aws

用户指南

Application Cost Profiler

Application Cost Profiler: 用户指南

Table of Contents

AWS 应用程序成本分析器将于 2024 年 9 月 30 日停产，不再接受新客户。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。

什么是 AWS Application Cost Profiler？

AWS Application Cost Profiler 可帮助您按服务租户区分 AWS 账单和成本。租户可以是一个用户、一组用户或一个项目。

资源是用户可以在 AWS 中使用的实体，例如 Amazon Elastic Compute Cloud (Amazon EC2) 实例。确保您可以根据所选租户识别您的资源使用情况。

典型的 AWS 资源使用情况包括支持组织内的多个租户的共享服务。某些资源使用基于时间的维度。要按租户而不是按资源的每小时使用量获取成本和账单信息，您可以将资源与 Application Cost Profiler 集成。通过这种精细的方法，您可以了解共享软件解决方案中 AWS 资源的消耗情况。

以下资源可以使用基于时间的维度或每小时使用量，系统为 Application Cost Profiler 启用了这些资源：

- Amazon EC2 实例（按需型实例和竞价型实例）
- Amazon Simple Queue Service (Amazon SQS) 队列
- Amazon Simple Notification Service (Amazon SNS) 主题
- Amazon DynamoDB 读取和写入

> **Note**
>
> Amazon SQS、Amazon SNS 和 DynamoDB 使用量不按时间收费，这与大多数资源不同。对它们而言，一小时内的使用量（例如，DynamoDB 中的读取和写入次数）按您分配给不同租户的小时百分比进行分类，而与在这小时内何时发生读取或写入无关。

您可以通过以下三个步骤将您的服务与 Application Cost Profiler 集成：

1. 启用和配置报告：此步骤定义您想要的最终输出是什么样子。
2. 将租户使用量数据发送到 Application Cost Profiler：此步骤需要服务中的代码来创建将租户与他们使用资源的时间相关联的使用量数据，然后将该使用量数据发送到 Application Cost Profiler。
3. 获取报告：Application Cost Profiler 按照您在报告配置中指定的节奏提供报告。这些报告显示与每个租户的使用量关联的成本，使您可以详细了解计费。

有关这些步骤的更多信息，请参阅开始使用。

Application Cost Profiler 入门

AWS Application Cost Profiler 通过按租户而不是整个资源报告资源使用情况，从而帮助您获取有关资源的成本信息。 AWS 租户可以是一个用户、一组用户或一个项目。确保您可以根据所选租户识别您的资源使用情况。要获取有关租户使用情况的成本报告，您可以配置报告并将使用量数据发送到 Application Cost Profiler。本节讨论使用 Application Cost Profiler 之前必须满足的先决条件。

主题

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

授权以编程方式访问

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS Management Console。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
人力身份 （在 IAM Identity Center 中管理的用户）	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的 “配置 AWS CLI 要使用”。 • 有关 AWS 软件开发工具包、工具和 AWS API，请参阅《软件开发工具包和AWS 工具参考指南》中的 IAM 身份中心身份验证。
IAM	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。
IAM	（不推荐使用） 使用长期凭证签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface

哪个用户需要编程式访问权限？	目的	方式
		• 有关 AWS SDK 和工具，请参阅 S AWS DK 和工具参考指南中的使用长期凭证进行身份验证。 • 有关 AWS API，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

Application Cost Profiler 特定先决条件

在开始使用 Application Cost Profiler 之前，您必须满足以下先决条件：

- 启用 Cost Explorer

  AWS Cost Explorer 为您的 AWS 账户启用。使用 Cost Explorer 设置账户可能需要长达 24 小时。您必须先完成 Cost Explorer 设置，然后 Application Cost Profiler 才能生成每日报告和每月报告。

  有关更多信息，请参阅《AWS Billing and Cost Management 用户指南》中的启用 Cost Explorer。

- 创建 S3 存储桶

  创建至少两个 Amazon Simple Storage Service (Amazon S3) 存储桶。Application Cost Profiler 使用一个 S3 存储桶向您提供报告。您可以使用另一个 S3 存储桶将使用量数据上传到 Application Cost Profiler。通常，您只需要一个 S3 存储桶即可上传使用量数据。但是，为了安全起见，您可能需要拥有多个 S3 存储桶，以便可以按不同权限在不同 S3 存储桶中保留不同服务的使用量数据。您必须向 Application Cost Profiler 授予对这些 S3 存储桶的权限。

  有关为 Application Cost Profiler 设置 Amazon S3 存储桶的更多信息，请参阅为 Application Cost Profiler 设置 Amazon S3 存储桶。

- 启用标签

  要按标签而不是按资源报告使用情况，您必须在 AWS Billing and Cost Management 控制台中启用这些标签。

有关激活 AWS 生成的标签的更多信息，请参阅AWS Billing and Cost Management 用户指南中的激活 AWS生成的成本分配标签。有关激活用户定义的标签的更多信息，请参阅《AWS Billing and Cost Management 用户指南》中的激活用户定义的成本分配标签。

