aws

用户指南

AWS 计费指挥家

AWS 计费指挥家: 用户指南

Table of Contents

什么是 AWS 计费指挥家？

AWS Billing Conductor 是一项定制计费服务，适用于有退款要求的 AWS Marketplace 渠道合作伙伴（合作伙伴）和组织。对于合作伙伴而言，信用卡拒付是获得客户付款的先决条件，并遵循 AWS 账户或 AWS Organizations 计费界限。对于组织而言，退款活动可确保组织将特定团队的成本（例如账目收集）分配给正确的内部预算或损益 (P&L) 报表。

为了实现这些活动，Billing Conductor使客户能够创建其成本的第二个形式版本，以便与客户或账户所有者分享。Pro forma 费用是指在 Billing Conductor 托管账户（分配给账单组的账户）中按照 Billing Conductor 中定义的定价费率使用量（例如，使用全球定价规则将公开定价应用于所有用量）。

> **Note**
>
> 客户将在整个月中观察到可计费成本（与 AWS 发票匹配）和预计成本（匹配Bill ing Conductor 配置）之间存在细微的使用差异。但是，一旦 AWS 开具发票，使用量值将在每个月底相匹配。

定义预估成本使客户能够统一建模其成本，以匹配以下用例之一：

1. 客户协议，可以是在外部协商的合作伙伴用例 AWS
2. 内部会计实务，通常是特定于组织的用例

Billing Conductor 配置不会影响客户的现有发票 AWS 或账单配置（例如，积分共享或基于承诺的折扣，例如预留实例或 Savings Plans）。

客户可以通过执行以下任务来分析管理账户中的预计成本：

- 在 Billing Conductor 中分析利润（同一组账户的预计成本和可计费成本之间的差额）
- 在账单详情页面上查看每月的预计费用
- 为每个账单组创建一个 AWS 成本和使用情况报告 (CUR)

Billing Conductor 托管账户（账单组中的账户）可以在成本和使用情况报告 AWS Cost Explorer、账单仪表板和账单详细信息页面中分析公式成本。

您可以在 Billing Conductor 控制台中或使用 Billing Conductor API 配置账单组、定价计划、定价规则和自定义行项目。

有关 Billing Cond AWS uctor 服务配额的更多信息，请参阅配额和限制。

主题

AWS 计费控制器中的功能

您可以使用 B AWS illing Conductor 功能执行以下操作：

群组账户

将账户整理到账单组中，以获得预计成本的汇总视图。模拟个人客户权益，例如跨服务折扣和 AWS Free Tier 针对每个群体的折扣。

自定义定价

设置全球或特定加价或折扣，并控制免费套餐访问权限。

费用和积分

向账单组添加一次性或定期固定费用或基于百分比的费用或抵免额。

预估形式分析

根据账单控制台中的定价配置分析成本。账单组中的账户可以在 AWS Cost Explorer中对其形式成本进行可视化、预测和创建自定义报告。主账户将跨账户查看账单组中账户应计的所有成本，而非主账户将看到自己的成本。

报告

为每个账单组配置成本和使用量报告。

费率分析

使用账单组毛利报告将应用费 AWS 率与实际费率进行比较。

相关服务

AWS 账单控制台

AWS 账单控制台是所有 AWS 客户的门户，从学生和初创公司到大型企业。您可以使用控制台查看 AWS 账户中运行的资源、管理账单偏好以及访问付款所需的账单工件 AWS。 AWS 账单控制台还提供对您账户支出的高级说明，并作为在 AWS 成本管理产品中注册产品的入口点。

有关更多信息，请参阅 AWS Billing 用户指南。

AWS Cost Explorer

您可以使用 Cost Explorer 界面来可视化、了解和管理一段时间内的 AWS 成本和使用情况。通过创建用于分析成本和使用情况数据的自定义报告，快速入门。在高层次上分析您的数据（例如，所有账户的总成本和使用情况），或者深入研究您的成本和使用情况数据，以确定趋势、查明成本驱动因素并检测异常情况。

有关更多信息，请参阅以下主题：

- 对中的预计成本进行临时分析 AWS Cost Explorer
- 《AWS Cost Management 用户指南》中使用 AWS Cost Explorer分析成本

AWS 成本和使用率报告

AWS 成本和使用情况报告 (AWS CUR) 包含最全面的成本和使用情况数据。您可以使用成本和使用情况报告将 AWS 账单报告发布到您拥有的亚马逊简单存储服务 (Amazon S3) 存储桶。您可以按小时或天、按产品或产品资源、或按您的自定义标签接收成本明细报告。

AWS 每天以逗号分隔值 (CSV) 或 Apache Parquet 格式更新存储桶中的报告一次。你可以使用微软 Excel 或 Apache C OpenOffice alc 等电子表格软件查看报告。您也可以使用 Amazon S3 或 Amazon Athena API 从应用程序访问它们。

AWS 成本和使用情况报告会跟踪您的 AWS 使用情况，并提供与您的账户相关的估计费用。每份报告都包含您在 AWS 账户中使用的 AWS 产品、使用类型和操作的每种独特组合的行项目。

AWS Identity and Access Management (IAM)

Bill AWS ing Conductor 服务与 AWS Identity and Access Management (IAM) 集成。您可以将 IAM 与 B AWS illing Conductor 配合使用，以确保在您的账户中工作的其他人只能获得完成工作所需的访问权限。

您还可以使用 IAM 来控制对所有 AWS 资源的访问权限。这包括但不限于您的账单信息。在开始设置账户结构之前，请务必熟悉 IAM 的基本概念和最佳实践。 AWS

有关如何使用 IAM 的更多信息，请参阅 《IAM 用户指南》中的 IAM 是什么？ 以及 IAM 安全最佳实践。

AWS Organizations（整合账单）

AWS 产品和服务可以适应各种规模的公司，从小型初创公司到企业。如果您的公司规模较大，或成长潜力很大，则您可能希望设置与公司结构相符的多个 AWS 账户。例如，您可以为整个公司设置一个账户，再为每个员工设置单独的员工账户，或者也可以为整个公司设置一个账户，并在其中为每个员工创建 IAM 用户。您可以为整个公司设置账户、为公司内的每个部门或小组设置账户，以及为每个员工设置账户。

如果您创建多个账户，则可以使用 AWS Organizations 的整合账单功能将所有成员账户合并到一个管理账户下，从而接收一个统一的账单。有关更多信息，请参阅AWS Billing 用户指南中的整合组织账单。

了解您的 AWS Billing Conductor 控制面板

AWS Billing Conductor 控制面板提供了关键指标的高级摘要，以帮助您了解自定义定价维度的影响。

关键绩效指标

本节定义了 AWS Billing Conductor 控制面板上提供的关键绩效指标 (KPI)。KPI 都是当月至今累计。在您创建账户或向 AWS Organizations 添加账户时，这些账户将计入此 KPI 中。当您删除账单组时，该账单组中的账户也会计入此 KPI。

- 收费金额 – 根据应用的定价方案定义的自定义费率，所有账单组应计使用量的合并费用。该计算未考虑在账单组之外购买的任何基于承诺的折扣、任何非公开定价或在可计费域中消耗的任何积分。基于承诺的折扣的示例包括预留实例和节省计划。
- AWS成本 — 根据 AWS 账单上的估计费用，所有账单组应计使用量的当月至今合并费用。该计算结果包括在账单组之外购买的任何基于承诺的折扣（如果这些优惠应用于计费域）、任何非公开定价、数量分级折扣和积分。基于承诺的折扣的示例包括预留实例和节省计划。
- 毛利 – 所有账单组应计的当月至今汇总毛利。毛利是通过从收费金额中减去 AWS 成本来计算得到的。根据定价方案和应用的自定义行项目等因素，毛利也可能是负值。

