ユーザーガイド

AWS Billing Conductor

AWS Billing Conductor: ユーザーガイド

Table of Contents

AWS Billing Conductor とは

AWS Billing Conductor は、 AWS Marketplace チャネルパートナー (パートナー) および請求要件を満たす組織のカスタム請求サービスです。パートナーの場合、 請求は顧客が支払いを受けるための前提条件であり、 AWS アカウント または AWS Organizations 請求境界に従います。組織の場合、チャージバックアクティビティにより、組織は特定のチームのコスト (アカウントの集合など) を正しい内部予算または利益と損失 (P&L) ステートメントに割り当てることができます。

Billing Conductor では、これらのアクティビティを実現するために、2 つ目の見積もりバージョンのコストを作成して、顧客またはアカウント所有者と共有できます。見積もりコストは、Billing Conductor 内で定義された料金レートでの Billing Conductor マネージドアカウント (請求グループに割り当てられたアカウント) 内の使用量を表します (例えば、グローバル料金ルールを使用してすべての使用量にパブリック料金を適用するなど)。

> **Note**
>
> お客様は、請求対象コスト (AWS 請求書の照合) と見積もりコスト (Billing Conductor 設定の照合) のわずかな使用上の違いを 1 か月間観察します。ただし、 AWS 請求書が発行されると、使用量の値は毎月の月末に一致します。

見積もりコストを定義すると、お客様は次のユースケースのいずれかにコストを一様にモデル化できます。

1. 顧客契約。これは、 の外部でネゴシエートされたパートナーユースケースである可能性があります。 AWS
2. 内部のアカウントプラクティス、多くの場合、組織固有のユースケース

Billing Conductor の設定は、 AWS または 請求設定からの顧客の既存の請求書には影響しません (たとえば、リザーブドインスタンスや Savings Plans などのクレジットやコミットメントベースの割引の共有など)。

お客様は、以下のタスクを実行して、管理アカウントの見積もりコストを分析できます。

- Billing Conductor 内のマージン (同じアカウントセットの見積もりコストと請求対象コストの差) を分析する
- 請求詳細ページで毎月の見積りコストを表示する

- 請求グループごとに AWS Cost and Usage Report (CUR) を作成する

Billing Conductor マネージドアカウント (請求グループのアカウント) は AWS Cost Explorer、、コストと使用状況レポート、請求ダッシュボード、請求詳細ページで見積りコストを分析できます。

Billing Conductor コンソールまたは Billing Conductor API を使用して、請求グループ、料金プラン、料金設定ルール、カスタム明細項目を設定できます。

AWS Billing Conductor のサービスクォータの詳細については、「」を参照してくださいクォータと制限。

トピック

- AWS Billing Conductor の機能
- 関連サービス

AWS Billing Conductor の機能

AWS Billing Conductor の機能を使用して、以下を実行できます。

グループアカウント

見積もりコストを集計して表示するには、アカウントを請求グループに分類します。クロスサービス割引やグループごとの個別の顧客利益をシミュレート AWS 無料利用枠 します。

カスタム料金

グローバルまたは特定の割増または割引を設定し、無料利用枠へのアクセスを制御します。

料金とクレジット

1 回限りまたは定期的な固定料金またはパーセンテージベースの料金またはクレジットを請求グループに追加します。

プロフォーマ分析

請求コンソールの料金設定に基づいてコストを分析します。請求グループのアカウントは、AWS Cost Explorer で見積りコストの視覚化、予測、カスタムレポートの作成を行うことができます。プライマリアカウントは、請求グループ内のアカウントによって発生したすべてのコストのクロスアカウントビューを使用できますが、プライマリアカウント以外のアカウントには独自のコストが表示されます。

レポート作成

請求グループごとにコストと使用状況レポートを設定します。

レート分析

適用されたレートと実際の AWS レートを請求グループのマージンレポートと比較します。

関連サービス

AWS 請求コンソール

AWS 請求コンソールは、学生やスタートアップから大規模な企業まで、すべての AWS お客様向けのポータルです。コンソールを使用して、 AWS アカウントで実行されているリソースの確認、請求設定の管理、 への支払いに必要な請求アーティファクトへのアクセスを行うことができます AWS。 AWS 請求コンソールには、アカウントの支出に関する大まかな説明も表示され、AWS コスト管理製品に製品を登録するためのエントリポイントとして機能します。

詳細については、『AWS Billing ユーザーガイド』を参照してください。

AWS Cost Explorer

Cost Explorer インターフェイスを使用して、経時的な AWS コストと使用状況を視覚化、把握、管理できます。コストと使用状況データを分析するカスタムレポートを作成して、すぐに使用を開始しましょう。データを概要レベルで分析するか (例えば、すべてのアカウントの合計コストと使用量)、コストと使用量のデータをさらに詳しく分析して、傾向を特定し、コスト要因を特定して、異常を検出します。

詳細については、次のトピックを参照してください。

- での見積りコストに対するアドホック分析の実行 AWS Cost Explorer
- 「AWS Cost Management ユーザーガイド」の「AWS Cost Explorer によるコストの分析」

AWS コストと使用状況レポート

AWS コストと使用状況レポート (AWS CUR) には、利用可能なコストと使用状況データの最も包括的なセットが含まれています。コストと使用状況レポートを使用して、所有する Amazon Simple Storage Service (Amazon S3) バケットに AWS 請求レポートを発行できます。コストを時間または日単位、製品または製品リソース別、またはお客様が定義したタグ別に分類したレポートを受け取ることができます。

AWS は、バケット内のレポートをカンマ区切り値 (CSV) または Apache Parquet 形式で 1 日 1 回更新します。Microsoft Excel や Apache OpenOffice Calc などのスプレッドシートソフトウェ

アを使用してレポートを表示できます。Amazon S3 または Amazon Athena API を使用して、アプリケーションからアクセスすることもできます。

AWS コストと使用状況レポートは AWS 、使用状況を追跡し、アカウントに関連する推定請求額を提供します。各レポートには、 AWS アカウントで使用する AWS 製品、使用タイプ、およびオペレーションの一意の組み合わせごとに明細項目が含まれます。

AWS Identity and Access Management (IAM)

AWS Billing Conductor サービスは AWS Identity and Access Management (IAM) と統合されています。Billing AWS Conductor で IAM を使用すると、アカウントで作業する他のユーザーが、自分のジョブを完了するために必要なアクセス権のみを持つようにできます。

また、IAM を使用して、すべての AWS リソースへのアクセスを制御します。これには請求情報が含まれますが、それに限定されるものではありません。 AWS アカウントの構造を設定する前に、IAM の基本概念とベストプラクティスを理解しておくことが重要です。

IAM の操作方法の詳細については、「IAM ユーザーガイド」の「IAM とは」および「IAM でのセキュリティのベストプラクティス」を参照してください。

AWS Organizations （ 一括請求 ）

AWS 製品とサービスは、小規模なスタートアップからエンタープライズまで、あらゆる規模の企業に対応できます。会社が大規模な場合、または成長が見込まれる場合、会社の構造を反映する複数の AWS アカウントの設定が必要になることがあります。例えば、会社全体に 1 つのアカウントと各従業員にアカウントを持ったり、各従業員に IAM ユーザーを持つ会社全体のアカウントを持ったりすることができます。会社全体のアカウント、会社内の各部門またはチームのアカウント、各従業員のアカウントを持つことができます。

複数のアカウントを作成する場合は、 AWS Organizations の一括請求機能を使用し、すべてのメンバーアカウントを 1 つの管理アカウントにまとめて、受け取る請求書を 1 つにすることができます。詳細については、「AWS Billing ユーザーガイド」の「Organizations の一括請求 (コンソリデーティッドビリング)」を参照してください。

見積り請求データとは何ですか？

このセクションでは、 AWS Billing Conductor によって生成された見積り請求書と標準 AWS 請求書の違いを明確にします。請求グループを作成すると、 AWS Billing Conductor の計算では、カスタム料金設定を使用して、その請求グループの見積り請求が生成されます。見積り請求と標準 AWS 請求には、いくつかの基本的な違いがあります。

見積り請求データは、請求データの代替バージョンのようになります。 AWS 請求書から分離されており、毎月の実際の請求額を反映していません。また、 の外部で独自のチャージバックワークフローの一部として見積り請求書を使用することもできます AWSが、このユースケースは現在 AWS Billing Conductor ではサポートされていません。