后续步骤

满足这些先决条件后，您可以：

- 配置报告并向 Application Cost Profiler 发送使用量数据。有关更多信息，请参阅 创建报告。
- 获取并分析生成的报告。有关更多信息，请参阅 使用 Application Cost Profiler 报告。

为 Application Cost Profiler 设置 Amazon S3 存储桶

要向 AWS Application Cost Profiler 发送使用量数据并从其中接收报告，您的 AWS 账户必须至少有一个用于存储数据的 Amazon Simple Storage Service (Amazon S3) 存储桶，以及一个用于接收报告的 S3 存储桶。

> **Note**
>
> 对于 AWS Organizations 的用户，Amazon S3 存储桶可位于管理账户中，也可以位于个人成员账户中。管理账户拥有的 S3 存储桶中的数据可用于为整个组织生成报告。在个人成员账户中，S3 存储桶中的数据只能用于为该成员账户生成报告。

您创建的 S3 存储桶归您在其中创建这些存储桶的 AWS 账户所有。S3 存储桶按标准的 Amazon S3 费率计费。有关如何创建 Amazon S3 存储桶的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的创建存储桶。

为了让 Application Cost Profiler 使用 S3 存储桶，您必须将策略附加到存储桶，以授予 Application Cost Profiler 读取和/或写入该存储桶的权限。如果您在设置报告后修改策略，则可能会导致 Application Cost Profiler 无法读取您的使用量数据或无法交付报告。

以下主题介绍如何在创建 Amazon S3 存储桶后设置对这些存储桶的权限。除了能够读取和写入对象外，如果您对存储桶进行了加密，则 Application Cost Profiler 还必须有权访问每个存储桶的 AWS Key Management Service (AWS KMS) 密钥。

主题

授予 Application Cost Profiler 访问报告交付 S3 存储桶的权限

您所配置供 Application Cost Profiler 将报告交付到其中的 S3 存储桶必须附加一个允许 Application Cost Profiler 创建报告对象的策略。此外，必须将 S3 存储桶配置为启用加密。

> **Note**
>
> 创建存储桶时，您必须选择对其进行加密。您可以选择使用 Amazon S3 托管密钥 (SSE-S3) 或您自己的 AWS KMS 托管密钥 (SSE-KMS) 来加密您的存储桶。如果您已经创建了未加密的存储桶，则必须编辑存储桶以添加加密。

授予 Application Cost Profiler 访问报告交付 S3 存储桶的权限

1. 转到 Amazon S3 控制台并登录。
2. 从左侧导航部分中选择存储桶，然后从列表中选择您的存储桶。
3. 选择权限选项卡，然后选择存储桶策略旁边的编辑。
4. 在策略部分，插入以下策略。将 *<bucket_name>* 替换为您的存储桶名称，将 *<AWS ##>* 替换为您的 AWS 账户 ID。

```
{
      "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 ##
>:*"
            }
          }
        }
      ]
    }
```

在此策略中，您将授予 Application Cost Profiler 服务主体 (`application-cost-profiler.amazonaws.com`) 访问权限，以将报告交付到指定的存储桶。它将代表您执行此操作，并在您的 AWS 账户中包含一个标头和特定于报告交付存储桶的 ARN。为确保 Application Cost Profiler 仅在代表您进行操作时才访问您的存储桶，`Condition` 会检查是否有这些标头。

5. 选择保存更改以保存您的策略，并将其附加到您的存储桶。

   如果您使用 SSE-S3 加密功能创建了存储桶，那么您的工作就完成了。如果您使用了 SSE-KMS 加密，则必须执行以下步骤才能授予 Application Cost Profiler 访问存储桶的权限。

6. （可选）选择存储桶的属性选项卡，然后在默认加密下面，为您的 AWS KMS 密钥选择“Amazon 资源名称 (ARN)”。此操作会显示 AWS Key Management Service 控制台并显示您的密钥。
7. （可选）添加策略以授予 Application Cost Profiler 访问 AWS KMS 密钥的权限。有关添加此策略的说明，请参阅授予 Application Cost Profiler 访问 SSE-KMS 加密 S3 存储桶的权限。

授予 Application Cost Profiler 访问您的使用量数据 S3 存储桶的权限

您配置的供 Application Cost Profiler 从其中读取使用量数据的 S3 存储桶必须附加一个策略，以允许 Application Cost Profiler 读取使用量数据对象。

> **Note**
>
> 授予 Application Cost Profiler 访问您的使用量数据的权限，即表示您同意我们在处理报告时可以将此类使用量数据对象临时复制到美国东部（弗吉尼亚州北部）AWS 区域。在生成完月度报告之前，这些数据对象将保留在美国东部（弗吉尼亚州北部）区域。