> **Note**
>
> 账单后期调整会影响您的历史毛利。有关更多信息，请参阅分析每个账单组的毛利。

- 账单组 - 包含主账户和相关定价方案的互斥账户组的数量。
- 受监控的账户 - 整合账单系列中当前分配给账单组的账户数量。
- 未受监控的账户 - 整合账单系列中尚未分配给账单组的账户数量。

AWS Billing Conductor 的其他定义

本节定义了整个 AWS Billing Conductor 中使用的其他术语，以帮助您有效地使用该服务。

- 应计费 — 由 AWS 生成并用作计算 AWS 发票的偏差的账单输出。
- 形式 — AWS Billing Conductor 生成的输出。它与您在费率管理（定价配置）和汇总账户可见性（账单组）方面所需的更改一致。
- 资源值 — 用于计算基于百分比的自定义行项目的输入。资源值包括账单组的应计成本以及账单周期内与给定账单组关联的任何固定费用自定义行项目。

按收费金额查看排名前五的账单组

通过参考视觉对象和表格视图，您可以了解产生收入的前五个账单组。要管理现有的账单组，请在控制面板页面上选择管理账单组。

创建账单组、定价配置和自定义行项目

本节介绍如何在 Billing Conductor 中创建 AWS 账单组、定价配置和自定义行项目。每节还概述了在创建每个项目后如何使用账单组表、定价规则表和自定义行项目表。

主题

创建账单组

您可以使用 B AWS illing Conductor 创建账单组来整理您的账户。默认情况下，具有管理员权限的付款人账户可以创建账单组。每个账单组都是相互排斥的。这意味着在给定的账单周期内，一个账户只能属于一个账单组。尽管您可以立即看到账单组细分，但在创建账单组后，最多需要 24 小时才能看到该组的自定义费率反映出来。

> **Note**
>
> 在月中跨账单组转移账户将启动两个账单组回到账单周期开始时间的重新计算。月中转移账户不会影响之前的账单周期。

使用以下步骤创建账单组。

创建账单组

1. 登录 AWS Management Console 并打开 B AWS illing Conduc tor，网址为 https://console.aws.amazon.com/billingconductor/。
2. 在导航窗格中，选择账单组。
3. 选择创建账单组。
4. 对于账单组详细信息，请输入账单组的名称。有关命名限制，请参阅 配额和限制。

5. （可选）对于 描述，输入账单组的描述。
6. 对于定价方案，请选择要与账单组关联的定价方案。要创建定价方案，请参阅 创建定价方案。
7. （可选）对于其他设置，您可以为账单组启用自动账户关联。

> **注意事项**
>
> - 只有一个账单组可以自动关联账户。
> - 启用此功能后，在您的组织中创建或添加的账户将自动关联到该账单组。
> - 如果您目前有 CloudTrail 日志记录，则可以在 CloudTrail 日志中查看您的自动账户关联。

8. 在账户下，选择一个或多个要添加到账单组的账户，或者选择导入组织单位以自动选择组织单位内的账户。有关授予导入 OU 功能访问权限的策略示例，请参阅 授予 Billing Conductor 对导入组织单位功能的访问权限。

   您可以使用表格筛选条件按账户名、账户 ID 或与账户关联的根电子邮件地址进行排序。
9. 主账户继承了查看整个账单组的预计费用和使用情况的功能，并且可以为账单组生成一份预计成本和使用情况报告 (AWS CUR)。

   如果您选择的主账户在当月加入您的组织，则该账单组中所有账户的预计费用将仅包括自主账户加入组织以来累积的费用和使用量。要检查加入日期，请选择验证加入日期。有关更多信息，请参阅 了解主账户加入日期的重要性。
10. 选择创建账单组。

> **注意事项**
>
> - 您必须在步骤 9 中选择您的主账户。账单组创建后，您无法更改主账户。要分配新的主账户，请删除账单组并重新分组您的账户。虽然付款人账户可以包含在账单组中，但不能为付款人账户分配主账户的角色。
> - 如果账单组的主账户离开您的组织，并且该账单组启用了自动账户关联，则该账单组将继续自动关联账户，直到月底。届时，账单组将被自动删除。您可以为现有账单组启用自动账户关联，也可以创建另一个账单组。

账单组表

创建账单组后，您可以在可筛选表中查看账单组的详细信息。可以使用以下维度进行筛选：

- 账单组名称
- 主账户名称
- 主账户 ID
- 账户数量
- 定价方案名称

要查看每个账单组的详细信息，请在表中选择账单组名称。您为自动账户关联功能启用的账单组在账单组名称旁边会有一个自动关联图标。

创建定价规则

您可以在 B AWS illing Conductor 中创建定价规则，以自定义各个账单组的账单费率。定价规则可以是全局的、服务特定的、计费实体特定的，也可以是特定于 SKU 的。您可以使用定价规则为每个相应范围应用折扣或加价。范围域不重叠。当具有不同范围的定价规则包含在单个定价方案中时，范围按从最精细到最不精细的顺序应用。对于全局定价规则，您也可以选择停用或启用 `Always Free Tier` 费率。停用永久免费套餐的定价规则默认为使用类型或操作的第一个付费套餐。默认情况下，具有管理员权限的付款人账户可以创建定价规则。将定价规则应用于账单组后，最长需要 24 小时才能看到账单组的自定义费率反映出来。

单个定价方案可以应用于多个账单组。

按照以下步骤创建定价规则。

创建定价规则

1. 打开 B AWS illing Cond uct o https://console.aws.amazon.com/billingconductor/
2. 在导航窗格中，选择定价配置。
3. 选择定价规则选项卡。
4. 选择创建定价规则。
5. 对于定价规则的详细信息，请输入定价规则的名称。有关命名限制，请参阅 配额和限制。
6. （可选）对于描述，输入定价规则的描述。
7. 对于范围，选择 `Global`、`Service`、`Billing entity` 或 SKU。

- 全局 - 适用于所有使用情况。
- 服务 - 仅适用于给定服务。选择服务时，请选择要为其配置定价费率的服务代码。选择服务时，请从价目表查询 API 中选择要调整的服务代码。
- 账单实体 - 仅适用于给定的账单实体。计费实体是指由 AWS其关联公司提供的服务的卖方，或通过其销售服务的第三方提供商 AWS Marketplace。
- SKU - 仅适用于服务（产品）代码、使用类型和/或操作的唯一组合。

8. 对于类型，选择折扣、加价或分层。

> **Note**
>
> 分层仅适用于全局和服务范围的定价规则。

9. 对于百分比，输入百分比金额。

   如果您以百分比形式输入 **0**，则定价方案将默认为 AWS 按需费率。如果输入十进制值，则会将其四舍五入到最接近的小数点后两位。

10. 对于分层类型，您可以选中分层配置下的复选框以停用“永久免费套餐”，或者保持激活状态。除非明确停用 “永久免费套餐”，否则该套餐将被激活。
11. （可选）要在同一工作流程中创建其他定价规则，请选择添加定价规则。
12. 选择创建定价规则。