> **Note**
>
> 見積り請求データは、標準 AWS 請求書には影響しません。お客様またはお客様の組織の による請求方法は変更されません AWS。

用語集

このセクションでは、 AWS Billing Conductor 全体で使用される主要な用語を定義し、サービスを効果的に使用できるようにします。

見積り請求書

請求グループごとに生成される請求データ。 AWS Billing Conductor の計算では、請求グループアカウントによって蓄積された使用量を取得し、請求グループの料金プランで定義されているカスタム料金を適用します。その後、請求データは、統合されたサービス にダウンストリームで提供されます。請求グループのアカウントがこれらのサービスのいずれかを通じてコストを表示すると、標準の請求データではなく見積り AWS 請求データが表示されます。

標準 AWS 請求書/請求対象 AWS 請求書

実際のコストを表す標準 AWS 請求書は、 に相当します AWS。

ドメイン

見積り請求データセットと標準 AWS 請求データセットは、別々の請求ドメインで互いに分離されています。見積りデータは見積りドメイン に存在し、標準の請求データは請求対象ドメイン に存在します。

請求対象

によって生成 AWS され、 AWS 請求書の計算の基礎として使用される請求出力。

リソース値

パーセンテージベースのカスタム明細項目の計算に使用される入力。リソース値には、請求グループの蓄積コストと、請求期間中に特定の請求グループに関連付けられている固定カスタム明細項目を含めることができます。

見積り請求データの理解

このセクションでは、見積り請求と標準請求の違いについて詳しく説明します。また、見積り請求データを使用する際のユースケースとベストプラクティスも提供します。

トピック

見積り請求データと標準 AWS 請求データの違いは何ですか？

各請求グループの見積り請求は、グループ内のアカウントが独自の一括請求ファミリーまたは組織であるかのように計算されます。その結果、見積りドメインのアカウント料金と標準の請求対象ドメインにはいくつかの主な違いがあります。

- リザーブドインスタンスと Savings Plans は、請求グループアカウントで購入した場合にのみ、請求グループ内で適用および共有されます。
- ボリューム階層化の割引は、請求グループ内のアカウントによってのみ蓄積された使用量に基づいて計算されます。

- 無料利用枠の消費量は、請求グループ内のアカウントによってのみ蓄積された使用量に基づいて計算されます。

次の明細項目タイプは、見積りドメインから除外されます。

- クレジット (支払い者または連結アカウントレベルで引き換え可能)
- サポートの料金
- 非公開割引 (ソリューションプロバイダープログラムなど)
- 使用量ベースの割引 (バンドル割引など)
- 税金

これらの要因により、請求グループのマージンは月によって異なります。

> **Note**
>
> これらの要因に加えて、料金プランと適用されたカスタム明細項目に基づいて、請求グループのマージンが負の数値になる可能性があります。

請求グループの見積りドメインでの料金の設定

料金設定ルールを作成して料金プランに関連付けることで、料金レートを調整できます。その後、その料金プランを請求グループに適用できます。マークアップまたは割引料金ルールは、パブリック AWS オンデマンド料金に対して計算されます。請求グループに空の料金プランを適用すると、料金レートはデフォルトでパブリック AWS オンデマンドレートになります。

その後、カスタム明細項目を作成して、特定の請求グループアカウントの見積り請求書にクレジットまたは料金を追加できます。

見積り請求データと標準 AWS 請求書は誰が確認できますか？

支払いアカウントは、これらの料金を AWS に支払う責任を負うため、常に標準の AWS 請求書を表示できます。また、請求ページと で請求グループの見積り請求を表示することもできます AWS Cost and Usage Report。

詳細については、「請求グループの詳細の表示」および「請求グループごとの Cost and Usage Report の設定」を参照してください。

請求グループに関連付けられているアカウントは、統合されたサービスを通じて請求の詳細を表示するときに、見積りデータを表示できます。プライマリアカウントにはクロスアカウント可視性があり、請求グループ内のすべてのアカウントの見積り請求データを表示できます。請求グループの他のアカウントは、自分のアカウントの見積り請求データを表示できます。見積りデータビューをサポートするサービスの完全なリストについては、「」を参照してくださいAWS のサービス 見積もりコストをサポートする。

見積りドメインでの無料利用枠の適用方法

12 か月間の無料利用枠

Billing Conductor は、見積り請求からこの無料利用枠を削除します。これは、特定の SKU の最初の有料オファーと交換されます。

常時無料利用枠

Billing Conductor は、見積り請求書からこの無料利用枠を削除しません。この無料利用枠を無効にするには、請求グループの料金プランに階層化料金ルールを適用します。詳細については、「料金設定ルールの作成」を参照してください。

無料トライアル

Billing Conductor は、見積りデータからほとんどの無料トライアルを削除します。ただし、既存の使用量をカバーできる後続の料金範囲データがない場合、無料トライアルを削除することはできません。

標準請求コストから見積り AWS 請求コストを導き出せますか？

標準請求のコストに基づいて、請求グループの見積り請求で生成されたコストを照合することはできません AWS 。例えば、標準 AWS 請求で請求されるプライベート割引と税金を差し引くことで、アカウントの見積りコストを導き出すことはできません。理由の詳細については、見積り請求データと標準 AWS 請求データの違いは何ですか？「」および「」を参照してください見積りドメインでの無料利用枠の適用方法。

見積りドメインには、リザーブドインスタンスと Savings Plans はどのように割り当てられますか？

リザーブドインスタンス (RI) または Savings Plans が請求グループ外のアカウントによって購入された場合、請求グループの見積り請求から完全に除外されます。RI または Savings Plans が請求グループ内のアカウントによって購入された場合、まず、購入請求グループアカウント内で発生した

対象となる使用量に特典が適用されます。残りの利点は、グループ内の他のアカウントに分配されます。

支払者レベルで行われた RI および Savings Plans の割引共有設定は、見積りドメインには影響しません。請求グループのアカウントによって購入した RI と Savings Plans は、常に同じグループのアカウントと共有されます。その結果、RI と Savings Plans の割引配分は、見積りドメインと請求対象ドメインで異なる場合があります。

請求グループは、リザーブドインスタンスと Savings Plans の割り当て方法に影響しますか？

Billing Conductor リソースとその結果の見積りデータは、実際の AWS 請求には影響しません。請求グループは、見積りドメインでの RIsと Savings Plans の適用方法に影響を与える可能性がありますが、請求対象ドメインでの同じ RIs と Savings Plans の適用方法には影響しません。

AWS Billing Conductor ダッシュボードについて

AWS Billing Conductor ダッシュボードには、カスタム料金ディメンションの影響を理解するのに役立つ主要なメトリクスの概要が表示されます。

重要業績評価指標

このセクションでは、 AWS Billing Conductor ダッシュボードで使用できる主要業績評価指標 (KPI) を定義します。KPIsです month-to-date。アカウントを作成または に追加すると AWS Organizations、アカウントはこの KPI に蓄積されます。請求グループを削除すると、その請求グループのアカウントもこの KPI に計上されます。

- 請求額 – すべての請求グループによって蓄積された使用量に対する、適用される料金プランによって定義されたカスタムレートに基づく合計請求額です。この計算では、請求グループ以外で購入したコミットメントベースの割引、非公開料金、請求対象ドメインで消費されたクレジットは考慮されません。コミットメントベースの割引の例には、リザーブドインスタンスと Savings Plans があります。
- AWS コスト – すべての請求グループによって蓄積された使用量の合計 month-to-date 料金。 AWS 請求の推定請求額に基づきます。請求対象ドメインで特典が適用された場合、計算には、請求グループ以外で購入したコミットメントベースの割引、非公開料金、従量制割引、クレジットが含まれます。コミットメントベースの割引の例には、リザーブドインスタンスと Savings Plans があります。
- マージン — すべての請求グループによって蓄積された合計 month-to-date マージン。マージンは、請求金額から AWS コストを差し引いて計算されます。マージンは、料金プラン、適用されたカスタム明細項目などの要因に基づいてマイナスになることもあります。

> **Note**
>
> 請求後の期間の調整は、マージン履歴に影響を及ぼします。詳細については、「請求グループごとのマージンの分析」を参照してください。

- 請求グループ — プライマリアカウントと関連する料金プランを持つ、相互に排他的なアカウントグループの数。
- モニタリングされているアカウント – 請求グループに現在割り当てられている一括請求ファミリー内のアカウント数。

