler

Application Cost Profiler: 사용자 가이드

Table of Contents

AWS Application Cost Profiler는 2024년 9월 30일까지 중단되며 더 이상 신규 고객을 받지 않습니다.

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

AWS Application Cost Profiler란?

AWS Application Cost Profiler를 사용하면 서비스 테넌트별로 AWS 청구서와 비용을 구분할 수 있습니다. 테넌트는 사용자, 사용자 그룹 또는 프로젝트일 수 있습니다.

리소스는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 같은 사용자가 작업할 수 있는 엔터티입니다. 선택한 테넌트의 리소스 사용량을 식별할 수 있는지 확인하세요.

일반적인 AWS 리소스 사용에는 조직 내 여러 테넌트를 지원하는 공유 서비스가 포함됩니다. 일부 리소스는 시간 기반 차원을 사용합니다. 리소스의 시간당 사용량이 아닌 테넌트별로 비용 및 청구 정보를 가져오려면 리소스를 Application Cost Profiler와 통합하세요. 이와 같이 세분화된 방식을 사용하면 공유 소프트웨어 솔루션에서 AWS 리소스가 어떻게 소비되는지 이해할 수 있습니다.

Application Cost Profiler에는 시간 기반 차원 또는 시간당 사용량을 사용할 수 있는 다음 리소스가 활성화되어 있습니다.

- Amazon EC2 인스턴스(온디맨드 및 스팟 인스턴스만)
- Amazon Simple Queue Service(Amazon SQS) 대기열
- Amazon Simple Notification Service(Amazon SNS) 주제
- Amazon DynamoDB 읽기 및 쓰기

> **Note**
>
> Amazon SQS, Amazon SNS 및 DynamoDB 사용량은 대부분의 리소스와 달리 시간 기준으로 청구되지 않습니다. 이 경우 한 시간 동안의 사용량(예: DynamoDB의 읽기 및 쓰기 횟수)은 해당 시간 동안 읽기 또는 쓰기가 발생한 시간에 관계없이 여러 테넌트에 할당한 시간의 백분율로 분류됩니다.

다음과 같은 세 단계로 서비스를 Application Cost Profiler와 통합합니다.

1. 보고서 활성화 및 구성 – 이 단계에서는 원하는 최종 결과물의 모습을 정의합니다.
2. 테넌트 사용 데이터를 Application Cost Profiler로 전송 - 이 단계를 진행하려면 테넌트가 리소스를 사용하는 시간과 연결하는 사용 데이터를 만든 다음 해당 사용 데이터를 Application Cost Profiler로 보내는 서비스 내 코드가 필요합니다.

3. 보고서 가져오기 – Application Cost Profiler는 보고서 구성에서 지정한 빈도에 따라 보고서를 제공합니다. 보고서에 테넌트별 사용과 관련된 비용이 표시되므로 청구 내역을 세부적으로 확인할 수 있습니다.

이 단계에 대한 자세한 내용은 시작하기 섹션을 참조하세요.

Application Cost Profiler 시작하기

AWS Application Cost Profiler를 사용하면 AWS 리소스 전체가 아닌 테넌트별로 리소스 사용량을 보고하여 리소스에 대한 비용 정보를 얻을 수 있습니다. 테넌트는 사용자, 사용자 그룹 또는 프로젝트일 수 있습니다. 선택한 테넌트별로 리소스 사용량을 식별할 수 있는지 확인하세요. 테넌트 사용에 대한 비용 보고서를 받으려면 보고서를 구성하고 사용량 데이터를 Application Cost Profiler로 보내세요. 이 섹션에서는 Application Cost Profiler를 사용하기 전에 충족해야 하는 사전 조건에 대해 설명합니다.

주제

에 가입 AWS 계정

가 없는 경우 다음 단계를 AWS 계정완료하여 를 생성합니다.

에 가입하려면 AWS 계정

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

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

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

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

관리자 액세스 권한이 있는 사용자 생성

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

보안 AWS 계정 루트 사용자

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

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하십시오.
2. 루트 사용자에 대해 다중 인증(MFA)을 켭니다.

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

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

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

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

관리 액세스 권한이 있는 사용자로 로그인

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

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

추가 사용자에게 액세스 권한 할당

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

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

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

프로그래밍 방식 액세스 권한 부여

사용자는 AWS 외부에서 와 상호 작용하려는 경우 프로그래밍 방식으로 액세스해야 합니다 AWS Management Console. 프로그래밍 방식 액세스를 부여하는 방법은 에 액세스하는 사용자 유형에 따라 다릅니다 AWS.

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
작업 인력 ID (IAMID 센터에서 관리하는 사용자)	임시 자격 증명을 사용하여 AWS CLI AWS SDKs, 또는 에 대한 프로그래밍 요청에 서명합니다 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 의 경우 AWS Command Line Interface 사용 설명서의 AWS CLI 를 사용하도록 구성을 AWS IAM Identity Center AWS CLI참조하세요. • AWS SDKs, 도구 및 의 경우 AWS SDKs 및 도구 참조 가이드의 IAM Identity Center 인증을 AWS APIs참조하세요.
IAM	임시 자격 증명을 사용하여 AWS CLI AWS SDKs, 또는 에 대한 프로그래밍 요청에 서명합니다 AWS APIs.	IAM 사용 설명서의 AWS 리소스와 함께 임시 자격 증명 사용의 지침을 따릅니다.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
IAM	(권장되지 않음) 장기 보안 인증 정보를 사용하여 AWS CLI AWS SDKs, 또는 에 대한 프로그래밍 요청에 서명합니다 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 의 경우 AWS Command Line Interface 사용 설명서의 IAM 사용자 자격 증명을 사용하여 인증을 AWS CLI참조하세요. • 및 도구에 대한 AWS SDKs 자세한 내용은 AWS SDKs 및 도구 참조 가이드의 장기 보안 인증 정보를 사용하여 인증을 참조하세요. • 의 경우 IAM 사용 설명서의 IAM 사용자에 대한 액세스 키 관리를 AWS APIs참조하세요.

Application Cost Profiler 관련 사전 조건

시작하기 전에 다음 사전 조건을 충족해야 합니다.

- Cost Explorer 활성화

  AWS 계정에 AWS Cost Explorer 대해 를 활성화합니다. Cost Explorer를 활성화하여 계정을 설정하기까지 최대 24시간이 걸릴 수 있습니다. Application Cost Profiler에서 일별 및 월별 보고서를 생성하려면 먼저 Cost Explorer 설정을 완료해야 합니다.

  자세한 내용은 AWS Billing and Cost Management 사용 설명서의 Cost Explorer 활성화를 참조하세요.

- S3 버킷 생성

  Amazon Simple Storage Service(Amazon S3) 버킷을 2개 이상 생성합니다. Application Cost Profiler는 S3 버킷 하나를 이용해 보고서를 제공합니다. 다른 S3 버킷을 사용하여 사용 데이터를

Application Cost Profiler에 업로드합니다. 일반적으로 사용 데이터를 업로드하려면 S3 버킷 1개가 필요합니다. 하지만 보안을 위해 필요한 경우 여러 서비스에 대한 사용량을 권한이 다른 별도의 S3 버킷에 보관할 수 있도록 두 개 이상의 S3 버킷을 사용하는 것이 좋습니다. 이러한 S3 버킷에 Application Cost Profiler 권한을 부여해야 합니다.