定价规则表

创建定价规则后，您可以在可筛选表格中查看定价规则的详细信息。您可以使用以下维度进行筛选：

- 定价规则名称
- 范围
- 类型
- 详细信息
- 费率

创建定价方案

您可以在 B AWS illing Conductor 中创建定价计划，以自定义账单组中账单详细信息的输出。默认情况下，具有管理员权限的付款人账户可以创建定价方案。将定价方案应用于账单组后，最长需要 24 小时才能看到账单组的自定义费率反映出来。

单个定价方案可以应用于多个账单组。

> **Note**
>
> 更新定价方案还会影响与定价方案关联的每个账单组的账单详细信息。如果定价方案与一个或一组账单组关联，则此更改仅影响当前的账单周期。之前的账单周期保持不变。

请按照以下步骤创建定价方案。

创建定价方案

1. 打开 B AWS illing Cond uct o https://console.aws.amazon.com/billingconductor/
2. 在导航窗格中，选择定价配置。
3. 从定价方案选项卡中，选择创建定价方案。
4. 对于定价方案详细信息，请输入定价方案的名称。有关命名限制，请参阅 配额和限制。
5. （可选）对于 描述，输入定价方案的描述。
6. 在定价规则表中，选择要与定价方案关联的定价规则。您可以按定价规则名称、范围、详细信息、类型或费率筛选定价规则。
7. 选择创建定价方案。

定价方案表

创建定价方案后，您可以在可筛选的表格中查看定价方案的详细信息。您可以使用以下维度进行筛选：

- 定价方案名称
- 描述
- 与定价方案关联的定价规则数量

针对每个账单组创建自定义行项目

AWS Billing Conductor 用于创建个性化订单项目并将其应用于账单组 AWS 账户 中的指定项目。

您可以使用自定义订单项来分配成本和折扣。您可以将自定义订单项目计算为固定费用或百分比费用值。将基于百分比的自定义行项目配置为包含或排除资源。这些资源将包括账单组费用和其他在账单周期内与账单组关联的固定自定义行项目。然后，您可以将自定义订单项设置为应用一个月，或者在多个月内重复使用。

创建自定义行项目的常见用例包括但不限于以下几种：

- 分配 AWS Support 费用
- 分配共享服务成本
- 收取托管服务费
- 收取税费
- 分配积分
- 分配 RI 和节省计划节省（而不是按需）
- 添加组织积分和折扣行项目

创建固定费用自定义行项目

使用以下步骤创建自定义行项目，将积分或费用行项目应用于单个账单组。

创建自定义行项目

1. 打开 B AWS illing Cond uct o https://console.aws.amazon.com/billingconductor/
2. 在导航窗格中，选择自定义行项目。
3. 选择创建自定义行项目。
4. 对于自定义行项目详细信息，输入自定义行项目的名称。有关命名限制，请参阅 配额和限制。
5. 对于描述，为自定义行项目输入描述。限制为 255 个字符。
6. 对于账单周期，选择现有账单周期或上一个账单周期。
7. 对于持续时间，选择一个月或循环（未定义结束日期）。
8. 对于账单组，请选择一个账单组。您一次只能将自定义费用与一个账单组关联。
    - （可选）对于已分配账户，您可以将自定义行项目应用于您选择的账单组账户。默认情况下，您的自定义订单项目将应用于您选择的账单组的主账户。

9. 为您的自定义订单项目类型选择固定费用。
10. 选择费用类型并输入输入金额。

    折扣行项目增加积分。这会减少向选定账单组收取的费用。加价行项目增加费用。这会增加向选定账单组收取的金额。所有自定义行项目均以美元为单位。
11. 选择创建。

创建百分比费用自定义行项目

使用以下步骤创建自定义行项目，将积分或费用行项目应用于单个账单组。

创建自定义行项目

1. 打开 B AWS illing Cond uct o https://console.aws.amazon.com/billingconductor/
2. 在导航窗格中，选择自定义行项目。
3. 选择创建自定义行项目。
4. 对于自定义行项目详细信息，输入自定义行项目的名称。有关命名限制，请参阅 配额和限制。
5. 对于描述，为自定义行项目输入描述。限制为 255 个字符。
6. 对于账单周期，选择现有账单周期或上一个账单周期。
7. 对于持续时间，选择一个月或循环（未定义结束日期）。
8. 对于账单组，请选择一个账单组。您一次只能将自定义费用与一个账单组关联。

   - （可选）对于已分配账户，您可以将自定义行项目应用于您选择的账单组账户。默认情况下，您的自定义订单项目将应用于您选择的账单组的主账户。
9. 为您的自定义订单项目类型选择费用百分比。
10. 选择费用类型并输入输入金额。

    折扣行项目增加积分。这会减少向选定账单组收取的费用。加价行项目增加费用。这会增加向选定账单组收取的金额。所有自定义行项目均以美元为单位。
11. （可选）对于资源值，选择要包含在计算中的值。默认情况下，选择账单组的总成本作为资源。这不包括所有固定费用自定义行项目。

    - （可选）默认情况下，节省计划折扣包括在内。要将它们排除在计算范围之外，请选中排除节省计划折扣复选框。
12. （可选）包括一个或多个扁平自定义订单项目。从表格中选择要包含在基于百分比的计算中的每个适用的扁平自定义行项目。

> **Note**
>
> 您可以创建不带关联资源的百分比自定义行项目。这些自定义行项目在您的账单数据中显示一个 $0.00 值。

13. 选择创建。

自定义行项目表

创建自定义行项目后，您可以在可筛选的表格中查看该行项目的详细信息。您可以使用以下维度进行筛选：

- 行项目名称
- 行项目描述
- 收取的金额
- 该行项目归属的账单组
- 该行项目的创建日期

要查看您在以前的账单周期中创建的自定义行项目，请使用日期选择器下拉列表。

编辑自定义行项目

使用以下步骤编辑自定义行项目。

编辑自定义行项目

1. 打开 B AWS illing Cond uct o https://console.aws.amazon.com/billingconductor/
2. 在导航窗格中，选择自定义行项目。
3. 选择创建自定义行项目。
4. 选择要编辑的自定义行项目。
5. 选择编辑。
6. 更改要编辑的参数。

> **Note**
>
> 您无法更改账单周期、账单组、已分配账户、费用类型（固定费用或百分比）或费用金额类型（信用额度或费用）。

7. 选择保存更改。

删除自定义行项目

使用以下步骤删除自定义行项目。

编辑自定义行项目

1. 打开 B AWS illing Cond uct o https://console.aws.amazon.com/billingconductor/
2. 在导航窗格中，选择自定义行项目。
3. 选择创建自定义行项目。
4. 选择要删除的自定义行项目。
5. 选择删除。
6. 阅读删除自定义行项目可能对您的影响，然后选择删除自定义行项目。

AWS 计费指挥家的最佳实践

本节重点介绍使用 AWS 计费控制器时的一些最佳实践。

主题

了解主账户加入日期的重要性

主账户加入贵组织的日期定义了该账单组预计费用的历史界限。如果您选择在月中创建或关联到您的管理账户的主账户，则预计费用将不包括账单组中其他账户的费用，包括在主账户加入之前属于您的组织的账户。

例如，假设主账户在 10 月 15 日加入您的组织。账单组中所有账户的形式账单将仅包括从该日期开始的费用和使用量。尽管账单组中的其他账户在本月之前已成为该组织的成员，但形式账单从10月15日开始生效。

账单组第一个月的计费域名和形式账单域名之间会有差异。pro forma 域名将不包括 10 月 15 日之前累积的任何使用量。第一个月之后，预计费用将包含所有使用量。