授予 Application Cost Profiler 访问您的使用量数据 S3 存储桶的权限

1. 转到 Amazon S3 控制台并登录。
2. 从左侧导航部分中选择存储桶，然后从列表中选择您的存储桶。
3. 选择权限选项卡，然后选择存储桶策略旁边的编辑。
4. 在策略部分，插入以下策略。将 *<bucket-name>* 替换为存储桶的名称，将 *<AWS ##>* 替换为您的 AWS 账户 ID。

```
{
      "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 ##
>:*"
            }
          }
        }
      ]
    }
```

在此策略中，您将授予 Application Cost Profiler 服务主体 (`application-cost-profiler.amazonaws.com`) 访问权限，以便从指定的存储桶中获取数据。它将代表您执行此操作，并在您的 AWS 账户中包含一个标头和特定于使用情况存储桶的 ARN。为确保 Application Cost Profiler 仅在代表您进行操作时才访问您的存储桶，`Condition` 会检查是否有这些标头。

5. 选择保存更改以保存您的策略，并将其附加到您的存储桶。

如果您的存储桶使用 AWS KMS 托管密钥进行了加密，则您必须按照下一节中的过程授予 Application Cost Profiler 对您的存储桶的访问权限。

授予 Application Cost Profiler 访问 SSE-KMS 加密 S3 存储桶的权限

如果您使用 AWS KMS (SSE-KMS) 中存储的密钥对为 Application Cost Profiler 配置的 S3 存储桶（报告存储桶所需）进行加密，则还必须授予 Application Cost Profiler 对其进行解密的权限。您可以通过授予对用于加密数据的 AWS KMS 密钥的访问权限来完成此操作。

> **Note**
>
> 如果您的存储桶已使用 Amazon S3 托管密钥加密，则您无需完成此过程。

授予 Application Cost Profiler 访问 AWS KMS 以访问 SSE-KMS 加密 S3 存储桶的权限

1. 转到AWS KMS控制台并登录。
2. 从左侧导航栏中选择客户托管密钥，然后从列表中选择用于加密存储桶的密钥。
3. 选择切换到策略视图，然后选择编辑。
4. 在策略部分，插入以下策略声明。

```
  {
    "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. 选择保存更改以保存您的策略，并将其附加到您的密钥。
6. 对加密 Application Cost Profiler 需要访问的 S3 存储桶的每个密钥重复此操作。

> **Note**
>
> 在导入到 Application Cost Profiler 管理的存储桶（已加密）时会从 S3 存储桶中复制数据。如果您撤销对密钥的访问权限，则 Application Cost Profiler 无法从存储桶中检索任何新对象。但是，任何已导入的数据仍可用于生成报告。

创建报告

满足先决条件后，您就可以为 AWS 账户配置报告，并将使用量数据发送到 AWS Application Cost Profiler。本部分介绍如何配置报告以及如何将使用量数据发送到 Application Cost Profiler。

配置 Application Cost Profiler 报告

以下过程介绍如何配置要根据使用日期生成的报告。您可以配置详细信息，例如报告的生成频率。

> **Note**
>
> 如果您的 AWS 账户属于 AWS 组织，则您可以使用管理账户或个人成员账户配置报告。为个人账户配置的报告仅包含该账户的数据。使用管理账户配置的报告可以包含整个组织的数据。用于报告输出的 Amazon S3 存储桶必须属于创建报告配置的账户。

配置 Application Cost Profiler 报告

1. 打开 Web 浏览器并登录 Application Cost Profiler 控制台。
2. 选择立即开始以配置或修改报告。
3. 为您的报告输入报告名称和报告描述。
4. 在输入 S3 存储桶名称字段中输入 S3 存储桶的名称，然后在输入 S3 前缀字段中输入 S3 前缀。有关创建 S3 存储桶和授予 Application Cost Profiler 权限的更多信息，请参阅为 Application Cost Profiler 设置 Amazon S3 存储桶。
5. 选择您希望报告包含的选项：
   - 时间频率：选择是按每日、每月还是按这两者的节奏生成报告。
   - 报告输出格式：选择要在 Amazon S3 存储桶中创建的文件的类型。如果您选择 CSV，则 Application Cost Profiler 会使用 gzip 压缩技术为报告创建一个逗号分隔值文本文件。如果选择 Parquet，则会为报告生成 Parquet 文件。
6. 选择配置以保存您的报告配置。

> **Note**
>
> 您还可以使用 AWS Application Cost Profiler API 来配置报告。

选择立即开始以查看当前报告配置，从而验证报告设置。

> **Note**
>
> 您只能配置单个报告。如果返回到配置页面，则将编辑现有报告。

配置报告后，将启用数据摄取。您可以将服务与 Application Cost Profiler 集成，以为资源提供使用量数据。

报告来自服务的租户使用量数据

配置报告后，就可以从账户中的资源或服务发送租户使用量数据。将资源用于特定租户时，必须通知 Application Cost Profiler。例如，如果服务接受不同租户的 API 调用，则在开始和结束每个租户的 API 调用时，您将记录该租户的开始和结束时间。Application Cost Profiler 使用这些数据按每个租户在工作上花费的时间来生成有关服务成本的报告。

要向 Application Cost Profiler 提供使用量数据，您可以执行以下操作：

- 准备资源使用量数据：创建表以描述特定租户使用资源的具体时间。
- 上传使用量数据：将表上传到您已向 Application Cost Profiler 授予其访问权限的 Amazon S3 存储桶。
- 导入使用量数据：调用 `ImportApplicationUsage` API 操作以通知 Application Cost Profiler 数据已准备就绪并可进行处理。

以下部分详细介绍了每个步骤。

主题

步骤 1：准备资源使用量数据

当服务中正在使用资源时，您可以跟踪哪个租户正在使用该资源。将这些数据记录到一个表中，您可以稍后上传此表以供 Application Cost Profiler 导入。表中的每一行都描述了一项资源、正在使用该资

源的租户，以及使用的开始和结束时间。例如，正在使用的 Amazon Elastic Compute Cloud (Amazon EC2) 实例就是一项资源。

此步骤要求您将代码集成到服务中，以输出有关使用情况的正确信息。

下表列出了资源使用情况表中的字段。

Field	描述
ApplicationId	标识系统中正在使用的应用程序或产品。定义租户元数据的范围。
TenantId	系统中正在消耗指定资源的租户的标识符。Application Cost Profiler 将在 ApplicationId 中聚合到此级别。
TenantDesc	（可选）有关租户的其他数据，供您自己进行其他报告。
UsageAccountId	资源运行所用的账户（对于组织中的账户很重要）。
StartTime	采用 UTC 的纪元时间戳（以毫秒和微秒为单位）。表示指定租户的使用周期的开始时间。
EndTime	采用 UTC 的纪元时间戳（以毫秒和微秒为单位）。表示指定租户的使用周期的结束时间。
ResourceId	正在使用的资源的 Amazon 资源名称 (ARN)。
名称	（可选）作为指定 ResourceId 的一种替代方法，您可以指定名称资源标签，将成本归因于一组资源（该字段必须包含要用于名称标签的值）。资源标签将作为成本和使用情况报告的一部分被启用。有关资源标签的更多信息，请参阅《成本和使用情况报告用户指南》中的资源标签详细信息。

输出必须位于包含标题行的逗号分隔值 (.csv) 文件中，如以下示例所示。