Application Cost Profiler의 Amazon S3 버킷 설정에 대한 자세한 내용은 Application Cost Profiler용 Amazon S3 버킷 설정의 내용을 참조하세요.

- 태그 활성화

  리소스가 아닌 태그별로 사용량을 보고하려면 AWS Billing and Cost Management 콘솔에서 해당 태그를 활성화해야 합니다.

  AWS 생성된 태그 활성화에 대한 자세한 내용은 AWS Billing and Cost Management 사용 설명서의 AWS-생성된 비용 할당 태그 활성화를 참조하세요. 사용자 정의 태그에 대한 자세한 내용은 AWS Billing and Cost Management 사용 설명서의 사용자 정의 비용 할당 태그를 참조하세요.

다음 단계

사전 조건을 모두 충족하면 다음과 같이 할 수 있습니다.

- 보고서를 구성하고 사용 데이터를 Application Cost Profiler로 전송 자세한 내용은 보고서 생성 단원을 참조하십시오.
- 생성된 보고서를 가져와서 분석 자세한 내용은 Application Profiler 보고서 사용 단원을 참조하십시오.

Application Cost Profiler용 Amazon S3 버킷 설정

AWS Application Cost Profiler에 사용 데이터를 보내고 이 보고서에서 보고서를 수신하려면 데이터를 저장할 Amazon Simple Storage Service(Amazon S3) 버킷이 AWS 계정에 하나 이상 있고 보고서를 수신할 S3 버킷 하나가 있어야 합니다.

> **Note**
>
> AWS Organizations 사용자의 경우 Amazon S3 버킷은 관리 계정 또는 개별 멤버 계정에 있을 수 있습니다. 관리 계정이 소유한 S3 버킷의 데이터를 사용하여 전체 조직에 대한 보고서를 생

성할 수 있습니다. 개별 멤버 계정의 경우 S3 버킷의 데이터는 해당 멤버 계정에 대한 보고서를 생성하는 데만 사용할 수 있습니다.

생성한 S3 버킷은 이를 생성한 AWS 계정의 소유가 됩니다. S3 버킷에는 표준 Amazon S3 요금이 청구됩니다. Amazon S3 버킷 생성 방법에 대해 자세히 알아보려면 Amazon Simple Storage Service 사용 설명서의 버킷 생성을 참조하세요.

Application Cost Profiler에서 S3 버킷을 사용하려면 Application Cost Profiler에 버킷 읽기 및/또는 쓰기 권한을 부여하는 정책을 해당 버킷에 연결해야 합니다. 보고서를 설정한 후 정책을 수정하면 Application Cost Profiler가 사용 데이터를 읽거나 보고서를 전달하지 못할 수 있습니다.

다음 주제에서는 Amazon S3 버킷을 생성한 후 해당 버킷에 대한 권한을 설정하는 방법을 보여줍니다. 객체 읽기 및 쓰기 기능 외에도 버킷을 암호화한 경우 Application Cost Profiler는 각 버킷의 AWS Key Management Service(AWS KMS) 키에 액세스할 수 있어야 합니다.

주제

Application Cost Profiler에 보고서 전송 S3 버킷에 대한 액세스 권한 부여

Application Cost Profiler가 보고서를 전송하도록 구성하는 S3 버킷에는 Application Cost Profiler가 보고서 객체를 생성하도록 허용하는 정책이 첨부되어 있어야 합니다. 또한 암호화를 활성화하도록 S3 버킷을 구성해야 합니다.

> **Note**
>
> 버킷을 생성할 때 버킷을 암호화하도록 선택해야 합니다. Amazon S3가 관리하는 키(SSE-S3) 또는 AWS KMS(SSE-KMS)에서 관리하는 자체 키(SSE-KMS)로 버킷을 암호화할 수 있습니다. 암호화되지 않은 버킷을 이미 생성한 경우, 버킷을 편집하여 암호화를 추가해야 합니다.

Application Cost Profiler에 보고서 전송 S3 버킷에 대한 액세스 권한을 부여하는 방법은 다음과 같습니다.

1. Amazon S3 콘솔에 로그인합니다.

2. 왼쪽 탐색 창에서 버킷을 선택한 다음 목록에서 버킷을 선택합니다.
3. 권한 탭을 선택한 다음 버킷 정책 옆에 있는 편집을 선택합니다.
4. 정책 섹션에 다음 정책을 삽입합니다. *<bucket_name>*을(를) 버킷 이름으로, *<AWS ##>*을(를) AWS 계정의 ID로 변경합니다.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
          "Action":[
            "s3:PutObject*",
            "s3:GetEncryptionConfiguration"
          ],
          "Resource": [
            "arn:aws:s3:::<bucket-name>",
            "arn:aws:s3:::<bucket-name>/*"
          ],
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<AWS ##>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS ##
>:*"
            }
          }
        }
      ]
    }
```

이 정책에서는 Application Cost Profiler 서비스 주체(`application-cost-profiler.amazonaws.com`)에 지정된 버킷으로 보고서를 전송하는 액세스 권한을 부여합니다. 이 작업은 사용자를 대신해서 실행되며, 보고서 전송 버킷과 관련된 AWS 계정 및 ARN과 헤더를 포함합니다. Application Cost Profiler가 사용자를 대신해서 버킷에 액세스할 때만 `Condition`에서 해당 헤더를 확인합니다.

5. 변경 사항 저장을 선택하면 정책을 버킷에 첨부하여 저장합니다.

SSE-S3 암호화를 이용해 버킷을 만들면 작업이 완료됩니다. SSE-KMS 암호화를 사용한 경우 Application Cost Profiler에 버킷에 대한 액세스 권한을 부여하려면 다음 단계를 따라야 합니다.

6. (선택 사항) 버킷의 속성 탭을 선택하고 기본 암호화에서 AWS KMS 키의 Amazon 리소스 이름(ARN)을 선택합니다. 이 작업을 수행하면 AWS Key Management Service 콘솔과 키가 표시됩니다.
7. (선택 사항) Application Cost Profiler에 AWS KMS 키에 대한 액세스 권한을 부여하는 정책을 추가합니다. 이 정책을 추가하는 방법에 대해 알아보려면 Application Cost Profiler에 SSE-KMS로 암호화된 S3 버킷에 대한 액세스 권한 부여의 내용을 참조하세요.

Application Cost Profiler에 사용 데이터 S3 버킷에 대한 액세스 권한 부여

Application Cost Profiler가 사용 데이터를 읽도록 구성한 S3 버킷에는 Application Cost Profiler가 사용 데이터 객체를 읽도록 허용하는 정책이 연결되어 있어야 합니다.

> **Note**
>
> Application Cost Profiler에 사용 데이터에 대한 액세스 권한을 부여하면 보고서를 처리하는 동안 해당 사용 데이터 객체를 미국 동부(버지니아 북부) AWS 리전에 일시적으로 복사할 수 있다는 데 동의하는 것으로 간주됩니다. 이러한 데이터 객체는 월별 보고서 생성이 완료될 때까지 미국 동부(버지니아 북부) 리전에 보관됩니다.

Application Cost Profiler에 사용 데이터 S3 버킷에 대한 액세스 권한을 부여하는 방법은 다음과 같습니다.

1. Amazon S3 콘솔에 로그인합니다.
2. 왼쪽 탐색 창에서 버킷을 선택한 다음 목록에서 버킷을 선택합니다.
3. 권한 탭을 선택한 다음, 버킷 정책 옆에서 편집을 선택합니다.
4. 정책 섹션에 다음 정책을 삽입합니다. *<bucket-name>*을(를) 버킷 이름으로, *<AWS ##>*을(를) AWS 계정의 ID로 변경합니다.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
```

```
            "Principal":{
              "Service":"application-cost-profiler.amazonaws.com"
            },
            "Action":[
              "s3:GetObject*"
            ],
            "Resource": [
              "arn:aws:s3:::<bucket-name>",
              "arn:aws:s3:::<bucket-name>/*"
            ],
            "Condition": {
              "StringEquals": {
                "aws:SourceAccount": "<AWS ##>"
              },
              "ArnEquals": {
                "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS ##
>:*"
              }
            }
          }
        ]
    }
```