为避免账单组第一份账单中的应计费数据和预计数据之间出现这种初始差异，请选择一个在整个月或更早时间内与管理账户关联的主账户。

控制对 AWS 账单指挥的访问权限

账单和成本管理仅可供有权访问付款人或管理账户的用户使用。要授予 IAM 用户创建账单组并在 Billing and Cost Management 控制台中查看 B AWS illing Conductor 关键绩效指标 (KPI) 的权限，您还必须向 IAM 用户授予以下权限：

- 列出组织内的账户

要详细了解如何让用户能够在 Billing Conductor 控制台中创建 AWS 账单组和定价计划，请参阅的身份和访问管理 AWS Billing Conductor。

您也可以使用 Billing Conductor API 以编程方式创建 AWS AWS 账单指挥资源。在配置对 B AWS illing Conductor API 的访问权限时，我们建议创建一个唯一的 IAM 用户以允许编程访问。这有助于您在组织中谁有权访问 B AWS illing Conductor 控制台和 API 之间定义更精确的访问控制。要向多个 IAM 用户授予对 B AWS illing Conductor API 的查询权限，我们建议为每个用户创建一个编程访问权限 IAM 角色。

了解 AWS 计费控制器数据集

虽然 B AWS illing Conductor 数据模型与标准 AWS 账单数据模型有许多相似之处，但仍有一些区别。

AWS 账单指挥不包括：

- 积分（在付款人或关联账户级别兑换）
- Tax
- AWS Support 收费

此外，无论您在标准 AWS 账单域中的共享偏好如何，Billing Conductor 都会与位于同一账单组中的账户共享预留实例和 Savings Plans。

了解 AWS 计费控制器的计算逻辑

B AWS illing Conductor 的计算可以灵活地适应您在给定月份所做的更改，同时保留前一时期账单数据的历史完整性。这最好用一个例子来说明。

在此示例中，我们有两个账单组，A 和 B。账单组 A 从该组中的账户 1 到 3 开始计费周期。在月中，付款人账户将 Account 3 移至 Billing Group B。那时，需要重新计算账单组 A 和 B 的成本，才能准确地模拟最新的变更。移动 Account 3 时，Billing Group A 的使用量将被建模，就好像在当前账单周期内 Account 3 不属于此账单组一样。此外，Billing Group B 的使用量被建模，就好像自计费期开始以来，Account 3 是 Billing Group B 中的一部分。当账户在账单周期内跨组转移时，这种方法无需计算复杂的费率和退款模型。

账单组 A	天数：1-15	天数：16-30	月底
账户 1	100 美元	100 美元	200 美元

账单组 A	天数：1-15	天数：16-30	月底
账户 2	100 美元	100 美元	200 美元
账户 3	100 美元	不适用	不适用
总计	300 美元	200 美元	400 美元

账单组 B	天数：1-15	天数：16-30	月底
账户 4	100 美元	100 美元	200 美元
账户 5	100 美元	100 美元	200 美元
账户 6	100 美元	100 美元	200 美元
账户 3	100 美元	100 美元	200 美元
总计	400 美元	400 美元	800 美元

了解 AWS 计费控制器的更新频率

AWS 账单数据每天至少更新一次。 AWS Billing Conductor 使用这些数据来计算您的形式账单数据。生成的应用于当月的自定义行项目将在 24 小时内反映出来。生成的适用于前一个账单周期的自定义行项目最多可能需要 48 小时才能反映在账单组 “ AWS 成本和使用情况报告” 中，或者反映在给定账单组的账单页面上。

了解 B AWS illing Conductor C AWS UR 和标准 AWS CUR 之间的区别

使用 B AWS illing Conductor 配置创建的标准成本和使用情况报告与预 AWS 计 CUR 之间有一些区别。

- 标准 AWS CUR 计算整合账单系列中每个账户的成本和使用量。每个账单组的预计 AWS CUR 仅包括计算时账单组中的账户。

- 标准 AWS CUR 在发票列中填充一次，发票由生成。 AWS pro forma AWS CUR 不会填充发票列。目前，没有 AWS 根据形式账单数据生成或开具发票。

分析每个账单组的毛利

您可以使用B AWS illing Conductor中的利润摘要和利润详细信息来分析您的总利润率和特定计费组的利润。

使用以下步骤查看单个账单组或一组账单组的毛利。

主题

使用利润摘要查看您的合计利润

查看您的账单组利润率摘要

1. 打开 AWS 账单指挥家，网址为 https://console.aws.amazon.com/billingconductor/。
2. 在导航窗格中的分析下，选择利润摘要。
3. 对于报告类型，选择所有账单组或选择账单组。
4. 如果您选择了选择账单组，请选择一个账单周期和一个或多个账单组。
5. 在 M onth-to-date 概览部分，您可以查看您的收费金额、AWS 成本和保证金。
6. 您可以通过两种方式查看您的利润分析：
   - 作为绩效（最近 13 个月）部分的条形图。
   - 作为利润分析表中的表格。

   图表中以红色显示负毛利，美元金额为负，百分比为负。

了解您的利润分析表

默认情况下，账单组毛利分析表按时间倒序排序。您可以按所有列对表格进行排序，其中包括以下各列：

- 月
- 收费金额
- AWS 成本

- 毛利金额
- 毛利百分比

图表和表格返回所选账单组最近 13 个月的值。如果账单组是在不同的时间创建的，则我们假设所选最早的帐单组的时间范围。

您可以将毛利分析表导出为可下载的 CSV 文件。在毛利分析表旁边，选择下载 CSV。您的下载将自动开始。

> **Note**
>
> 要下载包含账单组毛利分析的 CSV 文件，您必须在 IAM policy 中添加 `billingconductor:ListBillingGroupCostReport` 权限。

使用保证金详情查看您的每 AWS 服务 笔利润

查看您的账单组每项服务的利润

1. 打开 AWS 账单指挥家，网址为 https://console.aws.amazon.com/billingconductor/。
2. 在导航窗格的 “分析” 下，选择 “保证金详情”。
3. 在报告参数下，选择账单周期和账单组。
4. 您可以通过两种方式查看您的利润分析：
    - 作为前五大服务的利润趋势部分的折线图。
    - 作为利润分析表中的表格。

了解您的利润率趋势图

您的利润详细信息将显示一个折线图，该折线图显示所选账单周期内按利润率排在前五位的服务。折线图将显示过去三个月中每项服务的利润率以供比较。

该图表还将包括一个表格，显示所选账单周期内每项服务的利润。该表显示了过去三个月计算出的平均利润，其中包括以下各列：

- 服务名称
- 平均值

- 毛利

如果账单组在过去三个月内未处于活动状态，则图表将仅显示可用的成本报告数据。

了解您的利润分析表

账单组利润分析表包括以下各列：

- 服务名称
- 收费金额
- AWS 成本
- 毛利金额
- 毛利百分比

您可以将毛利分析表导出为可下载的 CSV 文件。在毛利分析表旁边，选择下载 CSV。您的下载将自动开始。

> **Note**
>
> 要下载包含账单组毛利分析的 CSV 文件，您必须在 IAM policy 中添加 `billingconductor:GetBillingGroupCostReport` 权限。

查看您的账单组详细信息

您可以使用账单组详细信息在 AWS Billing Conductor 中监控、分析和编辑您的账单组。账单组详细信息提供月初至今的毛利分析、已应用的自定义行项目的历史记录，以及根据需要编辑和删除账单组的功能。