- モニタリングされていないアカウント – 請求グループに割り当てられていない一括請求ファミリー内のアカウント数です。

請求金額あたりの上位 5 つの請求グループの表示

ビジュアルおよびテーブルビューを参照すると、収益を生み出す上位 5 つの請求グループを把握できます。既存の請求グループを管理するには、ダッシュボードページで [Manage billing groups] (請求グループの管理) を選択します。

請求グループ、料金設定、およびカスタム明細項目の作成

このセクションでは、Billing Conductor AWS で請求グループ、価格設定、カスタム明細項目を作成する方法を説明します。各セクションでは、各項目を作成した後、請求グループテーブル、料金設定ルールテーブル、およびカスタム明細項目テーブルを使用する方法についても概説します。

トピック

請求グループの作成

AWS Billing Conductor を使用して請求グループを作成し、アカウントを整理できます。デフォルトでは、管理者権限を持つ支払いアカウントが請求グループを作成できます。各請求グループは相互に排他的です。つまり、1 つのアカウントは特定の請求期間に 1 つの請求グループにのみ属することができます。請求グループのセグメンテーションはすぐに確認できますが、請求グループを作成してからグループのカスタムレートが反映されるまでに最大 24 時間かかります。

> **Note**
>
> 月の中旬に請求グループ間でアカウントを移動すると、請求期間の開始時に戻って、両方の請求グループの再計算が開始されます。月の中旬にアカウントを移動しても、以前の請求期間には影響を及ぼしません。

請求グループを作成するには、以下の手順に従います。

請求グループを作成するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/billingconductor/ AWS でビリングコンダクターを開きます。

2. ナビゲーションペインで、[Billing groups] (請求グループ) を選択します。
3. [Create billing group] (請求グループの作成) を選択します。
4. [Billing group details] (請求グループの詳細) に、請求グループの名前を入力します。命名制限については、「クォータと制限」を参照してください。
5. (オプション) [Description] (説明) に、請求グループの説明を入力します。
6. [Pricing plan] (料金プラン) で、請求グループに関連付ける料金プランを選択します。料金プランを作成するには、「料金プランの作成」を参照してください。
7. (オプション) 対象 [その他の設定]、請求グループの自動アカウント関連付けを有効にできます。

   > メモ
   >
   > - 1 つの請求グループのみ自動アカウント関連付けを行うことができます。
   > - この機能を有効にすると、組織で作成または追加されたアカウントは、自動的にこの請求グループに関連付けられます。
   > - CloudTrail 現在ログ記録がある場合は、 CloudTrail 自動アカウント関連付けをログで確認できます。

8. [Accounts] (アカウント) で、請求グループに追加するアカウントを 1 つ以上選択するか、[Import organizational unit] (組織単位をインポート) を選択して、組織単位内のアカウントを自動的に選択します。OU のインポート機能へのアクセス許可を付与するポリシーの例については、「Billing Conductor への組織単位のインポート機能に対するアクセスの付与」を参照してください。

   テーブルフィルターを使用して、アカウント名、アカウント ID、またはアカウントに関連付けられたルート E メールアドレスで並べ替えることができます。
9. プライマリアカウントは、請求グループ全体のプロフォーマコストと使用状況を確認する機能を継承し、請求グループのプロフォーマコストと使用状況レポート (AWS CUR) を生成できます。

   当月中に組織に加入したプライマリアカウントを選択した場合、その請求グループのすべてのアカウントのプロフォーマ費用には、プライマリアカウントが組織に加入してから発生した費用と使用量のみが含まれます。参加日を確認するには、[参加日を検証] を選択します。詳細については、「プライマリアカウントの参加日の重要性を理解する」を参照してください。
10. [Create billing group] (請求グループの作成) を選択します。

メモ

- ステップ 9 でプライマリアカウントを選択する必要があります。請求グループ作成後にプライマリアカウントを変更することはできません。新しいプライマリアカウントを割り当てるには、請求グループを削除してアカウントを再グループ化します。支払いアカウントは請求グループ内に含めることができますが、支払いアカウントにプライマリアカウントのロールを割り当てることはできません。
- 請求グループのプライマリアカウントが組織を離れ、その請求グループで自動アカウント関連付けが有効になっている場合は、月末までアカウントが自動的に関連付けられます。その後、請求グループは自動的に削除されます。既存の請求グループの自動アカウント関連付けを有効にすることも、別の請求グループを作成することもできます。

請求グループテーブル

請求グループを作成した後、フィルター可能なテーブルで請求グループの詳細を表示できます。以下のディメンションを使用してフィルタリングできます。

- 請求グループ名
- プライマリアカウント名
- プライマリアカウント ID
- アカウント数
- 料金プラン名

各請求グループの詳細を表示するには、テーブルで請求グループ名を選択します。自動アカウント関連付け機能を有効にした請求グループには、請求グループ名の横に[自動関連付け]アイコンが表示されます。

料金設定ルールの作成

AWS Billing Conductor で価格設定ルールを作成して、請求グループ全体の請求レートをカスタマイズできます。料金設定ルールは、グローバル、サービス固有、請求エンティティ固有、または範囲内で SKU 固有にすることができます。料金設定ルールでは、各範囲に割引または割増を適用で

きます。範囲は重複しません。異なる範囲の料金設定ルールが 1 つの料金プランに含まれている場合、範囲は最も粒度の高いものから最も低いものに適用されます。グローバル料金設定ルールでは、`Always Free Tier` レートを無効にするか有効にするかを選択することもできます。常時無料利用枠を無効にした料金設定ルールでは、その使用タイプまたはオペレーションの最初の有料利用枠がデフォルトで設定されます。デフォルトでは、管理者権限を持つ支払いアカウントが料金設定ルールを作成できます。請求グループに料金設定ルールを適用してから請求グループのカスタムレートに反映されるまで、最大で 24 時間かかります。

1 つの料金プランを複数の請求グループに適用できます。

料金設定ルールを作成するには、次の手順に従います。

料金設定ルールを作成するには

1. https://console.aws.amazon.com/billingconductor/ AWS でビリング・コンダクターを開きます。
2. ナビゲーションペインで、[Pricing configuration] (料金設定) を選択します。
3. [Pricing rules] (料金設定ルール) タブを選択します。
4. [Create pricing rules] (料金設定ルールの作成) を選択します。
5. [Pricing rule details] (料金設定ルールの詳細) に、料金設定ルールの名前を入力します。命名制限については、「クォータと制限」を参照してください。
6. (オプション) [Description] (説明) に、料金設定ルールの説明を入力します。
7. [Scope] (範囲) で、`Global`、`Service`、`Billing entity`、または `SKU` を選択します。
   - グローバル - すべての使用に適用されます。
   - サービス - 指定されたサービスにのみ適用されます。サービスを選択するときは、料金レートを設定するサービスコードを選択します。サービスを選択するときは、調整する Price List Query API からサービスコードを選択します。
   - 請求エンティティ - 任意の請求エンティティにのみ適用されます。請求主体とは AWS、その関連会社、またはサービスを販売する第三者プロバイダーが提供するサービスの販売者を指します。 AWS Marketplace
   - SKU - サービス (製品) コード、使用タイプ、オペレーションの固有の組み合わせにのみ適用されます。
8. [Type] (タイプ) で、[Discount] (割引)、[Markup] (割増) または [Tiering] (ティアリング) を選択します。

> **Note**
>
> [ティアリング] はグローバルおよびサービス向けの料金設定ルールでのみ利用できます。

9. [Percentage] (パーセンテージ) に、パーセンテージを入力します。

   パーセンテージとして **0** を入力すると、料金プランはデフォルトの AWS オンデマンド料金になります。小数点を入力すると、小数点以下 2 桁未満に四捨五入されます。

10. [Tiering] (ティアリング) タイプでは、[Tiering configuration] (ティアリングの設定) のチェックボックスをオンにして常時無料利用枠を無効にするか、有効のままにしておくことができます。常時無料利用枠は、明示的に無効にされない限り有効化されます。
11. (オプション) 同じワークフローで別の料金設定ルールを作成するには、[Add pricing rule] (料金ルールの追加) を選択します。
12. [Create pricing rule] (料金設定ルールの作成) を選択します。