이 정책에서는 Application Cost Profiler 서비스 주체(`application-cost-profiler.amazonaws.com`)에 지정된 버킷에서 데이터를 가져올 수 있는 액세스 권한을 부여합니다. 이 작업은 자동으로 실행되며, 사용 버킷에 대한 AWS 계정 및 ARN을 포함합니다. Application Cost Profiler가 사용자를 대신하여 버킷에 액세스할 때만 `Condition`에서 해당 헤더를 확인합니다.

5. 변경 사항 저장을 선택하면 정책을 버킷에 첨부하여 저장합니다.

버킷이 AWS KMS 관리 키로 암호화되면 다음 섹션의 절차에 따라 Application Cost Profiler에 버킷에 대한 액세스 권한을 부여해야 합니다.

Application Cost Profiler에 SSE-KMS로 암호화된 S3 버킷에 대한 액세스 권한 부여

Application Cost Profiler용으로 구성한 S3 버킷(보고서 버킷에 필요)을 AWS KMS(SSE-KMS)에 저장된 키로 암호화하는 경우에는 Application Cost Profiler에 이를 복호화하는 권한도 부여해야 합니다. 이를 위해 데이터를 암호화하는 데 사용된 AWS KMS 키에 액세스 권한을 부여하세요.

> **Note**
>
> Amazon S3 관리 키로 버킷을 암호화하면 이 절차를 완료하지 않아도 됩니다.

Application Cost Profiler에 SSE-KMS로 암호화된 S3 버킷의 AWS KMS에 대한 액세스 권한을 부여하는 방법은 다음과 같습니다.

1. AWS KMS 콘솔에 로그인합니다.
2. 왼쪽 탐색 메뉴에서 고객 관리 키를 선택한 다음 목록에서 버킷을 암호화하는 데 사용되는 키를 선택합니다.
3. 정책 보기로 전환을 선택한 다음 편집을 선택합니다.
4. 정책 섹션에 다음 정책 설명을 삽입합니다.

```
  {
    "Effect": "Allow",
    "Principal": {
        "Service": "application-cost-profiler.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
          "Condition": {
            "StringEquals": {
              "aws:SourceAccount": "<AWS ##>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS ##
>:*"
            }
  }
```

5. 변경 사항 저장을 선택하여 정책을 키에 첨부하여 저장합니다.
6. Application Cost Profiler가 액세스해야 하는 S3 버킷을 암호화하는 키별로 위의 과정을 반복합니다.

> **Note**
>
> 데이터는 Application Cost Profiler 관리 버킷(암호화됨)으로 가져올 때 S3 버킷에서 복사됩니다. 키에 대한 액세스를 취소하면 Application Cost Profiler가 버킷에서 새 객체를 검색할 수 없습니다. 하지만 이미 가져온 데이터는 보고서 생성에 계속 사용할 수 있습니다.

보고서 생성

사전 조건을 충족하면 AWS 계정 보고서를 구성하여 AWS Application Cost Profiler로 사용 데이터를 전송할 수 있습니다. 이 섹션에서는 보고서를 구성하는 방법과 사용 데이터를 Application Cost Profiler로 보내는 방법을 설명합니다.

Application Cost Profiler 보고서 구성

다음은 생성하려는 보고서를 사용 날짜에 따라 구성하는 방법입니다. 보고서 생성 빈도와 같은 세부 정보를 구성합니다.

> **Note**
>
> AWS 계정이(가) AWS 조직에 속하면 관리 계정 또는 개별 구성원 계정을 이용해 보고서를 구성할 수 있습니다. 개별 계정에 대해 구성된 보고서에는 해당 계정에 대한 데이터만 포함됩니다. 관리 계정을 사용하여 구성된 보고서에는 전체 조직에 대한 데이터가 포함될 수 있습니다. 보고서 출력에 사용되는 Amazon S3 버킷은 보고서 구성을 생성하는 계정에 속해야 합니다.

Application Cost Profiler 보고서 구성 방법

1. 웹 브라우저를 열고 Application Cost Profiler 콘솔에 로그인합니다.
2. 보고서를 구성하거나 수정하려면 지금 시작하기를 선택하세요.
3. 보고서 이름과 보고서 설명을 입력합니다.
4. S3 버킷 이름 입력 필드에 S3 버킷 이름을 입력하고 S3 접두사 입력 필드에 S3 접두사를 입력합니다. S3 버킷 생성 및 Application Cost Profiler 권한 부여에 대한 자세한 내용은 Application Cost Profiler용 Amazon S3 버킷 설정의 내용을 참조하세요.
5. 보고서에 포함하려는 옵션을 선택합니다.
   - 시간 빈도 — 보고서를 일별 또는 월별로 생성할지 또는 둘 다를 기준으로 생성할지 선택합니다.
   - 보고서 출력 형식 — Amazon S3 버킷 내에 생성할 파일 유형을 선택합니다. CSV를 선택하면 Application Cost Profiler가 보고서에 대해 gzip으로 압축된 쉼표로 구분된 값 텍스트 파일을 생성합니다. Parquet를 선택하면 보고서의 Parquet 파일이 생성됩니다.
6. 계속을 선택하여 구성을 저장합니다.

> **Note**
>
> AWSApplication Cost Profiler API를 사용하여 보고서를 구성할 수도 있습니다.

현재 보고서 구성을 보려면 지금 시작하기를 선택하여 보고서 설정을 확인하세요.

> **Note**
>
> 보고서를 하나만 구성할 수 있습니다. 구성 페이지로 돌아가면 기존 보고서가 편집됩니다.

보고서를 구성한 후에는 데이터 모으기가 활성화됩니다. 서비스를 Application Cost Profiler와 통합하여 리소스에 대한 사용 데이터를 제공할 수 있습니다.