按自定义定价维度查看账单详细信息

创建并分配账单组和定价方案后，您可以查看自定义账单维度以及所管理的每个账单组的使用类型粒度。

使用以下步骤查看您在形式域中的账单详细信息。

查看您的形式账单详细信息

1. 打开 AWS Billing 控制台，地址：https://console.aws.amazon.com/billing/。
2. 在导航窗格上，选择账单。
3. 选择账单详细信息右上角的设置。
4. 启用形式数据视图。
5. 对于账单组，选择要分析的账单。

您可以按服务和 AWS 地区分析账单组的使用情况，以查看该使用量的成本，这与 AWS Billing Conductor 中定义的费率一致。

您可以在账单详细信息页面的服务 AWS Billing Conductor 下找到自定义行项目。

配置每个账单组的成本和使用情况报告

您可以为创建的每个账单组创建形式 AWS 成本和使用情况报告 (AWS CUR)。形式 AWS CUR 具有与标准 AWS CUR 相同的文件格式、粒度和列数，并且包含给定时间段内可用的最全面的成本和使用情况数据集。

您可以将形式 AWS CUR 发布到您拥有的 Amazon Simple Storage Service (Amazon S3)存储桶。

AWS 每天以逗号分隔值 (CSV) 或 Apache Parquet 格式更新一次您存储桶中的报告。您可以使用 Microsoft Excel 或 Apache OpenOffice Calc 等电子表格软件查看这些报告。您也可以使用 Amazon S3 或 Amazon Athena API 从应用程序访问它们。有关标准 AWS CUR 的更多信息，请参阅AWS成本和使用情况报告用户指南。

使用以下步骤为账单组生成形式 AWS CUR。

为账单组创建形式成本和使用情况报告

1. 打开 AWS Billing 控制台，地址：https://console.aws.amazon.com/billing/。
2. 在导航窗格上，请选择成本和使用情况报告。
3. 在报告表的右上角，选择设置。
4. 启用形式数据视图。
5. 请选择启用。
6. 选择创建报告。
7. 对于报告名称，输入报告名称。
8. 对于数据视图，请选择形式。
9. 对于账单组，请选择一个账单组。
10. 对于其他报告详细信息，请选择包括资源 ID 以在报告中包含各个资源的 ID。
11. 对于数据刷新设置，选择是否希望在账单最终确定后使用成本和使用情况数据的任何新更改刷新 AWS 成本和使用情况报告。在报告刷新后，会将新报告上传到 Amazon S3。

    > **Note**
    >
    > 账单组成本和使用情况报告不包括抵免额、税费或支持费用。

12. 选择下一步。
13. 对于 S3 存储桶，选择配置。

14. 在配置 S3 存储桶 对话框中，执行下列操作之一：

    - 从下拉列表中选择现有存储桶，然后选择下一步。
    - 输入存储桶名称和您要在其中创建新存储桶的 AWS 区域，然后选择下一步。
15. 选择我确认此策略是正确的，然后选择保存。
16. 对于报告路径前缀，输入要在报告名称前面添加的报告路径前缀。

    对于 Amazon Redshift 或 Amazon QuickSight，此步骤是可选的，但对于 Amazon Athena 来说是必需的。

    如果您未指定前缀，默认前缀是您在步骤 4 中为报告指定的名称和报告的日期范围，采用以下格式：

    ```
    /report-name/date-range/
    ```
17. 对于时间粒度，请选择以下选项之一：

    - 小时：如果您希望按小时聚合报告中的行项目，请选择此选项。
    - 每天：如果您希望按天聚合报告中的行项目，请选择此选项。
18. 对于报告版本控制，选择您是希望报告的每个版本覆盖报告的先前版本，还是除了先前版本之外还要传送每个版本。
19. 对于启用报告数据集成，选择是要将成本和使用情况报告上传到 Amazon Athena、Amazon Redshift 还是 Amazon QuickSight。此报告按以下格式压缩：

    - Athena：parquet 压缩
    - Amazon Redshift 或 Amazon QuickSight：.gz 压缩
20. 选择下一步。
21. 在查看报告的设置之后，选择查看并完成。

对中的预计成本进行临时分析 AWS Cost Explorer

AWS 账户在 Billing Conductor 中，账单组可以在 Cost Explorer 中分析、预测和报告预计成本。账单组中的主账号可以为该组中的所有账户执行这些活动。如果您正在使用AWS Organizations，则管理账户无法在 Cost Explorer 中分析、预测或报告预计成本。

账单组托管账户（账单组成员）可以查看他们作为账单组成员的账单周期的成本和使用量数据，并提供预估数据。他们看不到历史可计费成本和使用量数据。

注意事项

- Billing Conductor 托管账户（账单组成员）可以在 Cost Explorer 中查看预计费用。
- Cost Explorer 中不支持按形式计算的每小时粒度数据。
- 要详细了解 Cost Explorer 支持的核心工作流程，请参阅 AWS Cost Management用户指南中的使用 Cost Explorer 浏览数据。

有关AWS 服务该支持形式费用的列表，请参阅AWS 服务 这支持形式成本。

AWS 服务 这支持形式成本

以下云财务管理服务及其功能支持形式成本。

服务和功能	各 AWS 账户 类型的 Support 等级		
	付款人（管理账户）	主账户	已关联（成员账户）
AWS 成本和使用情况报告	支持	是	支持
成本分摊	不支持	否	否
AWS Billing	否	是	支持
控制面板	不支持	是	支持
账单详细信息	支持	是	支持
下载 CSV	不支持	否	否
AWS Cost Explorer	否	是	支持
预测	不支持	是	支持
保存报告	不支持	是	支持
规模优化建议	不支持	否	不支持
成本异常监控	不支持	否	不支持
节省计划建议	不支持	否	不支持
节省计划使用率报告	不支持	否	不支持
节省计划覆盖率报告	不支持	否	不支持
预留建议	不支持	否	不支持
预留使用率报告	不支持	否	不支持

服务和功能	各 AWS 账户 类型的 Support 等级		
预留覆盖率报告	不支持	否	否
AWS Budgets	否	否	不支持
预算报告	不支持	否	不支持

对于不支持形式费用的服务和功能， AWS 账户 将看到按与发票相匹配的可计费费率计算的 AWS 费用。

相关信息

要管理关联账户对应计费退款、积分和折扣的访问权限，请参阅成本管理控制台中偏好设置页面上的AWS Cost Explorer章节。

如果您不希望您的 IAM 实体看到这些服务和功能的具体计费费率，则可以使用 IAM policy 拒绝访问。有关 IAM policy 示例，请参阅 拒绝 Billing 和 Cost Explorer 访问不支持形式费用的服务和功能。

您还可以自定义 IAM policy 以允许或拒绝特定权限。有关计费和成本管理的 IAM 操作的详细列表，请参阅以下主题：

- 《AWS Cost Management 用户指南》中的迁移 AWS Cost Management的访问控制
- 《AWS Billing 用户指南》中的迁移 AWS Billing的访问控制

使用 AWS Billing Conductor API

Billing Conductor API 有 Java、Python、.NET 和 Go 版本。Billing Conductor 中发布的新功能也将作为 API 提供。

有关 AWS Billing Conductor API 的更多信息，请参阅 AWS Billing Conductor API 参考。

AWS 计费控制器中的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 B AWS illing Conductor 的合规计划，请参阅按合规计划划分的 AWS 范围内的服务 服务。
- 云端安全-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。

本文档可帮助您了解在使用 B AWS illing Conductor 时如何应用分担责任模型。以下主题向您展示如何配置 Billing Con AWS ductor 以满足您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Billing Condu AWS ctor 资源。