料金設定ルールテーブル

料金設定ルールを作成した後、フィルター可能なテーブルで料金設定ルールの詳細を表示できます。以下のディメンションを使用して、フィルターできます。

- 料金設定ルール名
- スコープ
- タイプ
- 詳細
- Rate

料金プランの作成

AWS Billing Conductor で価格プランを作成して、請求グループ全体の請求詳細の出力をカスタマイズできます。デフォルトでは、管理者権限を持つ支払いアカウントは、料金プランを作成できます。請求グループに料金プランを適用してから請求グループのカスタムレートに反映されるまで、最大で 24 時間かかります。

1 つの料金プランを複数の請求グループに適用できます。

> **Note**
>
> 料金プランを更新すると、その料金プランが関連付けられている各請求グループの請求詳細にも影響します。料金プランが請求グループまたは請求グループのセットに関連付けられている場合、この変更は現在の請求期間にのみ影響します。以前の請求期間については、同じままです。

料金プランを作成するには、次の手順に従います。

料金プランを作成するには

1. https://console.aws.amazon.com/billingconductor/ AWS でビリングコンダクターを開きます。
2. ナビゲーションペインで、[Pricing configuration] (料金設定) を選択します。
3. [Pricing plan] (料金プラン) タブで、[Create pricing plan] (料金プランの作成) を選択します。
4. [Pricing rule details] (料金設定ルールの詳細) に、料金プランの名前を入力します。命名制限については、「クォータと制限」を参照してください。
5. (オプション) [Description] (説明) に、料金プランの説明を入力します。
6. [Pricing rules table] (料金設定ルールテーブル) で、料金プランに関連付ける料金設定ルールを選択します。料金設定ルール名、範囲、詳細、タイプ、またはレートにより料金設定ルールをフィルタリングできます。
7. [Create pricing plan] (料金プランの作成) を選択します。

料金設定ルールテーブル

料金プランを作成した後、フィルター可能なテーブルで料金プランの詳細を表示できます。以下のディメンションを使用して、フィルターできます。

- 料金プラン名
- 説明
- 料金プランに関連付けられている料金設定ルールの数

請求グループごとのカスタム明細項目の作成

AWS Billing Conductor を使用してパーソナライズした明細項目を作成し、 AWS アカウント 請求グループ内の指定項目に適用します。

カスタム品目を使用して費用と割引を割り当てることができます。カスタム明細項目は、定額料金またはパーセンテージ料金として計算できます。パーセンテージベースのカスタムラインアイテムを設定して、リソースを含めたり除外したりします。これらのリソースには、請求グループの費用や、請求期間中の請求グループに関連付けられているその他の固定カスタム項目が含まれます。その後、カスタム項目を 1 か月間適用するように設定することも、複数か月間適用するように設定することもできます。

カスタム明細項目を作成する一般的なユースケースを以下に示します (以下に限定されるわけではありません)。

- 手数料の配分 AWS Support
- 共有サービスコストの配分
- マネージドサービス料金の適用
- 税金の適用
- クレジットの割り振り
- RI と Savings Plans の削減額の割り振り (オンデマンドとは対照的)
- 組織のクレジットと割引明細項目の追加

固定料金カスタム明細項目の作成

次の手順に従って、クレジットまたは手数料の明細項目を個々の請求グループに適用する、カスタム明細項目を作成します。

カスタム明細項目を作成するには

1. https://console.aws.amazon.com/billingconductor/ AWS でビリング・コンダクターを開いてください。
2. ナビゲーションペインで、[Custom line items] (カスタム明細項目) を選択します。
3. [Create custom line item] (カスタム明細項目の作成) を選択します。
4. [Custom line item details] (カスタム明細項目の詳細) に、カスタム明細項目の名前を入力します。命名制限については、「クォータと制限」を参照してください。

5. [Description] (説明) には、カスタム明細項目の説明を入力します。上限は 255 文字です。
6. [Billing period] (請求期間) で、既存の請求期間または以前の請求期間のいずれかを選択します。
7. [Duration] (利用期間) には、「1 か月」または「継続」(終了日の指定なし) を選択します。
8. [Billing group] (請求グループ) で、任意の請求グループを選択します。カスタム請求は、一度に 1 つの請求グループにのみ関連付けることができます。

    - (オプション) 割り当て済みアカウントでは、選択した請求グループアカウントにカスタム明細項目を適用できます。カスタム明細項目は、デフォルトでは選択した請求グループのプライマリアカウントに適用されます。
9. カスタム明細項目タイプに [定額請求] を選択します。
10. 請求タイプを選択し、入力金額を入力します。

    割引明細項目にクレジットが追加されます。これにより、選択した請求グループに請求される金額が減少します。割増明細項目に料金が追加されます。これにより、選択した請求グループに請求される金額が増加します。カスタム明細項目はすべて USD 建てです。
11. [作成] を選択します。

割合料金カスタム明細項目の作成

次の手順に従って、クレジットまたは手数料の明細項目を個々の請求グループに適用する、カスタム明細項目を作成します。

カスタム明細項目を作成するには

1. https://console.aws.amazon.com/billingconductor/ AWS でビリング・コンダクターを開きます。
2. ナビゲーションペインで、[Custom line items] (カスタム明細項目) を選択します。
3. [Create custom line item] (カスタム明細項目の作成) を選択します。
4. [Custom line item details] (カスタム明細項目の詳細) に、カスタム明細項目の名前を入力します。命名制限については、「クォータと制限」を参照してください。
5. [Description] (説明) には、カスタム明細項目の説明を入力します。上限は 255 文字です。
6. [Billing period] (請求期間) で、既存の請求期間または以前の請求期間のいずれかを選択します。
7. [Duration] (利用期間) には、「1 か月」または「継続」(終了日の指定なし) を選択します。
8. [Billing group] (請求グループ) で、任意の請求グループを選択します。カスタム請求は、一度に 1 つの請求グループにのみ関連付けることができます。

- (オプション) 割り当て済みアカウントでは、選択した請求グループアカウントにカスタム明細項目を適用できます。カスタム明細項目は、デフォルトでは選択した請求グループのプライマリアカウントに適用されます。

9. カスタム品目タイプにパーセンテージチャージを選択してください。
10. 請求タイプを選択し、入力金額を入力します。

    割引明細項目にクレジットが追加されます。これにより、選択した請求グループに請求される金額が減少します。割増明細項目に料金が追加されます。これにより、選択した請求グループに請求される金額が増加します。カスタム明細項目はすべて USD 建てです。
11. (オプション) [リソース値] で、計算に含める値を選択します。デフォルトでは、請求グループの合計コストがリソースとして選択されます。これにより、すべての固定カスタム明細項目を除外します。
    - (オプション) デフォルトでは、Savings Plan の割引が含まれています。計算から除外するには、[Savings Plan 割引を除外] チェックボックスをオンにします。
12. (オプション) 固定カスタム明細項目を 1 つ以上含めます。割合ベースの計算に含める、該当する各固定カスタム明細項目を表から選択します。

    > **Note**
    >
    > リソースを関連付けずに割合のカスタム明細項目を作成できます。これらのカスタム明細項目には、請求データ内の `$0.00` 値が表示されます。

13. [作成] を選択します。

カスタム明細項目テーブル

カスタム明細項目を作成した後、フィルター可能なテーブルで明細項目の詳細を表示できます。以下のディメンションを使用して、フィルターできます。

- 明細項目名
- 明細項目の説明
- 請求金額
- 明細項目が属している請求グループ
- 明細項目の作成日

以前の請求期間中に作成されたカスタム明細項目を表示するには、[Date picker] (日付選択ツール) ドロップダウンリストを使用します。

カスタム明細項目の編集

カスタム明細項目を編集するには、次の手順を実行します。

カスタム明細項目を編集するには

1. https://console.aws.amazon.com/billingconductor/ AWS でビリング・コンダクターを開きます。
2. ナビゲーションペインで、[Custom line items] (カスタム明細項目) を選択します。
3. [Create custom line item] (カスタム明細項目の作成) を選択します。
4. 編集するカスタム明細項目を選択します。
5. [編集] を選択します。
6. 編集するパラメータを変更します。

> **Note**
>
> 請求期間、請求グループ、割り当てられたアカウント、請求タイプ (一律またはパーセンテージ)、または請求金額タイプ (クレジットまたは手数料) は変更できません。

7. [変更を保存]をクリックします。

カスタム明細項目の削除

カスタム明細項目を削除するには、次の手順を実行します。

カスタム明細項目を編集するには

1. https://console.aws.amazon.com/billingconductor/ AWS でビリング・コンダクターを開きます。
2. ナビゲーションペインで、[Custom line items] (カスタム明細項目) を選択します。
3. [Create custom line item] (カスタム明細項目の作成) を選択します。
4. 削除するカスタム明細項目を選択します。
5. [Delete] (削除) を選択します。
6. カスタム明細項目を削除するとどのような影響があるかを読んでから、[Delete custom line item] (カスタム明細項目の削除) を選択します。