서비스의 테넌트 사용 데이터 보고

보고서를 구성했으면 계정의 리소스 또는 서비스에서 테넌트 사용 데이터를 전송할 수 있습니다. 리소스가 특정 테넌트에 사용되면 이를 Application Cost Profiler에 알려야 합니다. 예를 들어 서비스가 다른 테넌트의 API 직접 호출을 수락하는 경우 해당 테넌트에서 API 직접 호출을 시작하고 종료할 때 각 테넌트의 시작 및 종료 시간을 기록합니다. Application Cost Profiler는 이 데이터를 사용하여 각 테넌트의 작업에 소요된 시간을 기준으로 서비스 비용에 대한 보고서를 생성합니다.

Application Cost Profiler에 사용 데이터를 제공하려면 다음과 같이 하세요.

- 리소스 사용 데이터 준비 - 특정 테넌트에 리소스가 사용되는 시기를 설명하는 테이블을 생성합니다.
- 사용 데이터 업로드 – Application Cost Profiler에 액세스 권한을 부여한 Amazon S3 버킷에 테이블을 업로드합니다.
- 사용 데이터 가져오기 – `ImportApplicationUsage` API 작업을 직접적으로 호출하여 Application Cost Profiler에 데이터를 처리할 준비가 되었음을 알립니다.

다음 단원에서는 이러한 단계에 대해 자세히 설명합니다.

주제

1단계: 리소스 사용 데이터 준비

서비스에서 리소스를 사용할 때 해당 리소스를 사용하는 테넌트를 추적할 수 있습니다. 이 데이터를 테이블에 기록해 두면 나중에 Application Cost Profiler가 가져올 수 있도록 업로드할 수 있습니다. 표의 각 행에는 리소스, 리소스를 사용하는 테넌트, 해당 사용의 시작 및 종료 시간에 대한 설명이 나와 있습니다. 예시 리소스는 사용 중인 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스입니다.

이 단계에서는 서비스에 코드를 통합하여 사용에 대한 올바른 정보를 출력해야 합니다.

리소스 사용 테이블에 있는 필드가 다음 테이블에 나와 있습니다.

필드	설명
ApplicationId	시스템에서 사용 중인 애플리케이션 또는 제품을 식별합니다. 테넌트 메타데이터의 범위를 정의합니다.
TenantId	시스템에서 지정된 리소스를 사용 중인 테넌트의 식별자입니다. Application Cost Profiler는 ApplicationId 내에서 이 수준으로 집계됩니다.
TenantDesc	(선택 사항) 자체 추가 보고를 위한 테넌트 관련 추가 데이터
UsageAccountId	리소스가 실행되는 계정(조직에 속한 계정에 중요)
StartTime	Epoch의 타임스탬프(밀리초 및 마이크로초 단위)(UTC) 지정된 테넌트가 사용한 기간의 시작 시간을 나타냅니다.
EndTime	Epoch의 타임스탬프(밀리초 및 마이크로초 단위)(UTC) 지정된 테넌트가 사용한 기간의 종료 시간을 나타냅니다.
ResourceId	사용 중인 리소스의 Amazon 리소스 이름(ARN)
이름	(선택 사항) ResourceId를 지정하는 대신 Name 리소스 태그를 지정하여 비용을 리소스 세트에 할당할 수 있습니다(Name 태그에 사용할 값이

필드	설명
	필드에 포함되어야 함). 비용 및 사용 보고서의 일부로 리소스 태그가 활성화됩니다. 리소스 태그에 대한 자세한 내용은 비용 및 사용 보고서 사용자 설명서의 리소스 태그 세부 정보를 참조하세요.

출력은 다음 예와 같이 제목 행을 포함하고 값이 쉼표로 구분된 파일(.csv)이어야 합니다.

```
ApplicationId,TenantId,TenantDesc,UsageAccountId,StartTime,EndTime,ResourceId
MyApp,Tenant1,,123456789012,1613681437032.9001,1613681437041.5312,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681245531.4426,1613681245551.1323,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant1,,123456789012,1613681904815.3381,1613681904930.0972,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681904765.1956,1613681904946.574,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
```

데이터를 확장명이.csv(또는 gzip으로 압축한 경우에는 .csv.gzip)인 파일로 저장합니다. 이 데이터를 Application Cost Profiler에 업로드하면 각 타임 슬라이스가 연결된 테넌트에 할당됩니다. 이 예시의 보고서에는 해당 테넌트에 대한 Amazon EC2 인스턴스 비용의 타임 슬라이스가 포함됩니다. Amazon EC2 인스턴스의 경우에만, 특정 테넌트와 연결되지 않은 슬라이스는 속성이 지정되지 않은 테넌트에 추가됩니다. 겹치는 타임 슬라이스는 여러 번 집계됩니다. 사용 테이블의 데이터가 정확한지 확인하는 것은 사용자의 책임입니다.

> **Note**
>
> 파일은 1시간 분량이어야 합니다. 리소스가 여러 시간에 걸쳐 사용되면 해당 시간에 사용을 종료하고 같은 시간에 시작되는 다음 파일에 새 레코드를 생성하세요.
> 전체 시간의 데이터가 포함된 파일 하나를 제출해야 합니다. 같은 시간 데이터에 대해 여러 파일이 제출되는 경우 Application Cost Profiler에서는 최신 파일의 데이터만 고려합니다.

예를 들어, 다음 테이블에는 Application Cost Profiler가 제공된 시간 분할을 기반으로 하는 시간(3,600,000밀리초) 동안 세 테넌트에 대한 사용량을 계산하는 방법이 나와 있습니다.

테넌트	제공된 타임 슬라이스	시간당 비용의 계산된 비율
Tenant1	1,200,000 ms	33.34%
Tenant2	600,000 ms	16.66%
<unattributed>		50.00%

이 예에서 Tenant1에는 시간의 1/3이 할당되고, Tenant2에는 시간의 1/6이 할당됩니다. 나머지 30분(1,800,000 ms)은 어느 클라이언트에게도 할당되지 않으며, 이는 시간의 50%에 해당합니다.

현재 Application Cost Profiler에는 다음과 같은 리소스가 활성화되어 있습니다.

- Amazon EC2 인스턴스(온디맨드 및 스팟 인스턴스만)
- Lambda 함수(Lambda 함수에 대한 데이터를 전송하는 경우 Unqualified Resource ARN을 `ResourceId`로 전송해야 함)
- Amazon Elastic Container Service(Amazon ECS) 인스턴스
- Amazon Simple Queue Service(Amazon SQS) 대기열
- Amazon Simple Notification Service(Amazon SNS) 주제
- Amazon DynamoDB 읽기 및 쓰기

> **Note**
>
> Amazon SQS, Amazon SNS 및 DynamoDB 사용량에 대해서는 대부분의 리소스와 달리 시간 단위로 청구되지 않습니다. 이 경우 한 시간 동안의 사용량(예: DynamoDB의 읽기 및 쓰기 횟수)은 해당 시간 동안 읽기 또는 쓰기가 발생한 시점에 관계없이 다른 테넌트에 할당한 시간의 백분율로 분류됩니다.

2단계: 리소스 사용량 업로드

테넌트별 사용량 파일이 있으면 데이터 파일을 Amazon S3에 업로드하고 이에 대한 액세스 권한이 Application Cost Profiler에 있는지 확인하세요.