```
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
```

将数据保存为扩展名为 .csv 的文件（如果使用 gzip 压缩，则扩展名为 .csv.gzip）。当您将这些数据上传到 Application Cost Profiler 时，每个时间切片都会分配给关联的租户。在此示例中，报告包含该租户的 Amazon EC2 实例成本的时间切片。未与特定租户关联的切片会添加到无可归属的租户，这仅适用于 Amazon EC2 实例。重叠的时间切片会被多次计数。您有责任确保使用情况表中的数据准确无误。

> **Note**
>
> 您的文件必须表示一小时的时间。如果资源被使用多个小时，请按小时结束使用，并在同时启动的下一个文件中记新记录。
>
> 您必须提交单个包含整整一小时的数据的文件。如果为同一小时的数据提交了多个文件，则 Application Cost Profiler 将仅考虑最新文件中的数据。

例如，下表显示了 Application Cost Profiler 如何根据提供的时间切片计算三个租户一小时（360 万毫秒）的使用量。

租户	提供的时间切片	计算出的每小时成本百分比
Tenant1	120 万毫秒	33.34%
Tenant2	60 万毫秒	16.66%
<无可归属>		50.00%

在此示例中，为 Tenant1 分配了三分之一小时，为 Tenant2 分配了六分之一小时。剩下的半小时（180 万毫秒），即一小时的 50%，未归属于任何一个客户端。

目前，为 Application Cost Profiler 启用了以下资源：

- Amazon EC2 实例（按需型实例和竞价型实例）
- Lambda 函数（如果您要为 Lambda 函数发送数据，则必须以 `ResourceId` 形式发送非限定资源 ARN。）
- Amazon Elastic Container Service (Amazon ECS) 实例
- Amazon Simple Queue Service (Amazon SQS) 队列
- Amazon Simple Notification Service (Amazon SNS) 主题
- Amazon DynamoDB 读取和写入

> **Note**
>
> Amazon SQS、Amazon SNS 和 DynamoDB 使用量不按时间收费，这与大多数资源不同。对它们而言，一小时内的使用量（例如，DynamoDB 中的读取和写入次数）按您分配给不同租户的小时百分比进行分类，而与在这小时内何时发生读取或写入无关。

第 2 步：上传资源使用量数据

获得租户使用情况文件后，将数据文件上传到 Amazon S3 并确保 Application Cost Profiler 有权访问此文件。

要了解有关创建 S3 存储桶的更多信息，请参阅 Application Cost Profiler 特定先决条件。

您必须确保 Application Cost Profiler 有权访问 S3 存储桶。对每个 S3 存储桶只需执行一次此操作（您可以重复使用同一个存储桶来上传多个使用情况文件）。有关提供对存储桶的访问权限的更多信息，请参阅授予 Application Cost Profiler 访问您的使用量数据 S3 存储桶的权限。如果存储桶已加密，请参阅授予 Application Cost Profiler 访问 SSE-KMS 加密 S3 存储桶的权限。

> **Note**
>
> 您不需要对用于存储使用量数据的 S3 存储桶进行加密。

每小时将数据作为扩展名为 .csv 的文件上传到 S3 存储桶（如果使用 gzip 进行了压缩，则扩展名为 .csv.gzip）。上传新文件后，您必须通知 Application Cost Profiler 您已上传该文件，以便该文件可以导入到报告中。

> **Note**
>
> 授予 Application Cost Profiler 访问您的使用量数据的权限，即表示您同意我们在处理报告时可以将此类使用量数据对象临时复制到美国东部（弗吉尼亚州北部）AWS 区域。在生成完月度报告之前，这些数据对象将保留在美国东部（弗吉尼亚州北部）区域。

步骤 3：将使用量数据导入 Application Cost Profiler

将使用量数据上传到 Application Cost Profiler 有权访问的 Amazon S3 存储桶后，通知 Application Cost Profiler 该数据存在并将其导入到最终报告中。您可以使用 Application Cost Profiler API 中的 `ImportApplicationUsage` 操作来执行此操作。