AWS Billing Conductor のベストプラクティス

このセクションでは、 AWS Billing Conductor を使用する際のベストプラクティスをいくつか紹介します。

トピック

プライマリアカウントの参加日の重要性を理解する

プライマリアカウントが組織に加わった日付によって、その請求グループの見積もりコストの過去の境界が定義されます。月の途中で管理アカウントを作成またはリンクしたプライマリアカウントを選択した場合、見積もりのコストには、プライマリアカウントが参加する前に組織に含まれていたアカウントを含む、請求グループ内の他のアカウントのコストは含まれません。

例えば、10 月 15 日にプライマリアカウントが組織に参加したとします。請求グループ内のすべてのアカウントの見積もり請求には、その日付以降のコストと使用量のみが含まれます。見積り請求は、請求グループの他のアカウントが当月より前に組織のメンバーであった場合でも、10 月 15 日に開始されます。

請求グループの最初の月の請求対象ドメインと見積もり請求ドメインの間に不一致があります。見積りドメインには、10 月 15 日より前に発生した使用量は含まれません。最初の月以降の見積もりコストは、すべての使用量をキャプチャします。

請求グループの最初の請求で請求対象データと見積もりデータの間にこのような最初の不一致が発生しないようにするには、月全体またはそれ以前に管理アカウントにリンクされていたプライマリアカウントを選択します。

AWS Billing Conductor へのアクセスの制御

Billing and Cost Management には、支払人または管理アカウントにアクセスできるユーザーのみがアクセスできます。請求グループを作成し、請求情報とコスト管理コンソールで AWS Billing Conductor キーパフォーマンスインジケータ (KPIsを表示する許可を IAM ユーザーに付与するには、IAM ユーザーに以下も付与する必要があります。

- 組織内のアカウントを一覧表示

AWS Billing Conductor コンソールで請求グループと料金プランを作成できるようにする方法の詳細については、「」を参照してくださいの Identity and Access Management AWS Billing Conductor。

AWS Billing Conductor API を使用して、プログラムで AWS Billing Conductor リソースを作成することもできます。 AWS Billing Conductor API へのアクセスを設定する場合は、プログラムによるアクセスを許可するための一意の IAM ユーザーを作成することをお勧めします。これにより、組織内の誰が AWS Billing Conductor コンソールと API にアクセスできるかをより正確にアクセス制御を定義できます。Billing Conductor API へのクエリアクセスを複数の IAM AWS ユーザーに付与するには、それぞれにプログラムによるアクセスの IAM ロールを作成することをお勧めします。

AWS Billing Conductor データセットについて

AWS Billing Conductor データモデルは、標準の AWS Billing データモデルと多くの類似点を共有しますが、いくつかの違いがあります。

AWS Billing Conductor には以下は含まれません。

- クレジット (支払い者または連結アカウントレベルで引き換え可能)
- 税金
- AWS Support 料金

さらに、 AWS Billing Conductor は、スタンダード請求ドメインの共有設定に関係なく、同じ請求グループに配置されたアカウントとリザーブドインスタンスと Savings Plans を共有します。

AWS Billing Conductor の計算ロジックを理解する

AWS Billing Conductor の計算は、前期間の請求データの履歴整合性を維持しながら、特定の月に行った変更に柔軟に対応します。これは例を挙げて説明するのが一番です。

この例では、A と B の 2 つの請求グループがあります。請求グループA は、グループ内のアカウント 1 ~ 3 で請求期間を開始します。月の半ばに、支払いアカウントは Account 3 を Billing Group B に移動します。その時点で、請求グループ A および B のコストを再計算して、最新の変更を正確にモデル化する必要があります。Account 3 が移動されると、Billing Group A の使用状況は、Account 3 が現在の請求期間中に請求グループに含まれていなかったかのようにモデル化されます。さらに、Billing Group B の使用量は、請求期間の開始時から Account 3 が Billing Group B の一部で使用されたかのようにモデル化されます。このアプローチにより、請求期間内にアカウントがグループ間で移動した場合に、複雑なレートやチャージバックモデルを計算する必要がなくなります。

請求グループ A	日数: 1 ~ 15	日数: 16 ~ 30	月末
アカウント 1	100 USD	100 USD	200 USD
アカウント 2	100 USD	100 USD	200 USD
アカウント 3	100 USD	該当なし	該当なし
合計	300 USD	200 USD	400 USD

請求グループ B	日数: 1 ~ 15	日数: 16 ~ 30	月末
アカウント 4	100 USD	100 USD	200 USD
アカウント 5	100 USD	100 USD	200 USD
アカウント 6	100 USD	100 USD	200 USD
アカウント 3	100 USD	100 USD	200 USD
合計	400 USD	400 USD	800 USD

AWS Billing Conductor の更新頻度について

AWS 請求データは少なくとも 1 日 1 回更新されます。 AWS Billing Conductor はこのデータを使用して見積り請求データを計算します。当月に適用するように生成されたカスタム明細項目は、24 時間以内に反映されます。前の請求期間に適用するために生成されたカスタム明細項目が請求グループ

の AWS コストと使用状況レポートに反映されるまで、または特定の請求グループの請求ページに反映されるまでに最大 48 時間かかる場合があります。

AWS Billing Conductor AWS CUR と標準 AWS CUR の違いを理解する

AWS Billing Conductor 設定を使用して作成された標準コストと使用状況レポートと見積もり AWS CUR には、いくつかの違いがあります。

- 標準 AWS CUR は、一括請求ファミリーの各アカウントのコストと使用量を計算します。請求グループあたりの見積もり AWS CUR には、計算時の請求グループ内のアカウントのみが含まれます。
- 標準 AWS CUR は請求書列に一度入力すると、請求書は によって生成されます AWS。見積もり AWS CUR は請求書列にデータを入力しません。現在、見積り請求データ AWS に基づいて によって請求書が生成されたり発行されたりすることはありません。

請求グループごとのマージンの分析

AWS Billing Conductor のマージン概要とマージン詳細を使用して、マージンを集計または特定の請求グループのマージンを分析できます。

個々の請求グループまたは一連の請求グループのマージンを表示するには、次の手順に従います。

トピック

マージン概要を使用してマージンを集計して表示できます。

請求グループのマージンの概要を表示するには

1. https://console.aws.amazon.com/billingconductor/ AWS でビリングコンダクターを開きます。
2. ナビゲーションペインの「分析」で、「マージンサマリー」を選択します。
3. レポートタイプには、[すべての請求グループ] または [請求グループの選択] を選択します。
4. [請求グループを選択] を選択した場合は、請求期間と 1 つ以上の請求グループを選択します。
5. M onth-to-date 概要セクションでは、請求金額、AWS 費用、マージンを確認できます。
6. マージン分析は次の 2 つの方法で表示できます。
   - 「パフォーマンス (過去 13 か月まで)」セクションの棒グラフとして表示。
   - マージン分析表の表として使用。

   マイナスのマージンは、グラフで赤色で表示され、マイナス金額とマイナスのパーセンテージが示されます。

マージン分析表を理解する

請求グループのマージン分析テーブルは、デフォルトで逆の時系列でソートされます。次の項目を含むすべての列でテーブルを並べ替えることができます。

- 月
- 請求金額

- AWS コスト
- マージンの金額
- マージンのパーセント

グラフとテーブルは、選択した請求グループの過去 13 か月間の値を返します。請求グループが異なる時間に作成された場合は、選択された最も古い請求グループの時間範囲を前提としています。

マージン分析テーブルをダウンロード可能な CSV ファイルにエクスポートできます。マージン分析テーブルの横にある [CSV をダウンロード]を選択します。ダウンロードが自動的に開始します。

> **Note**
>
> 請求グループのマージン分析を含む CSV ファイルをダウンロードするには、IAM ポリシーに `billingconductor:ListBillingGroupCostReport` アクセス許可を追加する必要があります。