S3 버킷 생성에 대해 자세히 알아보려면 Application Cost Profiler 관련 사전 조건의 내용을 참조하세요.

Application Cost Profiler가 S3 버킷에 액세스할 수 있는지 확인해야 합니다. 이 작업은 S3 버킷당 한 번만 하면 됩니다(동일한 버킷을 재사용하여 여러 사용 파일을 업로드할 수 있음). 이 버킷에 대한 액세스 권한에 대해 알아보려면 Application Cost Profiler에 사용 데이터 S3 버킷에 대한 액세스 권한 부여의 내용을 참조하세요. 버킷이 암호화된 경우 Application Cost Profiler에 SSE-KMS로 암호화된 S3 버킷에 대한 액세스 권한 부여의 내용을 참조하세요.

> **Note**
>
> 사용 데이터에 사용하는 S3 버킷은 암호화하지 않아도 됩니다.

1시간 간격으로 데이터를 확장명이.csv(또는 gzip으로 압축한 경우는.csv.gzip) 인 파일로 S3 버킷에 업로드합니다. 새 파일을 업로드한 후에는 파일을 보고서로 가져올 수 있도록 Application Cost Profiler에 업로드했음을 알려야 합니다.

> **Note**
>
> Application Cost Profiler에 사용 데이터에 대한 액세스 권한을 부여하면 보고서를 처리하는 동안 해당 사용 데이터 개체를 미국 동부(버지니아 북부) AWS 리전에 일시적으로 복사할 수 있다는 데 동의한 것으로 간주됩니다. 이러한 데이터 객체는 월별 보고서 생성이 완료될 때까지 미국 동부(버지니아 북부) 리전에 있습니다.

3단계: Application Cost Profiler로 사용 데이터 가져오기

Application Cost Profiler가 액세스할 수 있는 Amazon S3 버킷에 사용 데이터를 업로드한 후, Application Cost Profiler에 데이터가 있음을 알리고 이를 최종 보고서로 가져오세요. Application Cost Profiler API의 `ImportApplicationUsage` 작업을 이용해 이 작업을 처리할 수 있습니다.

`ImportApplicationUsage` 작업을 포함하여 AWS Application Cost Profiler API에 대해 자세히 알아보려면 AWS Application Cost Profiler API 참조를 참조하세요.

다음 예에는 `ImportApplicationUsage`를 직접적으로 호출하는 방법이 나와 있습니다. `### ## # # ###`를 S3 버킷과 업로드된 객체의 값으로 대체하세요.

```
POST /ImportApplicationUsage HTTP/1.1
Content-type: application/json

{
```

```
    "sourceS3Location" : {
        "bucket": "<bucket-name>",
        "key": "<object-key>",
        "region": "<region-id>"
    }
}
```

> **Note**
>
> `region` 파라미터는 버킷이 기본적으로 비활성화된 AWS 리전 상태인 경우에만 필요합니다. 자세한 내용은 AWS 일반 참조의 관리 AWS 리전를 참조하세요.

Application Cost Profiler는 `ImportApplicationUsage`로 가져온 데이터를 이용해 보고서를 구성할 때 요청한 빈도에 따라 새 보고서를 생성합니다.

보고서를 구성하고 사용 데이터를 Application Cost Profiler로 자동으로 가져오면 생성된 보고서를 볼 수 있습니다. 보고서에 대한 자세한 내용은 Application Profiler 보고서 사용의 내용을 참조하세요.

Application Profiler 보고서 사용

사용량 데이터를 AWS Application Cost Profiler와 통합하고 시간별 데이터를 전송하면 Application Cost Profiler가 보고서를 자동으로 생성합니다.

보고서를 구성할 때 선택한 옵션에 따라 일별 또는 월별로 보고서가 생성됩니다. 보고서를 구성할 때 선택한 Amazon Simple Storage Service(Amazon S3) 버킷으로 보고서가 전송됩니다.

매월 1일 생성되는 일일 보고서에는 이전 달의 데이터가 포함됩니다.

Application Cost Profiler 보고서에서 제공되는 데이터

사용 보고서에서 생성된 열이 다음 테이블에 나와 있습니다.

열 이름	설명
PayerAccountId	조직의 관리 계정 ID 또는 계정이 AWS Organizations에 속하지 않으면 계정 ID
UsageAccountId	사용 중인 계정의 계정 ID
LineItemType	레코드 유형 항상 Usage입니다.
UsageStartTime	에포크의 타임스탬프(밀리초 단위)(UTC) 지정된 테넌트가 사용한 기간의 시작 시간을 나타냅니다.
UsageEndTime	에포크의 타임스탬프(밀리초 단위)(UTC) 지정된 테넌트가 사용한 기간의 종료 시간을 나타냅니다.
ApplicationIdentifier	Application Cost Profiler로 전송된 사용 데이터에 지정된 ApplicationID
TenantIdentifier	Application Cost Profiler로 전송된 사용 데이터에 지정된 TenantId 사용 데이터에 기록이 없는 데이터는 `unattributed` 에서 수집됩니다.

열 이름	설명
TenantDescription	Application Cost Profiler로 전송된 사용 데이터에 지정된 `TenantDesc`
ProductCode	청구 대상 AWS 제품(예: `AmazonEC2`)
UsageType	청구 대상 사용량 유형(예: `BoxUsage:c5.large`)
Operation	청구 대상 작업(예: `RunInstances`)
ResourceId	청구 대상 리소스의 리소스 ID 또는 Amazon 리소스 이름(ARN)
ScaleFactor	예를 들어 리소스가 1시간 동안 초과 할당된 경우(예: 보고된 사용량 데이터가 1시간이 아닌 2시간으로 표시됨) 총액이 실제 청구 금액(이 경우 0.5)과 같도록 스케일 팩터가 적용됩니다. 이 열에는 해당 시간 동안 특정 리소스에 사용된 스케일 팩터가 표시됩니다. 스케일 팩터는 항상 0보다 크고 1보다 작거나 같습니다.
TenantAttributionPercent	지정된 테넌트에 귀속된 사용량 비율(0에서 1 사이)
UsageAmount	지정된 테넌트에 귀속된 사용량
CurrencyCode	요율 및 비용을 기준으로 하는 통화(예: `USD`)
Rate	사용량에 대한 청구 요금(단위당)
TenantCost	지정된 테넌트의 해당 리소스 총비용
리전(Region)	리소스의 AWS 리전

열 이름	설명
이름	비용 및 사용량 보고서 또는 리소스 사용 데이터를 통해 리소스에 대한 리소스 태그를 생성한 경우 Name 태그가 여기에 표시됩니다. 리소스 태그에 대해 자세히 알아보려면 비용 및 사용량 보고 관련 사용 설명서의 리소스 태그 세부 정보를 참조하세요.