主题

- AWS 计费控制器中的数据保护
- 的身份和访问管理 AWS Billing Conductor
- 在 AWS 计费指挥中记录和监控
- AWS 计费控制器的合规性验证
- AWS 计费导体的弹性
- 《 AWS 计费指挥家》中的基础设施安全

AWS 计费控制器中的数据保护

分 AWS 担责任模型适用于 AWS 账单指挥中的数据保护。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 multi-factor authentication（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）。这包括当你 AWS 服务 使用控制台、API 或 SDK 与 B AWS illing Con AWS ducto AWS CLI r 或其他人合作时。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。

的身份和访问管理 AWS Billing Conductor

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）并获得授权（具有权限）来使用 Billing Conductor 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 如何 AWS Billing Conductor 与 IAM 配合使用
- AWS Billing Conductor 基于身份的策略示例
- AWSAWS 账单指挥官的托管策略
- AWS Billing Conductor 基于资源的策略示例

- 对 AWS Billing Conductor 身份和访问进行故障排除

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 Billing Conductor 中所做的工作。

服务用户：如果您使用 Billing Conductor 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 Billing Conductor 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 Billing Conductor 中的功能，请参阅 对 AWS Billing Conductor 身份和访问进行故障排除。

服务管理员：如果您在公司负责管理 Billing Conductor 资源，您可能拥有对 Billing Conductor 全部访问权限。您有责任确定您的服务用户应访问哪些 Billing Conductor 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 Billing Conductor 结合使用的更多信息，请参阅 如何 AWS Billing Conductor 与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望详细了解如何编写策略来管理对 Billing Conductor 的访问。要查看可在 IAM 中使用的 Billing Conductor 基于身份的策略示例，请参阅 AWS Billing Conductor 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 账户根用户

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，我们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 角色与基于资源的策略有何不同。
- 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 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，此操作然后在不同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。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

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式策略。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 Simple Storage Service（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。

其它策略类型

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特征，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身份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。

如何 AWS Billing Conductor 与 IAM 配合使用

在使用 IAM 管理对 Billing Conductor 的访问之前，您应了解哪些 IAM 功能可与 Billing Conductor 结合使用。要全面了解 Billing Conductor 和其他 AWS 服务如何与 IAM 配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

主题

- Billing Conductor 基于身份的策略
- Billing Conductor 基于资源的策略
- 访问控制列表 (ACL)

- 基于 Billing Conductor 标签的授权
- Billing Conductor IAM 角色

Billing Conductor 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。Billing Conductor 支持特定的操作、资源和条件键。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。

Billing Conductor 的策略操作在操作前使用以下前缀：`Billing Conductor:`。例如，要授予某人使用 Amazon EC2 `RunInstances` API 操作运行 Amazon EC2 实例的权限，您应将 `ec2:RunInstances` 操作纳入其策略。策略语句必须包含 `Action` 或 `NotAction` 元素。Billing Conductor 定义了一组自己的操作，来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": [
      "ec2:action1",
      "ec2:action2"
```

您也可以使用通配符（*) 指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

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

要查看账单导体操作列表，请参阅 IAM 用户指南中的AWS 账单导体定义的操作。

资源

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。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

Amazon EC2 实例资源具有以下 ARN：

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

有关 ARN 格式的更多信息，请参阅 A mazon 资源名称 (ARN) 和 AWS 服务命名空间。

例如，要在语句中指定 i-1234567890abcdef0 实例，请使用以下 ARN：

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

要指定属于特定账户的所有实例，请使用通配符 (*)：

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

无法对特定资源执行某些 Billing Conductor 操作，例如，用于创建资源的操作。在这些情况下，您必须使用通配符 （*)。

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

许多 Amazon EC2 API 操作涉及多种资源。例如，AttachVolume 将一个 Amazon EBS 卷附加到一个实例，从而使 IAM 用户必须获得相应权限才能使用该卷和该实例。要在单个语句中指定多个资源，请使用逗号分隔 ARN。

```
"Resource": [
```

```
    "resource1",
    "resource2"
```

要查看 Billing Conductor 资源类型及其 ARN 的列表，请参阅 IAM 用户指南中的AWS 计费导体定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 B AWS illing Conductor 定义的操作。

条件键

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。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。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。

Billing Conductor 定义了一组自己的条件键，还支持使用一些全局条件键。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。

所有 Amazon EC2 操作都支持 aws:RequestedRegion 和 ec2:Region 条件键。有关更多信息，请参阅示例：限制对特定区域的访问。

要查看账单导体条件键列表，请参阅 IAM 用户指南中的AWS 账单导体条件密钥。要了解您可以使用哪些操作和资源使用条件密钥，请参阅 Billing Conducto r AWS 定义的操作。

示例

要查看 Billing Conductor 基于身份的策略示例，请参阅 AWS Billing Conductor 基于身份的策略示例。

Billing Conductor 基于资源的策略

基于资源的策略是 JSON 策略文档，它们指定了指定主体可在 Billing Conductor 资源上执行的操作以及在什么条件下可执行。Amazon S3 支持针对 Amazon S3 ###的基于资源的权限策略。基于资源的策略允许您基于资源向其他账户授予使用权限。您还可以使用基于资源的策略来允许 AWS 服务访问您的 Amazon S3 存储#。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的委托人。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源位于不同的 AWS 账户中时，您还必须向委托人实体授予访问资源的权限。通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》 中的 IAM 角色与基于资源的策略有何不同。

Amazon S3 服务仅支持一种类型的基于资源的策略（称为###策略），这种策略附加到###。此策略定义哪些主体实体（账户、用户、角色和联合用户）可以在 *Billing Conductor* 上执行操作。

示例

要查看 Billing Conductor 基于资源的策略示例，请参阅 AWS Billing Conductor 基于资源的策略示例。

访问控制列表 (ACL)

访问控制列表 (ACL) 是您可以附加到资源的被授权者列表。他们向账户授予访问所附加到的资源的权限。您可以将 ACL 附加到 Amazon S3 ###资源。

借助 Amazon S3 访问控制列表 (ACL)，您可以管理对###资源的访问。每个###都有一个作为子资源而附加的 ACL。它定义了向哪些 AWS 账户、IAM 用户或用户组或 IAM 角色授予访问权限以及访问权限的类型。收到资源请求时， AWS 会检查相应的 ACL 以验证请求者是否具有必要的访问权限。

创建###资源时，Amazon S3 将创建一个默认 ACL 以授予资源拥有者对资源的完全控制权限。在以下示例### ACL 中，John Doe 被列为该###的拥有者，并被授予对该###的完全控制权。ACL 可以拥有最多 100 个被授权者。