AWS のサービス マージンの詳細を使用してマージンを確認する

請求グループのサービスごとのマージンを確認するには

1. https://console.aws.amazon.com/billingconductor/ AWS でビリング・コンダクターを開きます。
2. ナビゲーションペインの「分析」で、「マージンの詳細」を選択します。
3. [レポートパラメータ] で、請求期間と請求グループを選択します。
4. マージン分析は次の 2 つの方法で表示できます。
   - 「上位 5 つのサービス別のマージントレンド」セクションの折れ線グラフとして表示。
   - マージン分析表の表として。

マージントレンドチャートを理解する

マージンの詳細には、選択した請求期間におけるマージン別の上位 5 つのサービスを示す折れ線グラフが表示されます。折れ線グラフには、比較できるように、過去 3 か月間の各サービスのマージンが表示されます。

グラフには、選択した請求期間における各サービスのマージンを示す表も含まれています。この表には、過去 3 か月間に計算された平均マージンが表示されます。これには以下の列が含まれます。

- サービス名
- [Average] (平均)
- マージン

請求グループが過去 3 か月間ずっとアクティブではなかった場合、グラフには利用可能なコストレポートデータのみが表示されます。

マージン分析表を理解する

請求グループのマージン分析表には以下の列があります。

- サービス名
- 請求金額
- AWS 費用
- マージンの金額
- マージンのパーセント

マージン分析テーブルをダウンロード可能な CSV ファイルにエクスポートできます。マージン分析テーブルの横にある [CSV をダウンロード]を選択します。ダウンロードが自動的に開始します。

> **Note**
>
> 請求グループのマージン分析を含む CSV ファイルをダウンロードするには、IAM ポリシーに `billingconductor:GetBillingGroupCostReport` アクセス許可を追加する必要があります。

請求グループの詳細の表示

請求グループの詳細を使用して、AWS Billing Conductor で請求グループを監視、分析、編集できます。請求グループの詳細では、過去 1 か月のマージン分析、適用されたカスタム明細項目の履歴、および必要に応じて請求グループを編集および削除する機能が提供されます。

カスタム価格ディメンションによる請求詳細の表示

請求グループと料金プランを作成して割り当てた後、管理下にある各請求グループの使用タイプの詳細度で、カスタム請求ディメンションを表示できます。

次の手順に従って、見積もりドメインでの請求の詳細を表示します。

見積もりの請求詳細を表示するには

1. AWS Billing コンソール https://console.aws.amazon.com/billing/ を開きます。
2. ナビゲーションペインで [Bills (請求書)] を選択します。
3. [billing details] (請求の詳細) の右上隅にある [Settings] (設定) を選択します。
4. [Pro forma data view] (見積もりデータビュー) を有効にします。
5. [Billing group] (請求グループ) で、分析する請求を選択します。

サービスと AWS リージョンごとに請求グループの使用量を分析し、AWS Billing Conductor で定義されたレートと一致する、その使用のコストを確認できます。

カスタム明細項目は、[請求の詳細] ページのサービス AWS Billing Conductor の下にあります。

請求グループごとの Cost and Usage Report の設定

作成する請求グループごとに、プロフォーマ AWS コストと使用状況レポート (AWS CUR) を作成できます。プロフォーマAWS CUR には、標準 AWS CUR と同じファイル形式、詳細度、および列が使用されており、所定の期間に使用可能なコストと使用状況データの最も包括的なセットが含まれています。

プロフォーマ AWS CUR は、所有している Amazon Simple Storage Service (Amazon S3) バケットに公開できます。

AWS では、お客様のバケットのレポートを CSV (カンマ区切り値) 形式、または Apache Parquet 形式で 1 日 1 回更新します。Microsoft Excel や Apache OpenOffice Calc などのスプレッドシートソフトウェアを使用してレポートを表示できます。Amazon S3 または Amazon Athena API を使用して、アプリケーションからアクセスすることもできます。標準 AWS の詳細については、AWS コストと使用状況レポートユーザーガイドを参照してください。

次の手順を使用して、請求グループのプロフォーマ AWS CUR を生成します。

請求グループの見積もりの Cost and Usage Report を作成するには

1. AWS Billing コンソール https://console.aws.amazon.com/billing/ を開きます。
2. ナビゲーションペインで、[Cost & Usage Reports] (コストと使用状況レポート) を選択します。
3. [report table] (レポートテーブル) の右上にある [Settings] (設定) を選択します。
4. [Pro forma] (見積もり) データビューを有効にします。
5. [Enable] (有効化) を選択します。
6. [Create report (レポートを作成)] を選択します。
7. [レポート名] に、レポートの名前を入力します。
8. [Data view] (データビュー) で、[pro forma] (見積もり) を選択します。
9. [Billing group] (請求グループ) で、任意の請求グループを選択します。
10. [Additional report details] で、[Include resource IDs] を選択して各リソースの ID をレポートに含めます。
11. [データ更新設定] で、請求書を確定した後、コストと使用状況データの新しい変更でAWS コストと使用状況レポートを更新するかどうかを選択します。レポートが更新されると、新しいレポートが Amazon S3 にアップロードされます。

> **Note**
>
> 請求グループのコストと使用状況レポートには、クレジット、税金、またはサポート料金は含まれていません。

12. [Next] (次へ) をクリックします。
13. [S3 バケット] で、[設定] を選択します。
14. [S3 バケットの設定] ダイアログボックスで、次のいずれかを実行します。
    - ドロップダウンリストから既存のバケットを選択し、[Next] (次へ) を選択します。
    - バケット名と、新しいバケットを作成する AWS リージョンを入力し、[Next] (次へ) を選択します。
15. [I have confirmed that this policy is correct] (このポリシーが正しいことを確認しました) を選択した後、[Save] (保存) を選択します。
16. [Report path prefix (レポートパスのプレフィックス)] に、レポート名に付加するレポートパスのプレフィックスを入力します。

    この手順は Amazon Redshift または Amazon QuickSight ではオプションですが、Amazon Athena では必須です。

    プレフィックスを指定しない場合、既定のプレフィックスは、ステップ 4 でレポートに指定した名前とレポートの日付範囲です。形式は次のとおりです。

    ```
    /report-name/date-range/
    ```
17. [Time granularity] で、次のいずれかを選択します。
    - Hourly: レポートの明細項目を 1 時間ごとに集計する場合に選択します。
    - Daily: レポートの明細項目を 1 日ごとに集計する場合に選択します。
18. [Report versioning (レポートバージョニング)] で、レポートの各バージョンでレポートの以前のバージョンを上書きするのか、以前のバージョンに加えて配信するのかを選択します。
19. [Enable report data integration for] (レポートデータ統合の有効化) で、Cost and Usage Report を Amazon Athena、Amazon Redshift、または Amazon QuickSight にアップロードできるようにするかを選択します。レポートは、以下の形式で圧縮されています。
    - Athena: parquet 圧縮
    - Amazon Redshift または Amazon QuickSight: .gz 圧縮

20. [Next] (次へ) をクリックします。
21. レポートの設定を確認したら、[Review and Complete] (確認して完了) を選択します。

での見積りコストに対するアドホック分析の実行 AWS Cost Explorer

AWS アカウント Billing Conductor 請求グループの は、Cost Explorer で見積りコストを分析、予測、レポートできます。請求グループのプライマリアカウントは、グループ内のすべてのアカウントのためにこれらのアクティビティを実行できます。を使用している場合AWS Organizations、管理アカウントは Cost Explorer で見積りコストを分析、予測、またはレポートできません。

請求グループ管理アカウント (請求グループメンバー) は、請求グループのメンバーであった請求期間のコストと使用状況データを表示でき、見積もりデータを使用できます。請求対象のコストと使用状況の履歴データを表示することはできません。

> メモ
>
> - Billing Conductor マネージドアカウント (請求グループメンバー) は、Cost Explorer で見積もりコストを確認できます。
> - 時間単位の粒度データは、Cost Explorer では見積もりコストをサポートしていません。
> - Cost Explorer がサポートするコアワークフローの詳細については、「AWS Cost Management ユーザーガイド」の「Cost Explorer を使用してデータを探索する」を参照してください。