다음은 리소스 1개에 대한 2시간 출력 보고서의 예입니다.

```
PayerAccountId,UsageAccountId,LineItemType,UsageStartTime,UsageEndTime,ApplicationIdentifier,Te
123456789012,123456789012,Usage,2021-02-01T00:00:00.000Z,2021-02-01T00:30:00.000Z,Canary,unattr
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T00:30:00.000Z,2021-02-01T01:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
```

이 예에서는 처음 1시간이 해당 시간의 절반 동안 Tenant1에 할당됩니다. 30분은 unattributed로 남아 있습니다. 두 번째 1시간에는 4명의 테넌트 모두에게 1시간 전체가 할당됩니다. 이 경우 스케일 팩터에 따라 모두 0.25씩 축소되어 각 테넌트에게 1/4 시간이 할당됩니다. TenantCost 열에서 최종 비용을 확인할 수 있습니다.

AWS Application Cost Profiler 할당량 및 엔드포인트

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 다르게 표시되지 않는 한 AWS 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

다음 테이블에는 Application Cost Profiler의 계정별 서비스 할당량 및 AWS 리전 엔드포인트가 나와 있습니다.

서비스 할당량

리소스	기본값	설명
PutReportDefinition 요청 비율	5	계정별 초당 최대 PutReportDefinition 요청 수
UpdateReportDefinition 요청 비율	5	계정별 초당 최대 UpdateReportDefinition 요청 수
GetReportDefinition 요청 비율	5	계정별 초당 최대 GetReportDefinition 요청 수
DeleteReportDefinition 요청 비율	5	계정별 초당 최대 DeleteReportDefinition 요청 수
ListReportDefinitions 요청 비율	5	계정별 초당 최대 ListReportDefinitions 요청 수
ImportApplicationUsage 요청 비율	5	계정별 초당 최대 ImportApplicationUsage 요청 수
사용량 데이터 파일의 최대 크기	10MB	시간당 사용량 데이터 파일의 최대 크기

Service endpoints

Application Cost Profiler는 글로벌 서비스입니다. 모든 API 직접 호출은 미국 동부(버지니아 북부) 엔드포인트로 이루어져야 합니다.

- 미국 동부(버지니아 북부) – `application-cost-profiler.us-east-1.amazonaws.com`

AWS Application Cost Profiler의 보안

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

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

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램의 일환으로 보안 효과를 정기적으로 테스트하고 검증합니다. Application Cost Profiler에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램의 범위에 속하는 AWS 서비스를 참조하세요.
- 클라우드 내 보안 - 사용자의 책임은 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS Application Cost Profiler 사용 시 책임 분담 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 보안 및 규정 준수 목표에 맞게 Application Cost Profiler를 구성하는 방법을 보여줍니다. 또한 Application Cost Profiler 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아보세요.

목차

AWS Application Cost Profiler의 데이터 보호

AWS 공동 책임 모델 AWS Application Cost Profiler의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 섹션을

FAQ참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 책임 공유 모델 및 GDPR 블로그 게시물을 참조하세요.

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

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

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

저장 중 암호화

AWS Application Cost Profiler는 항상 추가 구성 없이 저장 중인 서비스에 저장된 모든 데이터를 암호화합니다. Application Cost Profiler를 사용하면 이 암호화가 자동으로 실행됩니다.

제공하는 Amazon S3 버킷의 경우 보고서 버킷을 암호화해야 하며, 사용 데이터 버킷을 암호화하고 Application Cost Profiler에 액세스 권한을 부여할 수 있습니다. 자세한 내용은 Application Cost Profiler용 Amazon S3 버킷 설정 단원을 참조하십시오.

전송 중 데이터 암호화

AWS Application Cost Profiler는 전송 계층 보안(TLS) 및 클라이언트 측 암호화를 사용하여 전송 중 암호화를 수행합니다. Application Cost Profiler와의 통신은 항상 를 통해 수행HTTPS되므로 전송 중에 데이터가 항상 암호화됩니다. 이 암호화는 Application Cost Profiler를 사용할 때 기본적으로 구성됩니다.

AWS Application Cost Profiler의 자격 증명 및 액세스 관리

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

주제

고객

AWS Identity and Access Management (IAM) 사용 방법은 Application Cost Profiler에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Application Cost Profiler 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Application Cost Profiler 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Application Cost Profiler의 기능에 액세스할 수 없으면 AWS Application Cost Profiler 자격 증명 및 액세스 문제 해결의 내용을 참조하세요.

서비스 관리자 – 회사에서 리소스를 책임지고 있는 경우 Application Cost Profiler에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Application Cost Profiler 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 이해합니다IAM. 회사

에서 Application Cost ProfilerIAM를 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS Application Cost Profiler의 작동 방식 IAM.

IAM 관리자 - IAM 관리자인 경우 Application Cost Profiler에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. 에서 사용할 수 있는 Application Cost Profiler 자격 증명 기반 정책 예제를 보려면 섹션을 IAM참조하세요AWS Application Cost Profiler 자격 증명 기반 정책 예제.

ID를 통한 인증

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

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

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

AWS 프로그래밍 방식으로 에 액세스하는 경우 는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공하여 자격 증명을 사용하여 요청에 암호화 방식으로 서명합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서 의 AWS API 요청에 대한 서명 버전 4를 참조하세요.

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

AWS 계정 루트 사용자

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

IAM 사용자 및 그룹

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

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

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

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 비슷하지만 특정 사람과는 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 역할(콘솔)로 전환할 AWS Management Console수 있습니다. IAM 또는 AWS API 작업을 호출 AWS CLI 하거나 사용자 지정 를 사용하여 역할을 수임할 수 있습니다URL. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자에 대한 역할 생성을 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 의 역할과 상호 연관시킵니다IAM. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 특정 작업에 대해 일시적으로 다른 권한을 맡을 IAM 역할을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 누군가(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다.

그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 에서 교차 계정 리소스 액세스를 IAM 참조하세요.

- 교차 서비스 액세스 - 일부 는 다른 에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가 Amazon에서 애플리케이션을 실행EC2하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하면 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 액세스 세션 전달을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM 역할입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 에 권한을 위임할 역할 생성을 AWS 서비스 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon에서 실행되는 애플리케이션 EC2 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 보안 인증을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장하는 것보다 좋습니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 가져올 수 있습니다. 자세한 내용은 IAM 사용 설명서EC2의 IAM 역할 사용을 참조하세요.

정책을 사용한 액세스 관리

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

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

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

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

보안 인증 기반 정책

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

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

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

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

액세스 제어 목록(ACLs)

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

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

기타 정책 타입

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

- 권한 경계 - 권한 경계는 자격 증명 기반 정책이 IAM 개체(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - 의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책 SCPs입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러 을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직의 모든 기능을 활성화하면 서비스 제어 정책(SCPs)을 계정의 일부 또는 전체에 적용할 수 있습니다. 는 각 를 포함하여 멤버 계정의 엔터티에 대한 권한을 SCP 제한합니다 AWS 계정 루트 사용자. 조직 및 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 SCPs참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

AWS Application Cost Profiler의 작동 방식 IAM

IAM 를 사용하여 Application Cost Profiler에 대한 액세스를 관리하기 전에 Application Cost Profiler에서 사용할 수 있는 IAM 기능을 이해해야 합니다. Application Cost Profiler 및 기타 AWS 서비스가 에서 작동하는 방식을 자세히 알아보려면 IAM 사용 설명서의 AWS 에서 작업하는 서비스를 IAM IAM참조하세요.