有关 AWS Application Cost Profiler API 的信息（包括 `ImportApplicationUsage` 操作），请参阅 AWS Application Cost Profiler API 参考。

以下示例显示了如何调用 `ImportApplicationUsage`。将########替换为您的 S3 存储桶和已上传对象的值。

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

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

> **Note**
>
> 只有当存储桶处于默认禁用的 AWS 区域中时，才需要 `region` 参数。有关更多信息，请参阅 AWS 一般参考中的管理 AWS 区域。

Application Cost Profiler 使用您通过 `ImportApplicationUsage` 导入的数据按照您在配置报告时请求的频率生成新报告。

配置报告并将使用量数据自动导入到 Application Cost Profiler 后，您就可以查看生成的报告了。有关报告的更多信息，请参阅使用 Application Cost Profiler 报告。

使用 Application Cost Profiler 报告

将使用量数据与 AWS Application Cost Profiler 集成并每小时发送一次数据后，Application Cost Profiler 会自动生成报告。

根据您在配置报告时选择的选项，系统会每天或每月生成一次报告。报告将传送到您在配置报告时选择的 Amazon Simple Storage Service (Amazon S3) 存储桶。

当月第一天生成的每日报告包含上个月的数据。

Application Cost Profiler 报告中提供的数据

下表显示了使用情况报告中创建的列。

列名称	描述
PayerAccountId	组织中的管理账户 ID，或者是账户 ID（如果账户不属于 AWS Organizations）。
UsageAccountId	使用情况账户的账户 ID。
LineItemType	记录的类型。始终为 `Usage`。
UsageStartTime	采用 UTC 的纪元时间戳（以毫秒为单位）。表示指定租户的使用周期的开始时间。
UsageEndTime	采用 UTC 的纪元时间戳（以毫秒为单位）。表示指定租户的使用周期的结束时间。
ApplicationIdentifier	发送到 Application Cost Profiler 的使用量数据中指定的 ApplicationId。
TenantIdentifier	发送到 Application Cost Profiler 的使用量数据中指定的 TenantId。`unattributed` 中收集了使用量数据中没有记录的数据。
TenantDescription	发送到 Application Cost Profiler 的使用量数据中指定的 `TenantDesc` 。

列名称	描述
ProductCode	正被计费的 AWS 产品（例如 AmazonEC2 ）。
UsageType	正被计费的使用量的类型（例如 BoxUsage:c5.large ）。
操作	正被计费的操作（例如 RunInstances ）。
ResourceId	正被计费的资源的资源 ID 或 Amazon 资源名称 (ARN)。
ScaleFactor	如果超额分配资源一小时，例如，报告的使用量数据等于 2 小时而不是 1 小时，则会应用比例系数使总额等于实际账单金额（本例中为 0.5）。此列报告该小时用于特定资源的比例系数。比例系数始终大于零 (0) 且小于或等于 1。
TenantAttributionPercent	归属于指定租户的使用量百分比（介于零 (0) 和 1 之间）。
UsageAmount	归属于指定租户的使用量。
CurrencyCode	费率和成本所使用的货币（例如 USD）。
费率	每单位使用量的账单费率。
TenantCost	指定租户的该资源的总成本。
区域	资源的 AWS 区域。
名称	如果您在成本和使用情况报告上或通过资源使用量数据为资源创建了资源标签，则此处会显示名称标签。有关资源标签的更多信息，请参阅《成本和使用情况报告用户指南》中的资源标签详细信息。

以下是一项资源两小时的输出报告示例。