見積もりコストAWS のサービスをサポートする のリストについては、「」を参照してくださいAWS のサービス 見積もりコストをサポートする。

AWS のサービス 見積もりコストをサポートする

次の クラウド財務管理サービスとその機能は、見積もりコストをサポートします。

サービスと特徴	AWS アカウント タイプ別のサポートレベル		
	支払者 (管理アカウント)	プライマリアカウント	リンク済み (メンバーアカウント)
AWS Cost and Usage Report	はい	はい	はい
分割コストの配分	いいえ	いいえ	いいえ
AWS Billing	いいえ	はい	はい
ダッシュボード	いいえ	はい	はい
請求の詳細	はい	はい	はい
CSV をダウンロードする	いいえ	いいえ	いいえ
AWS Cost Explorer	いいえ	はい	はい
予測	いいえ	はい	はい
レポートを保存する	いいえ	はい	はい
適切なサイズ設定に関する推奨事項	いいえ	いいえ	いいえ
コスト異常モニター	いいえ	いいえ	いいえ
Savings Plans に関する推奨事項	いいえ	いいえ	いいえ
Savings Plans 使用状況レポート	いいえ	いいえ	いいえ

サービスと特徴	AWS アカウント タイプ別のサポートレベル		
Savings Plans カバレッジレポート	いいえ	いいえ	いいえ
予約のレコメンデーション	いいえ	いいえ	いいえ
予約の使用状況レポート	いいえ	いいえ	いいえ
予約カバレッジレポート	いいえ	いいえ	いいえ
AWS Budgets	いいえ	いいえ	いいえ
予算レポート	いいえ	いいえ	いいえ

見積もりコストをサポートしていないサービスや機能については、 AWS 請求書と一致する請求可能な料金でコスト AWS アカウント を確認できます。

関連情報

請求可能な返金、クレジット、割引に対するリンクされたアカウントのアクセスを管理するには、コスト管理コンソールの [詳細設定] ページの [AWS Cost Explorer] セクションを参照してください。

これらのサービスや機能に関する特定の請求可能な料金を IAM エンティティに表示したくない場合は、IAM ポリシーを使用してアクセスを拒否できます。IAM ポリシーの例については、「Billing and Cost Explorer による、見積りコストをサポートしていないサービスや機能へのアクセスを拒否する」を参照してください。

IAM ポリシーをカスタマイズして、特定の許可を付与または拒否することもできます。Billing and Cost Management の IAM アクションの詳細なリストについては、次のトピックを参照してください。

- 「AWS Cost Management ユーザーガイド」の「AWS Cost Management のアクセスコントロールの移行」
- 「AWS Billing のアクセスコントロールの移行」および「AWS Billing ユーザーガイド」

AWS Billing Conductor API を使用する場合

Billing Conductor API は、Java、Python、.NET、Go で利用できます。Billing Conductor でリリースされた新機能は API としても利用できます。

AWS Billing Conductor API の詳細については、「AWS Billing Conductor API リファレンス」を参照してください。

AWS Billing Conductor のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルではこれを、クラウドのセキュリティ、およびクラウド内でのセキュリティと説明しています:

- クラウドのセキュリティ — AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する責任 AWS を担います。 AWS また、 では、安全に使用できるサービスも提供しています。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。 AWS Billing Conductor に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」「コンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 AWS Billing Conductor を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために AWS Billing Conductor を設定する方法を示します。また、 AWS Billing Conductor リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

- AWS Billing Conductor でのデータ保護
- の Identity and Access Management AWS Billing Conductor
- AWS Billing Conductor でのログ記録とモニタリング
- AWS Billing Conductor のコンプライアンス検証
- AWS Billing Conductor の耐障害性
- AWS Billing Conductor のインフラストラクチャセキュリティ

AWS Billing Conductor でのデータ保護

責任 AWS 共有モデル、 AWS Billing Conductor でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された記事「AWS 責任共有モデルおよび GDPR」を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- を使用して API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、または SDK を使用して AWS Billing Conductor AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

の Identity and Access Management AWS Billing Conductor

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、Billing Conductor リソースの使用について、誰を認証し (サインインを許可し)、誰を認可するか (許可を付与するか) を管理します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、Billing Conductor で行う作業によって異なります。

サービスユーザー – 業務遂行に Billing Conductor サービスを使用する場合、管理者から必要な認証情報と許可が提供されます。業務遂行のためにより多くの Billing Conductor 機能を使用するにつれて、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。 Billing Conductor の機能にアクセスできない場合は、「AWS Billing Conductor ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 – Billing Conductor リソースの社内担当者には、Billing Conductor に対するフルアクセスが付与されているはずです。サービスユーザーがどの Billing Conductor 機能やリソースにアクセスするかを決定するのは、管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。企業が Billing Conductor で IAM を使用する方法の詳細については、「が IAM と AWS Billing Conductor 連携する方法」を参照してください。

IAM 管理者 – お客様が IAM 管理者である場合は、Billing Conductor へのアクセスを管理するポリシーの作成方法の詳細について理解しておくことをお勧めします。IAM で使用できる Billing Conductor のアイデンティティベースのポリシー例を確認するには、「AWS Billing Conductor アイデンティティベースのポリシーの例」を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、『AWS IAM Identity Center ユーザーガイド』の「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」を参照してください。

AWS アカウントのルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強く

お勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドの「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する権限を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、『IAM ユーザーガイド』の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティ

が認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、『IAM ユーザーガイド』の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、『IAM ユーザーガイド』の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、『Amazon Simple Storage Service デベロッパーガイド』の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

が IAM と AWS Billing Conductor 連携する方法

Billing Conductor へのアクセスを管理するために IAM を使用する前に、 Billing Conductor で使用できる IAM 機能を理解しておく必要があります。Billing Conductor およびその他の AWS のサービスが IAM と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

トピック

- Billing Conductor のアイデンティティベースのポリシー
- Billing Conductor のリソースベースのポリシー
- アクセスコントロールリスト (ACL)
- Billing Conductor タグに基づく承認
- Billing Conductor の IAM ロール

Billing Conductor のアイデンティティベースのポリシー

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、アクションを許可または拒否する条件を指定できます。Billing Conductor は、特定のアクション、リソース、条件キーをサポートしています。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

アクション

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーのAction要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

Billing Conductor のポリシーアクションは、アクション `Billing Conductor:` の前に次のプレフィックスを使用します。たとえば、 Amazon EC2 `RunInstances` API オペレーションで Amazon EC2 インスタンスを実行するためのアクセス許可をユーザーに付与するには、ポリシー

に ec2:RunInstances アクションを含めます。ポリシーステートメントには、Action または NotAction エレメントを含める必要があります。Billing Conductor は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一ステートメントに複数アクションを指定するには、次のようにカンマで区切ります:

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

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、Describe という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

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

Billing Conductor アクションのリストを確認するには、「IAM ユーザーガイド」の AWS 「 Billing Conductor で定義されるアクション」を参照してください。

リソース

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

Amazon EC2 インスタンスのリソースには次のような ARN があります:

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

ARN の形式の詳細については、「Amazon リソースネーム (ARNs AWS 「サービス名前空間」を参照してください。

例えば、ステートメントで i-1234567890abcdef0 インスタンスを指定するには、次の ARN を使用します。

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

特定のアカウントに属するすべてのインスタンスを指定するには、ワイルドカード (*) を使用します。

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

リソースを作成するためのアクションなど、一部の Billing Conductor は特定のリソースでは実行できません。このような場合は、ワイルドカード *を使用する必要があります。

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

Amazon EC2 API アクションの多くが複数のリソースと関連します。例えば、AttachVolume では Amazon EBS ボリュームをインスタンスにアタッチするため、IAM ユーザーはボリュームおよびインスタンスを使用する権限が必要です。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

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

Billing Conductor リソースタイプとその ARNsAWS 「 Billing Conductor で定義されるリソース」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、AWS 「 Billing Conductor で定義されるアクション」を参照してください。

条件キー

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

Billing Conductor は独自の条件キーのセットを定義し、一部のグローバル条件キーの使用をサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイドAWS 」の「グローバル条件コンテキストキー」を参照してください。

すべての Amazon EC2 アクションは、aws:RequestedRegion および ec2:Region 条件キーをサポートします。詳細については、「例: 特定のリージョンへのアクセスの制限」を参照してください。

Billing Conductor の条件キーのリストを確認するには、「IAM ユーザーガイド」のAWS 「 Billing Conductor の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、AWS 「 Billing Conductor で定義されるアクション」を参照してください。

例

Billing Conductor のアイデンティティベースのポリシー例を確認するには、「AWS Billing Conductor アイデンティティベースのポリシーの例」を参照してください。

Billing Conductor のリソースベースのポリシー

リソースベースのポリシーとは、指定されたプリンシパルが Billing Conductor リソースに対して、実行できるアクションとその条件を指定する JSON ポリシードキュメントです。Amazon S3 は、Amazon S3 ####に関するリソースベースのアクセス許可ポリシーをサポートします。リソースベースのポリシーでは、リソースごとに他の アカウントに使用許可を付与することができます。リ