주제

Application Cost Profiler 자격 증명 기반 정책

IAM 자격 증명 기반 정책을 사용하면 작업이 허용되거나 거부되는 조건 외에도 허용되거나 거부된 작업 및 리소스를 지정할 수 있습니다. Application Cost Profiler는 특정 작업을 지원합니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

작업

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

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. 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.

Application Cost Profiler의 정책 작업은 작업 앞에 다음 접두사를 사용합니다. `application-cost-profiler:`. 예를 들어 Application Cost Profiler 보고서 정의의 세부 정보 조회 권한을 특정 사용자에게 부여하려면 해당 정책에 `application-cost-profiler:GetReportDefinition` 작업을 포함합니다. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Application Cost Profiler는 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 정의합니다.

명령문 하나에 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "application-cost-profiler:ListReportDefinitions",
      "application-cost-profiler:GetReportDefinition"
```

Application Cost Profiler에서 사용할 수 있는 작업은 다음과 같습니다. 각각은 동일한 이름의 API 작업을 허용합니다. Application Cost Profiler에 대한 자세한 내용은 AWS Application Cost Profiler API 참조를 API참조하세요.

- `application-cost-profiler:ListReportDefinitions` - AWS 계정의 보고서 정의가 있는 경우 나열할 수 있습니다.
- `application-cost-profiler:GetReportDefinition` – Application Cost Profiler 보고서에 대한 보고서 정의의 세부 정보를 가져올 수 있습니다.
- `application-cost-profiler:PutReportDefinition` – 새 보고서 정의를 생성할 수 있습니다.
- `application-cost-profiler:UpdateReportDefinition` – 보고서 정의를 업데이트할 수 있습니다.
- `application-cost-profiler:DeleteReportDefinition` - 보고서를 삭제할 수 있습니다 (Application Cost Profiler를 통해서만 사용 가능API).
- `application-cost-profiler:ImportApplicationUsage` – Application Cost Profiler가 지정된 Amazon S3 버킷에서 사용 데이터를 가져오도록 요청할 수 있습니다.

리소스

Application Cost Profiler는 정책에서 리소스 Amazon 리소스 이름(ARNs) 지정을 지원하지 않습니다.

조건 키

Application Cost Profiler는 서비스별 조건 키를 제공하지 않지만, 일부 전역 조건 키 사용을 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

예시

Application Cost Profiler 자격 증명 기반 정책의 예를 보려면 AWS Application Cost Profiler 자격 증명 기반 정책 예제의 내용을 참조하세요.

Application Cost Profiler 리소스 기반 정책

Application Cost Profiler는 리소스 기반 정책을 지원하지 않습니다.

Application Cost Profiler 태그 기반 권한 부여

Application Cost Profiler는 리소스 태그 지정 또는 태그 기반 액세스 제어를 지원하지 않습니다.

Application Cost Profiler IAM 역할

IAM 역할은 AWS 계정 내에서 특정 권한이 있는 엔터티입니다.

Application Cost Profiler와 함께 임시 자격 증명 사용

임시 자격 증명을 사용하여 페더레이션으로 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole 또는 와 같은 작업을 호출 AWS STS API하여 임시 보안 자격 증명을 얻을 수 있습니다GetFederationToken.

Application Cost Profiler는 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 표시되며 서비스가 소유합니다. 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수는 없습니다.

Application Cost Profiler는 서비스 연결 역할을 지원하지 않습니다.

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 표시되며 계정에서 소유합니다. 즉, 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

Application Cost Profiler는 서비스 역할을 지원하지 않습니다.

AWS Application Cost Profiler 자격 증명 기반 정책 예제

기본적으로 IAM 사용자 및 역할에는 AWS Application Cost Profiler 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 를 사용하여 작업을 수행할 수 없습니다 AWS API. 관리자는 사용자와 역할에 필요한 특정 API 작업을 수행할 수 있는 권한을 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한을 필요로 하는 IAM 사용자 또는 그룹에 해당 정책을 연결해야 합니다.

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

주제

- 정책 모범 사례
- Application Cost Profiler 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 하나의 Amazon S3 버킷에 액세스

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Application Cost Profiler 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 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 작업 함수에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 - IAM 정책으로 권한을 설정할 때 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 적용하는 IAM 방법에 대한 자세한 내용은 IAM 사용 설명서의 에서 정책 및 권한을 IAM 참조하세요.
- IAM 정책의 조건을 사용하여 액세스를 추가로 제한합니다. - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 정책 조건을 작성하여 를 사용하여 모든 요청을 전송하도록 지정할 수 있습니다SSL. AWS 서비스와 같은 특정 를 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 정책이 정책 언어(JSON) 및 IAM 모범 사례를 준수하도록 새 정책 및 기존 IAM 정책을 검증합니다. IAM Access Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 확인 및 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer를 사용한 정책 검증을 참조하세요.
- 다중 인증 필요(MFA) - 에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 MFA 위해 를 AWS 계정켭니다. API 작업을 호출할 MFA 때 를 요구하려면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 를 사용한 보안 API 액세스를 MFA 참조하세요.

의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 의 보안 모범 사례를 IAM IAM참조하세요.

Application Cost Profiler 콘솔 사용

AWS Application Cost Profiler 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 AWS 계정의 Application Cost Profiler 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 생성하는 경우 콘솔은 해당 정책이 있는 엔터티(IAM 사용자 또는 역할)에 대해 의도한 대로 작동하지 않습니다.

이러한 엔터티가 Application Cost Profiler 콘솔을 사용하여 AWS 계정에 대한 Application Cost Profiler 보고서 정의를 볼 수 있도록 하려면 다음 권한을 엔터티에 연결합니다.

```
application-cost-profiler:ListReportDefinitions
application-cost-profiler:GetReportDefinition
```

예를 들어 읽기 전용 사용자를 위해 다음 정책을 생성할 수 있습니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "application-cost-profiler:ListReportDefinitions",
            "application-cost-profiler:GetReportDefinition"
         ],
         "Resource":"*"
      }
   ]
}
```

자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

AWS CLI 또는 에만 전화를 거는 사용자에 대해 최소 콘솔 권한을 허용할 필요는 없습니다 AWS API. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 허용합니다.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함되어 있습니다 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": "*"
        }
    ]
}
```

하나의 Amazon S3 버킷에 액세스

이 예제에서는 AWS 계정의 IAM 사용자에게 Amazon S3 버킷 중 하나인 에 대한 액세스 권한을 부여하려고 합니다examplebucket. 또한 사용자가 객체를 추가, 업데이트 및 삭제하도록 허용하려고 합니다.

이 정책에서는 `s3:PutObject`, `s3:GetObject` 및 `s3:DeleteObject` 권한을 사용자에게 부여할 뿐만 아니라 `s3:ListAllMyBuckets`, `s3:GetBucketLocation` 및 `s3:ListBucket` 권한도 부여합니다. 이러한 권한은 콘솔에 필요한 추가 권한입니다. 또한 콘솔에서 객체를 복사, 자르기 및 붙여넣기를 할 수 있으려면 `s3:PutObjectAcl` 및 `s3:GetObjectAcl` 작업이 필요합니다. 사용자에게 권

한을 부여하고 콘솔을 사용하여 권한을 테스트하는 예제 연습은 예제 연습: 사용자 정책을 사용하여 버킷에 대한 액세스 제어를 참조하십시오.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

AWS Application Cost Profiler 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 AWS Application Cost Profiler 및 AWS Identity and Access Management ()로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다IAM.

주제

Application Cost Profiler에서 작업을 수행할 권한이 없음

에 작업을 수행할 권한이 없다고 AWS Management Console 표시되면 관리자에게 문의하여 지원을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 Application Cost Profiler 보고서에 대한 세부 정보를 보려고 하지만 `application-cost-profiler:ListReportDefinitions` 권한이 없는 경우에 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 application-cost-profiler:ListReportDefinitions on resource: Report Definition
```