```
<?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>
```

ACL 中的 ID 字段是 AWS 账户规范用户 ID。要了解如何在您拥有的账户中查看此 ID，请参阅查找 AWS 账户规范用户 ID。

基于 Billing Conductor 标签的授权

您可以将标签附加到 Billing Conductor 资源或将请求中的标签传递到 Billing Conductor。要基于标签控制访问，您需要使用 `Billing Conductor:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

Billing Conductor IAM 角色

I AM 角色是您的 AWS 账户中具有特定权限的实体。

对 Billing Conductor 使用临时凭证

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。

Billing Conductor 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。IAM 管理员可以查看但不能编辑服务相关角色的权限。

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，IAM 管理员可以更改该角色的权限。但是，这样做可能会中断服务的功能。

Billing Conductor 支持服务角色。

在 Billing Condoctor 中选择 IAM 角色

在 Billing Conductor 中创建资源时，您必须选择一个角色以允许 Billing Conductor 代表您访问 Amazon EC2。如果您之前已经创建了一个服务角色或服务相关角色，Billing Conductor 会为您提供一个角色列表供您选择。选择一个允许访问以启动和停止 Amazon EC2 实例的角色很重要。

AWS Billing Conductor 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 Billing Conductor 资源的权限。他们也无法使用 AWS Management Console AWS CLI、或 AWS API 执行任务。IAM 管理员必须创建 IAM 策略，以便为用户和角色授予权限以对所需的指定资源执行特定的 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

基于身份的策略决定某人是否可以在您的账户中创建、访问或删除 Billing Conductor 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，请遵循以下准则和建议：

- 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的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 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 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

Billing Conductor 基于身份策略示例

本主题包含几个示例策略，您可以将它们附加到您的 IAM 用户或组以控制对您的账户的信息和工具的访问权限。

主题

- 授予对 Billing Condoctor 控制台的完全访问权限
- 授予对 Billing Condoctor API 的完全访问权限
- 授予对 Billing Condoctor 控制台的只读访问权限
- 通过账单控制台授予 Billing Conductor 访问权限
- 通过 AWS 成本和使用情况报告授予计费指挥员访问权限
- 授予 Billing Conductor 对导入组织单位功能的访问权限
- 拒绝 Billing 和 Cost Explorer 访问不支持形式费用的服务和功能

授予对 Billing Condoctor 控制台的完全访问权限

要访问 Billing Conductor 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有关您的 AWS 账户中的 Billing Conductor 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。

为确保这些实体仍然可以使用 Billing Conductor 控制台，还需要将以下 AWS 托管策略附加到这些实体。有关更多信息，请参阅 《IAM 用户指南》中的为用户添加权限：

除 `billingconductor:*` 权限外，创建定价规则需要 `pricing:DescribeServices`，并且列出与付款人账户关联的关联账户需要 `organizations:ListAccounts`。

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

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。

授予对 Billing Condoctor API 的完全访问权限

在此示例中，您授予 IAM 实体对 Billing Conductor API 的完全访问权限。

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

```
        }
    ]
}
```

授予对 Billing Condoctor 控制台的只读访问权限

在本示例中，您授予 IAM 实体对 Billing Conductor 控制台的只读访问权限。

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

通过账单控制台授予 Billing Conductor 访问权限

在此示例中，IAM 实体可以通过账单控制台中的账单页面切换和查看形式账单数据。

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

```
        }
    ]
}
```

通过 AWS 成本和使用情况报告授予计费指挥员访问权限

在此示例中，IAM 实体可以通过其账单控制台中的 “成本和使用情况报告” 页面切换和查看形式账单数据。

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

授予 Billing Conductor 对导入组织单位功能的访问权限

在此示例中，IAM 实体对创建账单组时导入组织单位 (OU) 账户所需的特定 AWS Organizations API 操作具有只读访问权限。导入 OU 功能在 B AWS illing Conductor 控制台上。

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

```
}
```

拒绝 Billing 和 Cost Explorer 访问不支持形式费用的服务和功能

在此示例中，IAM 实体被拒绝访问不支持形式费用的服务和功能。该政策包括管理账户和个人成员账户中可能采取的操作清单。

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

有关更多信息，请参阅 AWS 服务 这支持形式成本。

AWSAWS 账单指挥官的托管策略

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只

读权限。有关工作职能策略的列表和说明，请参阅《IAM 用户指南》中的适用于工作职能的AWS 托管式策略。

AWS 托管策略： AWSBillingConductorFullAccess

AWSBillingConductorFullAccess 托管策略授予对 AWS 账单指挥控制台和 API 的完全访问权限。用户可以列出、创建和删除 Billing Cond AWS uctor 资源。

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

AWS 托管策略： AWSBillingConductorReadOnlyAccess

AWSBillingConductorReadOnlyAccess 托管策略授予 Billing Conduct AWS or 控制台和 API 的只读权限 用户可以查看和列出所有 AWS 计费指挥资源。用户无法创建或删除资源。

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

```
    ]
}
```

AWS 账单指挥官更新了 AWS 托管政策

查看自该服务开始跟踪这些更改以来，B AWS illing Conductor AWS 托管政策更新的详细信息。要获得有关此页面变更的自动提醒，请在 B AWS illing Conductor 文档历史记录页面上订阅 RSS 提要。

更改	描述	日期
AWSBillingConductorReadOnlyAccess	已`GetBillingGroupCostReport` 添加到`AWSBillingConductorReadOnlyAccess` 策略中。	2024 年 2 月 8 日
AWSBillingConductorFullAccess	创建策略	2022 年 3 月 29 日
AWSBillingConductorReadOnlyAccess	创建策略	2022 年 3 月 29 日
AWS 账单指挥变更日志已发布	AWS Billing Conductor 开始跟踪其 AWS 托管策略的变化	2022 年 3 月 29 日

AWS Billing Conductor 基于资源的策略示例

主题

- 限制 Amazon S3 存储桶对特定 IP 地址的访问权限

限制 Amazon S3 存储桶对特定 IP 地址的访问权限

以下示例向任何用户授予对指定存储桶中的对象执行任何 Amazon S3 操作的权限。但是，请求必须来自条件中指定的 IP 地址范围。

此语句中的条件确定允许的 Internet 协议版本 4 (IPv4) IP 地址范围为 54.240.143.*，只有一个例外：54.240.143.188。

该Condition模块使用IpAddress和NotIpAddress条件和aws:SourceIp条件键，后者是一个 AWS 宽条件键。有关这些条件键的更多信息，请参阅在策略中指定条件。aws:sourceIp IPv4 值使用标准 CIDR 表示法。有关更多信息，请参阅 《IAM 用户指南》中的 IP 地址条件运算符。