```
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
```

在此示例中，第一个小时的一半时间分配给了 Tenant1。还剩半个小时为 unattributed。在第二个小时内，为四个租户都分配了整整一小时。在本例中，比例系数会将它们全部缩小 0.25，并且为它们都分配了四分之一小时。您可以在 TenantCost 列中看到最终成本。

AWS Application Cost Profiler 限额和端点

您的 AWS 账户对于每项 AWS 服务都具有默认配额（以前称为限制）。除非另有说明，否则，每个限额都特定于 AWS 区域。您可以请求增加某些配额，但其他一些配额无法增加。

下表列出了 Application Cost Profiler 的每个账户的服务限额以及 AWS 区域端点。

Service Quotas

资源	默认值	描述
PutReportDefinition 请求速率	5	每个账户每秒的最大 PutReportDefinition 请求数。
UpdateReportDefinition 请求速率	5	每个账户每秒的最大 UpdateReportDefinition 请求数。
GetReportDefinition 请求速率	5	每个账户每秒的最大 GetReportDefinition 请求数。
DeleteReportDefinition 请求速率	5	每个账户每秒的最大 DeleteReportDefinition 请求数。
ListReportDefinitions 请求速率	5	每个账户每秒的最大 ListReportDefinitions 请求数。
ImportApplicationUsage 请求速率	5	每个账户每秒的最大 ImportApplicationUsage 请求数。
使用量数据文件的最大大小	10 MB	每小时使用量数据文件的最大大小。

服务端点

Application Cost Profiler 是一项全球服务。所有 API 调用都必须是对美国东部（弗吉尼亚州北部）端点的调用。

- 美国东部（弗吉尼亚北部）– `application-cost-profiler.us-east-1.amazonaws.com`

AWS Application Cost Profiler 的安全性

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是AWS和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS Compliance Programs 的一部分。要了解适用于 Application Cost Profiler 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 AWS Application Cost Profiler 时应用责任共担模式。它说明了如何配置 Application Cost Profiler 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务以帮助您监控和保护 Application Cost Profiler 资源。

目录

AWS 应用程序成本剖析器中的数据保护

分 AWS 担责任模型适用于 AWS 应用程序成本概要分析器中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括使用控制台、API 或 AWS SDK AWS 服务 使用应用程序成本分析器或其他工具包的情况。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

AWS Application Cost Profiler 始终对存储在服务中的所有静态数据进行加密，而无需进行任何其他配置。当您使用 Application Cost Profiler 时，此加密是自动进行的。

对于您提供的 Amazon S3 存储桶，您必须加密报告存储桶，并且可以加密使用量数据存储桶并授予 Application Cost Profiler 访问权限。有关更多信息，请参阅 为 Application Cost Profiler 设置 Amazon S3 存储桶。

传输中加密

AWS 应用程序成本概要分析器使用传输层安全 (TLS) 和客户端加密对传输过程进行加密。与 Application Cost Profiler 的通信始终通过 HTTPS 完成，因此您的数据在传输过程中始终处于加密状态。当您使用 Application Cost Profiler 时，系统默认配置此加密。

AWS 应用程序成本剖析器的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（获取权限）来使用 Application Cost Profiler 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在应用程序成本分析器中所做的工作。

服务用户：如果您使用 Application Cost Profiler 服务来完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Application Cost Profiler 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Application Cost Profiler 中的功能，请参阅对 AWS 应用程序成本概要分析器身份和访问权限进行故障排除。

服务管理员：如果您在公司负责管理 Application Cost Profiler 资源，则您可能具有 Application Cost Profiler 的完全访问权限。您有责任确定您的服务用户应访问哪些 Application Cost Profiler 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Application Cost Profiler 搭配使用的更多信息，请参阅 AWS 应用程序成本分析器如何与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解关于如何编写策略以管理对 Application Cost Profiler 的访问的详细信息。要查看您可在 IAM 中使用的 Application Cost Profiler 基于身份的策略示例，请参阅 AWS 应用程序成本分析器基于身份的策略示例。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

AWS 应用程序成本分析器如何与 IAM 配合使用

在使用 IAM 管理对 Application Cost Profiler 的访问之前，您应了解哪些 IAM 功能可与 Application Cost Profiler 结合使用。要大致了解 Application Cost Profiler 和其他 AWS 服务如何与 IAM 协同工作，请参阅《IAM 用户指南》中的与 IAM 协同工作的AWS 服务。

主题

- Application Cost Profiler 基于身份的策略
- Application Cost Profiler 基于资源的策略