이 경우 Mateo는 `application-cost-profiler:ListReportDefinitions` 작업을 사용하여 보고서 정의 리소스에 액세스할 수 있도록 정책을 업데이트할 것을 관리자에게 요청합니다.

iam을 수행할 권한이 없음:PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Application Cost Profiler에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있도록 AWS 서비스 허용합니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 이름이 인 IAM 사용자가 콘솔을 사용하여 Application Cost Profiler에서 작업을 수행하려고 `marymajor` 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 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사람이 내 애플리케이션 비용 프로파일러 리소스에 액세스하도록 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(ACLs)을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Application Cost Profiler가 이러한 기능을 지원하는지 여부를 알아보려면 AWS Application Cost Profiler의 작동 방식 IAM의 내용을 참조하세요.
- 소유 AWS 계정 한 의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유 AWS 계정 한 다른 의 IAM 사용자에게 액세스 권한 제공을 참조하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유 에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- 자격 증명 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부 인증 사용자(자격 증명 페더레이션)에 대한 액세스 제공을 참조하세요.
- 교차 계정 액세스를 위한 역할 및 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 에서 교차 계정 리소스 액세스를 IAM 참조하세요.

AWS 애플리케이션 비용 프로파일러의 규정 준수 검증

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 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 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.

- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 적합한 애플리케이션을 만드는 AWS HIPAA 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 자격이 있는 것은 아닙니다. HIPAA 자세한 내용은 HIPAA적격 서비스 참조를 참조하십시오.

- AWS 규정AWS 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 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (국립 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (), 국제 표준화 기구 ()) 를 포함한PCI) 전반의 보안 제어에 대한 지침을 매핑합니다. ISO
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. 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— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

AWS Application Cost Profiler의 복원성

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

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

AWS 애플리케이션 비용 프로파일러의 인프라 보안

AWS 애플리케이션 비용 프로파일러는 관리형 서비스로서 글로벌 네트워크 보안의 보호를 받습니다 AWS . 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 애플리케이션 비용 프로파일러에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

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

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

EventBridge의 Application Cost Profiler 이벤트 모니터링

Amazon EventBridge를 사용하면 AWS 서비스를 자동화하고 애플리케이션 가용성 문제나 리소스 변경 같은 시스템 이벤트에 자동으로 대응할 수 있습니다. AWS 서비스의 이벤트는 거의 실시간으로 EventBridge로 전송됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.

EventBridge에서 AWS Application Cost Profiler 이벤트를 모니터링할 수 있습니다. EventBridge는 해당 데이터를 AWS Lambda, Amazon Simple Notification Service(SNS) 등의 대상으로 라우팅합니다. 이러한 이벤트는 Amazon CloudWatch Events에 나타나는 이벤트와 동일하며, 이를 통해 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트의 스트림을 거의 실시간 제공합니다.

EventBridge를 이용한 보고서 생성 모니터링

EventBridge를 사용하면 Application Cost Profiler가 생성 중인 보고서에 대한 알림을 전송할 때 수행할 작업을 정의하는 규칙을 생성할 수 있습니다. 예를 들어 보고서가 생성될 때마다 이메일 메시지를 전송하는 규칙을 생성할 수 있습니다.

보고서 생성을 모니터링하는 방법은 다음과 같습니다.

1. EventBridge 및 Application Cost Profiler를 모두 사용할 수 있는 권한이 있는 계정으로 AWS에 로그인합니다.
2. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
3. 다음 값을 사용하여 보고서가 생성될 때 생성되는 이벤트를 모니터링하는 EventBridge 규칙을 생성합니다.

   - 규칙 유형(Rule type)에서 이벤트 패턴이 있는 규칙(Rule with an event pattern)을 생성합니다.
   - 이벤트 소스(Event source)에서 기타(Other)를 선택합니다.
   - 이벤트 패턴 섹션에서 사용자 지정 패턴(JSON 편집기)을 선택하고 다음 이벤트 패턴을 텍스트 영역에 붙여 넣습니다.

```
{
  "source": ["aws.application-cost-profiler"],
  "detail-type": ["Application Cost Profiler Report Generated"]
}
```

- 대상 유형에서는 AWS서비스를 선택하고, 대상 선택에서는 EventBridge가 선택한 유형의 이벤트를 감지했을 때 실행할 AWS 서비스를 선택합니다. 규칙에 정의된 이벤트 패턴과 일치하는 이벤트를 수신할 때 대상이 트리거됩니다.

규칙 생성에 대해 자세히 알아보려면 Amazon EventBridge 사용 설명서의 이벤트에 대응하는 Amazon EventBridge 규칙 생성을 참조하세요.

보고서 생성 이벤트의 예

이 이벤트는 보고서가 생성되고 검색할 준비가 되면 알려줍니다. `message` 필드에서는 Amazon Simple Storage Service(Amazon S3) 버킷과 보고서가 저장된 Amazon S3 객체의 키를 제공합니다.

```
{
   "version": "0",
   "id": "01234567-EXAMPLE",
   "detail-type": "Application Cost Profiler Report Generated",
   "source": "aws.application-cost-profiler",
   "account": "123456789012",
   "time": "2021-03-31T10:23:43Z",
   "region": "us-east-1",
   "resources": [],
   "detail": {
     "message": "Application Cost Profiler report delivered in bucket: SampleBucket,
 key: SampleReport-112233445566"
   }
}
```

문서 기록

다음 테이블에서는 AWS Application Cost Profiler에 대한 문서 릴리스를 소개합니다.

변경 사항	설명	날짜
서비스 지원 중단 알림	AWS Application Cost Profiler는 2024년 9월 30일에 단종되며 더 이상 신규 고객을 받지 않습니다.	2023년 8월 11일
이벤트 모니터링	EventBridge 콘솔의 변경으로 인해 Application Cost Profiler 이벤트를 모니터링하는 규칙을 생성하는 방식이 변경되었습니다. 자세한 내용은 EventBridge의 Application Cost Profiler 이벤트 모니터링을 참조하세요.	2022년 7월 5일
S3 버킷 정책 예시 업데이트	S3 버킷 정책 예시에 대한 설명서 업데이트 자세한 내용은 Application Cost Profiler의 Amazon S3 버킷설정을 참조하세요.	2021년 12월 6일
정식 출시	Application Cost Profiler의 최초 공개 릴리스입니다.	2021년 5월 13일