```
{
  "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"}
      }
    }
  ]
}
```

对 AWS Billing Conductor 身份和访问进行故障排除

以下信息可帮助您诊断和修复在使用 Billing Conductor 和 IAM 时可能遇到的常见问题。

主题

- 我没有在 Billing Conductor 中执行操作的权限
- 我无权执行 iam：PassRole
- 我想允许 AWS 账户以外的人访问我的 Billing Conductor 资源

我没有在 Billing Conductor 中执行操作的权限

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。管理员是指提供用户名和密码的人员。

如果 mateojackson IAM 用户尝试使用控制台查看有关 *Billing Conductor* 的详细信息，但没有 Billing Conductor:*GetWidget* 权限，则会出现以下示例错误。

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

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 `Billing Conductor:GetWidget` 操作访问 *my-example-Billing Conductor* 资源。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Billing Conductor。

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 Billing Conductor 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 Billing Conductor 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 Billing Conductor 是否支持这些功能，请参阅 如何 AWS Billing Conductor 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存取之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

在 AWS 计费指挥中记录和监控

监控是维护 AWS 账户可靠性、可用性和性能的重要组成部分。有多种工具可用于监控您的 Billing Condu AWS ctor 使用情况。

AWS 成本和使用情况报告

AWS 成本和使用情况报告会跟踪您的 AWS 使用情况，并提供与您的账户相关的估计费用。每份报告都包含您在 AWS 账户中使用的 AWS 产品、使用类型和操作的每种独特组合的行项目。您可以自定义“ AWS 成本和使用情况报告”，以按小时或按天汇总信息。

有关 AWS 成本和使用情况报告的更多信息，请参阅《成本和使用情况报告指南》。

使用记录 AWS Billing Conductor API 调用 AWS CloudTrail

AWS Billing Conductor 与一项服务集成 AWS CloudTrail，该服务提供用户、角色或 AWS 服务在 B AWS illing Conductor 中采取的操作的记录。 CloudTrail 将 AWS 计费指挥的所有 API 调用捕获为事件。捕获的调用包括来自 B AWS illing Conductor 控制台的调用和对 AWS 账单指挥器 API 操作的代码调用。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Billing Conducto AWS r 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的“事件历史记录”中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 B AWS illing Conductor 发出的请求、发出请求的 IP 地址、谁提出了请求、何时提出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail 用户指南。

AWS Billing Conductor CloudTrail 事件

本部分显示了与 Billing and Cost Management 相关 CloudTrail 的事件的完整列表。

事件名称	定义
`AssociateAccounts`	记录账号与账单组的关联。

事件名称	定义
AssociatePricingRules	记录定价规则与定价计划的关联。
AutoAssociateAccount	记录账户与账单组的自动关联。
AutoDisassociateAccount	记录在下一个账单周期内自动取消账户与账单组关联的情况。
BatchAssociateResourcesToCustomLineItem	记录资源与百分比自定义订单项的批量关联。
BatchDisassociateResourcesFromCustomLineItem	记录资源与百分比自定义订单项的批量解除关联的情况。
CreateBillingGroup	记录账单组的创建情况。
CreateCustomLineItem	记录自定义订单项的创建情况。
CreatePricingPlan	记录定价计划的创建情况。
CreatePricingRule	记录定价规则的创建情况。
DeleteBillingGroup	记录账单组的删除。
DeleteCustomLineItem	记录自定义订单项的删除情况。
DeletePricingPlan	记录定价计划的删除。

事件名称	定义
DeletePricingRule	记录定价规则的删除。
DisassociateAccounts	记录账号与账单组的取消关联情况。
DisassociatePricingRules	记录定价规则与定价计划的取消关联情况。
ListAccountAssociations	记录对账单组中账户 ID 的访问权限。
ListBillingGroupCostReports	记录对账单组实际 AWS 费用的访问权限。
ListBillingGroups	记录账单周期内对账单组的访问权限。
ListCustomLineItems	记录账单周期内对自定义订单项目的访问权限。
ListCustomLineItemVersions	记录对自定义订单项目版本的访问权限。
ListPricingPlans	记录账单周期内对定价计划的访问权限。
ListPricingPlansAssociatedWithPricingRule	记录对与定价规则关联的定价计划的访问权限。
ListPricingRules	记录账单周期内对定价规则的访问权限。
ListPricingRulesAssociatedToPricingPlan	记录对与定价计划相关的定价规则的访问权限。

事件名称	定义
ListResourcesAssociatedToCustomLineItem	记录对与自定义订单项目关联的资源的访问权限。
ListTagsForResource	记录对资源标签的访问权限。
TagResource	记录资源上标签的关联。
UpdateBillingGroup	记录账单组的更新。
UpdateCustomLineItem	记录自定义订单项的更新。
UpdatePricingPlan	记录定价计划的更新。
UpdatePricingRule	记录定价规则的更新。

AWS 账单指挥员信息位于 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 B AWS illing Conductor 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的事件 AWS 账户，包括 Billing Conduct AWS or 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有 B AWS illing Conductor 操作都由 Billing Cond AWS uctor 记录 CloudTrail 并记录在案

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅CloudTrail 用户身份元素。

了解 B AWS illing Conducto

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

主题

- AutoAssociateAccount
- CreateBillingGroup

AutoAssociateAccount

以下示例显示了演示该AutoAssociateAccount操作的 CloudTrail 日志条目。

```
{
    "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

以下示例显示了演示该CreateBillingGroup操作的 CloudTrail 日志条目。

```
{
    "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 计费控制器的合规性验证

作为多个合规计划的一部分，第三方审计师对 AWS 服务的安全性和 AWS 合规性进行评估。 AWS Billing Conductor 不在任何 AWS 合规计划的范围内。

有关特定合规计划范围内的 AWS 服务列表，请参阅按合规计划划分的 AWS 范围内的服务 AWS 按合规计划。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，请参阅在 AWS Artifact 中下载报告。

您在使用 Billing AWS Conductor 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：

- 安全性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 AWS上部署基于安全性和合规性的基准环境的步骤。
- 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。
- 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— 此 AWS 服务可全面了解您的安全状态 AWS ，帮助您检查是否符合安全行业标准和最佳实践。

AWS 计费导体的弹性

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。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失效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 计费指挥家》中的基础设施安全

作为一项托管服务 AWS Billing Conductor ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Billing Conductor。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。

配额和限制

下表描述 AWS Billing Conductor 中的配额和限制。

配额

每个付款人账户的账单组数	5,000
每个账单组的账户数量	1,000
定价方案数量	5,000
定价规则数量	50,000
可以与定价方案关联的定价规则数量	500
可以与定价规则关联的定价方案数量	1,000
自定义行项目数量	50,000
可以与百分比自定义行项目关联的源值数量	100
可以与固定自定义行项目关联的百分比自定义数量	100

限制

下表中的其他限制不能增加。

每个账单组的账单组成本和使用情况报告数量	10
账单组名称	• 必须在 128 个字符以内 • 不能包含 space • 不能包含特殊字符
账单组描述	必须在 1,024 个字符以内

定价方案名称	• 必须在 128 个字符以内 • 不能包含 space • 不能包含特殊字符
定价方案描述	必须在 1,024 个字符以内
自定义行项目名称	• 必须在 128 个字符以内 • 不能包含 space • 不能包含特殊字符

文档历史记录

下表描述了此版本的 Billing Conduct AWS or 的文档。

变更	说明	日期
已更新的文档	更新了什么是 AWS Billing Conductor？ 话题。	2024 年 3 月 7 日
更新了 AWS 托管策略的文档	已GetBillingGroupCostReport 添加到AWSBillingConductorReadOnlyAccess 策略中。有关信息，请参阅AWS 托管策略 AWS Billing Conductor。	2024年2月8日
添加了利润摘要文档	您可以按 AWS 服务 账单组查看您的保证金明细。请参阅分析每个账单组的利润。	2023 年 12 月 14 日
添加了有关自定义订单项的文档	您可以为账单组中的特定关联账户应用自定义订单项。请参阅为每个账单组创建自定义行项目。	2023 年 12 月 4 日
添加了有关主账户的文档	了解选择主账户会如何影响账单组的形式成本。请参阅了解主账户加入日期的重要性。	2023 年 10 月 26 日
增加了对自定义行项目筛选条件的支持	现在，您可以为自定义行项目指定行项目筛选条件。有关更多信息，请参阅创建百分比费用自定义行项目。	2023 年 9 月 5 日
添加了有关形式费用的文档	请参阅以下主题： • 对预计成本进行临时分析 AWS Cost Explorer	2023 年 8 月 22 日

	• AWS 服务 这支持形式成本 • IAM 策略示例：拒绝访问形式费用	
增加了对自动账户关联的支持	现在，您可以启用账单组以实现自动账户关联。有关更多信息，请参阅创建账单组、定价配置和自定义行项目。	2023 年 7 月 26 日
添加了 CSV 下载支持	现在，您可以为账单组毛利分析表下载 CSV 文件。有关更多信息，请参阅分析每个账单组的毛利。	2023 年 6 月 6 日
初始版本	Billing Con AWS ductor 用户指南和 API 参考的首次发布。	2022 年 3 月 16 日

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

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。