- 基于 Application Cost Profiler 标签的授权
- Application Cost Profiler IAM 角色

Application Cost Profiler 基于身份的策略

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源，以及允许或拒绝操作的条件。Application Cost Profiler 支持特定操作。要了解在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》 中的 IAM JSON 策略元素参考。

操作

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

Application Cost Profiler 中的策略操作在操作前面使用以下前缀：`application-cost-profiler:`。例如，要授予某人查看 Application Cost Profiler 报告定义详细信息的权限，您应将 `application-cost-profiler:GetReportDefinition` 操作纳入其策略中。策略语句必须包含 `Action` 或 `NotAction` 元素。Application Cost Profiler 定义了一组自身的操作，以描述您可以使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示。

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

以下是 Application Cost Profiler 中可用的操作。每个都允许同名的 API 操作。有关 Application Cost Profiler API 的更多信息，请参阅 AWS Application Cost Profiler API 参考。

- `application-cost-profiler:ListReportDefinitions`— 允许列出您 AWS 账户的报告定义（如果有）。

- `application-cost-profiler:GetReportDefinition`：允许获取 Application Cost Profiler 报告的报告定义详细信息。
- `application-cost-profiler:PutReportDefinition`：允许创建新的报告定义。
- `application-cost-profiler:UpdateReportDefinition`：允许更新报告定义。
- `application-cost-profiler:DeleteReportDefinition`：允许删除报告（只能通过 Application Cost Profiler API 获取）。
- `application-cost-profiler:ImportApplicationUsage`：允许请求 Application Cost Profiler 从指定的 Amazon S3 存储桶导入使用量数据。

资源

Application Cost Profiler 不支持在策略中指定资源 Amazon 资源名称 (ARN)。

条件键

Application Cost Profiler 不提供任何特定于服务的条件键，但支持使用某些全局条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

示例

要查看 Application Cost Profiler 基于身份的策略的示例，请参阅 AWS 应用程序成本分析器基于身份的策略示例。

Application Cost Profiler 基于资源的策略

Application Cost Profiler 不支持基于资源的策略。

基于 Application Cost Profiler 标签的授权

Application Cost Profiler 不支持标记资源或基于标签的访问控制。

Application Cost Profiler IAM 角色

I AM 角色是您的 AWS 账户中具有特定权限的实体。

将临时凭证与 Application Cost Profiler 一起使用

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。您可以通过调用AssumeRole或之类的 AWS STS API 操作来获取临时安全证书GetFederationToken。

Application Cost Profiler 支持使用临时凭证。

服务相关角色

服务相关角色允许 AWS 服务访问其他服务中的资源以代表您完成操作。服务相关角色显示在 IAM 账户中，并归该服务所有。管理员可以查看但不能编辑服务相关角色的权限。

Application Cost Profiler 不支持服务相关角色。

服务角色

此功能允许服务代表您担任服务角色。此角色允许服务访问其他服务中的资源以代表您完成操作。服务角色显示在 IAM 账户中，并归该账户所有。这意味着管理员可以更改此角色的权限。但是，这样做可能会中断服务的功能。

Application Cost Profiler 不支持服务角色。

AWS 应用程序成本分析器基于身份的策略示例

默认情况下，IAM 用户和角色没有创建或修改 AWS Application Cost Profiler 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。管理员必须创建 IAM 策略来向用户和角色授予权限，以便执行所需的特定 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅《IAM 用户指南》中的 在 JSON 选项卡上创建策略。

主题

- 策略最佳实践
- 使用 Application Cost Profiler 控制台
- 允许用户查看他们自己的权限
- 访问一个 Amazon S3 存储桶

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Application Cost Profiler 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的AWS 托管策略。

- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 Application Cost Profiler 控制台

要访问 AWS 应用程序成本分析器控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看 AWS 账户中应用程序成本分析器资源的详细信息。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。

为确保这些实体可以使用应用程序成本分析器控制台来查看您 AWS 账户的应用程序成本概要分析器报告定义，请为这些实体附加以下权限。

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

例如，您可以为只读用户创建以下策略。

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

```
         ],
         "Resource":"*"
      }
   ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

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

访问一个 Amazon S3 存储桶

在本示例中，您想向 AWS 账户中的 IAM 用户授予访问您的 Amazon S3 存储桶的权限。examplebucket您还想要允许该用户添加、更新和删除对象。

除了授予该用户 s3:PutObject、s3:GetObject 和 s3:DeleteObject 权限外，此策略还授予 s3:ListAllMyBuckets、s3:GetBucketLocation 和 s3:ListBucket 权限。这些是控制台所需的其他权限。此外，s3:PutObjectAcl 和 s3:GetObjectAcl 操作需要能够在控制台中复制、剪切和粘贴对象。有关向用户授予权限并使用控制台测试这些权限的演练示例，请参阅演练示例：使用用户策略控制对存储桶的访问。

```
{
   "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/*"
      }
   ]
}
```

对 AWS 应用程序成本概要分析器身份和访问权限进行故障排除

使用以下信息来帮助您诊断和修复在使用 AWS 应用程序成本分析器和 AWS Identity and Access Management (IAM) 时可能遇到的常见问题。

主题

- 我无权在 Application Cost Profiler 中执行操作
- 我无权执行 iam：PassRole
- 我想允许 AWS 账户以外的人访问我的应用程序成本分析器资源

我无权在 Application Cost Profiler 中执行操作

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供登录凭证的人。

当 `mateojackson` IAM 用户尝试使用控制台查看有关 Application Cost Profiler 报告的详细信息，但不具有 `application-cost-profiler:ListReportDefinitions` 权限时，会发生以下示例错误。

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

在这种情况下，Mateo 请求管理员更新其策略，以允许他使用 `application-cost-profiler:ListReportDefinitions` 操作访问报告定义资源。

我无权执行 iam：PassRole

如果您收到一个错误，指示您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Application Cost Profiler。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Application Cost Profiler 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许 AWS 账户以外的人访问我的应用程序成本分析器资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Application Cost Profiler 是否支持这些功能，请参阅 AWS 应用程序成本分析器如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

AWS 应用程序成本剖析器的合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业指导方针和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

AWS Application Cost Profiler 中的故障恢复能力

AWS全球基础设施围绕AWS区域和可用区构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之

间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关AWS区域和可用区的更多信息，请参阅AWS全球基础设施。

AWS Application Cost Profiler 的基础设施安全性

作为一项托管式服务，AWS Application Cost Profiler 受 AWS 全球网络安全功能的保护。有关 AWS 安全服务以及 AWS 如何保护基础架构的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础设施保护。

您可以使用 AWS 发布的 API 调用来通过网络访问 Application Cost Profiler。客户端必须支持以下内容：

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

在 EventBridge 中监控 Application Cost Profiler 事件

您可以使用 Amazon EventBridge 自动执行您的 AWS 服务并自动响应系统事件，例如应用程序可用性问题或资源更改。AWS 服务中的事件将近乎实时地传输到 EventBridge。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。

您可以在 EventBridge 中监控 AWS Application Cost Profiler 事件。EventBridge 将该数据路由到诸如 AWS Lambda 和 Amazon Simple Notification Service (Amazon SNS) 之类的目标。这些事件与 Amazon CloudWatch Events 中出现的事件相同，可提供近乎实时的系统事件流，这些系统事件描述 AWS 资源的变化。

使用 EventBridge 监控报告的生成

使用 EventBridge，您可以创建规则，以定义在 Application Cost Profiler 发送告知正在生成报告的通知时要采取的操作。例如，您可以创建一条规则，以便每次生成报告时都向您发送一封电子邮件。

监控报告的生成

1. 使用有权使用 EventBridge 和 Application Cost Profiler 的账户登录 AWS。
2. 访问 https://console.aws.amazon.com/events/，打开 Amazon EventBridge 控制台。
3. 使用以下值创建 EventBridge 规则来监控生成报告时创建的事件：

   - 对于规则类型，选择具有事件模式的规则。
   - 对于事件源，选择其他。
   - 在事件模式部分，选择自定义模式(JSON 编辑器)，然后将以下事件模式粘贴到文本区域：

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

   - 对于目标类型，选择 AWS 服务，对于选择目标，选择要在 EventBridge 检测到所选类型的事件时执行的 AWS 服务。在收到与规则中定义的事件模式匹配的事件时将触发目标。

   要了解如何创建规则的详细信息，请参阅《Amazon EventBridge 用户指南》中的创建对事件作出反应的 Amazon EventBridge 规则。

生成报告事件的示例

当报告已生成并可供您检索时，此事件会通知您。该 `message` 字段为您提供存储报告的 Amazon S3 对象的 Amazon Simple Storage Service (Amazon S3) 存储桶和密钥。

```
{
   "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"
   }
}
```

文档历史记录

下表描述了 AWS Application Cost Profiler 的文档版本。

变更	说明	日期
服务弃用通知	AWS Application Cost Profiler 将于 2024 年 9 月 30 日停用，不再接受新客户。	2023 年 8 月 11 日
监控事件	由于 EventBridge 控制台发生了变化，您创建规则来监控 Application Cost Profiler 事件的方式也发生了变化。有关更多信息，请参阅在 EventBridge 中监控 Application Cost Profiler 事件。	2022 年 7 月 5 日
S3 存储桶策略示例更新	S3 存储桶策略示例的纯文档更新。有关更多信息，请参阅为 Application Cost Profiler 设置 Amazon S3 存储桶。	2021 年 12 月 6 日
通用版	Application Cost Profiler 的第一个公开发行版。	2021 年 5 月 13 日