ソースベースのポリシーを使用して、 AWS サービスが Amazon S3 #### にアクセスすることを許可することもできます。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる AWS アカウントにある場合は、プリンシパルエンティティにリソースへのアクセス許可も付与する必要があります。アクセス許可は、アイデンティティベースのポリシーをエンティティにアタッチすることで付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、ID ベースのポリシーをさらに付与する必要はありません。詳細については、IAM ユーザーガイドの「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Amazon S3 サービスは、####ポリシーと呼ばれるリソースベースのポリシーの 1 つのタイプのみサポートし、それが####にアタッチされます。このポリシーは、 *Billing Conductor* に対してアクションを実行できるプリンシパルエンティティ (アカウント、ユーザー、ロール、フェデレーションユーザー) を定義します。

例

Billing Conductor のリソースベースのポリシー例を確認するには、「AWS Billing Conductor リソースベースのポリシーの例」を参照してください。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、リソースにアタッチできる被付与者のリストです。これらは、アタッチされているリソースにアクセスするための権限をアカウントに付与します。Amazon S3 ####リソースに ACL をアタッチできます。

Amazon S3 アクセスコントロールリスト (ACL) を使用すると、####リソースへのアクセスを管理できます。各####には、サブリソースとして ACL がアタッチされています。どの AWS アカウント、IAM ユーザーまたはユーザーのグループ、または IAM ロールにアクセス権が付与されているか、およびアクセス権のタイプを定義します。リソースのリクエストを受信すると、 は対応する ACL AWS をチェックして、リクエスタに必要なアクセス許可があることを確認します。

####リソースを作成すると、Amazon S3 は、リソースに対する完全なコントロールをリソース所有者に付与するデフォルト ACL を作成します。次の####の ACL 例では、John Doe が####の所有者として表示され、その####に対する完全な制御が許可されています。1 つの ACL には最大 100 個の許可を指定することができます。

```
<?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 の ID フィールドは、 AWS アカウントの正規ユーザー ID です。所有しているアカウントでこの ID を表示する方法については、AWS 「アカウント正規ユーザー ID の検索」を参照してください。

Billing Conductor タグに基づく承認

Billing Conductor リソースにタグをアタッチしたり、 Billing Conductor へのリクエストでタグを渡したりすることができます。タグに基づいてアクセスを管理するには、`Billing Conductor:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの 条件要素でタグ情報を提供します。

Billing Conductor の IAM ロール

IAM ロールは、特定のアクセス許可を持つ AWS アカウント内のエンティティです。

Billing Conductor での一時的な認証情報の使用

一時的な認証情報を使用して、フェデレーションでサインインする、IAM ロールを引き受ける、またはクロスアカウントロールを引き受けることができます。一時的なセキュリティ認証情報を取得するには、 AssumeRoleやGetFederationトークン などの AWS STS API オペレーションを呼び出します。

Billing Conductor では、一時的な認証情報の使用がサポートされています。

サービスリンクロール

サービスにリンクされたロールを使用すると、 AWS サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。サービスリンクロールは IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

サービスロール

この機能により、ユーザーに代わってサービスがサービスロールを引き受けることが許可されます。このロールにより、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービスロールは、IAM アカウントに表示され、アカウントによって所有されます。つまり、IAM 管理者は、このロールの権限を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

Billing Conductor では、サービスロールがサポートされています。

Billing Conductor での IAM ロールの選択

Billing Conductor でリソースを作成する場合、 Billing Conductor ユーザーに代わって Amazon EC2 にアクセスすることを許可するロールを選択します。サービスロールまたはサービスにリンクされたロールを以前に作成している場合、 Billing Conductor は選択できるロールのリストを表示します。Amazon EC2 インスタンスの起動と停止のためのアクセスを、許可するロールを選択することが重要です。

AWS Billing Conductor アイデンティティベースのポリシーの例

デフォルトでは、IAM ユーザーおよびロールには、 Billing Conductor リソースを作成または変更するアクセス許可はありません。また、、 AWS Management Console AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

トピック

ポリシーのベストプラクティス

アイデンティティベースのポリシーは、アカウントで Billing Conductor アカウントの作成、アクセス、削除を行えるユーザーを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイドの「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権権限とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、IAM ユーザーガイドの [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、『IAM ユーザーガイド』の「IAM でのセキュリティのベストプラクティス」を参照してください。

Billing Conductor アイデンティティベースのポリシーの例

このトピックには、アカウント情報とツールへのアクセスを管理するために IAM ユーザーまたはグループにアタッチできるポリシー例が含まれています。

トピック

- Billing Conductor コンソールに対するフルアクセスの許可
- Billing Conductor API へのフルアクセスの許可
- Billing Conductor コンソールへの読み取り専用アクセス許可の付与
- 請求コンソールにより Billing Conductor にアクセス許可を付与する
- AWS コストと使用状況レポートによる Billing Conductor アクセスの付与
- Billing Conductor への組織単位のインポート機能に対するアクセスの付与
- Billing and Cost Explorer による、見積りコストをサポートしていないサービスや機能へのアクセスを拒否する

Billing Conductor コンソールに対するフルアクセスの許可

Billing Conductor コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらの許可により、 AWS アカウント の Billing Conductor コンソールリソースの一覧と詳細を表示できます。最小限必要な許可よりも厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (IAM ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

これらのエンティティが Billing Conductor コンソールを引き続き使用できるようにするには、エンティティに次の AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへの許可の追加」を参照してください。

料金設定ルールの作成には、`billingconductor:*` のアクセス許可に加えて `pricing:DescribeServices` が必要で、支払いアカウントにリンクされている連結アカウントを一覧表示するには、`organizations:ListAccounts` が必要です。

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

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

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

Billing Conductor API へのフルアクセスの許可

この例では、IAM エンティティに Billing Conductor API へのフルアクセスを付与します。

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

```
}
```

Billing Conductor コンソールへの読み取り専用アクセス許可の付与

この例では、IAM エンティティに Billing Conductor コンソールへの読み取り専用アクセスを付与します。

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

請求コンソールにより Billing Conductor にアクセス許可を付与する

この例では、IAM エンティティは、請求コンソールの請求ページから見積り請求データを切り替えて表示できます。

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

```
        }
    ]
}
```

AWS コストと使用状況レポートによる Billing Conductor アクセスの付与

この例では、IAM エンティティは、請求コンソールのコストと使用状況レポートページから見積り請求データを切り替えて表示できます。

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

Billing Conductor への組織単位のインポート機能に対するアクセスの付与

この例では、請求グループの作成時に組織単位 (OU) アカウントをインポートするために必要な特定の AWS Organizations API オペレーションへの読み取り専用アクセス権が IAM エンティティに付与されます。OU のインポート機能は Billing AWS Conductor コンソールにあります。

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

```
    ]
}
```

Billing and Cost Explorer による、見積りコストをサポートしていないサービスや機能へのアクセスを拒否する

この例では、IAM エンティティは、見積りコストをサポートしていない のサービスや機能へのアクセスを拒否されます。このポリシーには、管理アカウントおよび個々のメンバーアカウント内で実行できるアクションのリストが含まれています。

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

詳細については、「AWS のサービス 見積もりコストをサポートする」を参照してください。

AWSAWS Billing Conductor の マネージドポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを記述するよりも、AWS 管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに開始するには、 AWS マネージドポリシーを使用できます。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、「IAM ユーザーガイド」の「 AWS 管理ポリシー」を参照してください。

AWS サービスは、 AWS マネージドポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。サービスでは、新しい機能を利用できるようにするために、 AWS マ

ネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が中断されることはありません。

さらに、 は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートします。例えば、 ReadOnlyアクセス AWS 管理ポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、 は新しいオペレーションとリソースの読み取り専用アクセス許可 AWS を追加します。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

AWS マネージドポリシー： AWSBillingConductorFullAccess

AWSBillingConductorFullAccess 管理ポリシーは、 AWS Billing Conductor コンソールと APIs。ユーザーは Billing Conductor AWS リソースを一覧表示、作成、削除できます。

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

AWS マネージドポリシー： AWSBillingConductorReadOnlyAccess

AWSBillingConductorReadOnlyAccess 管理ポリシーは、 AWS Billing Conductor コンソールと APIs への読み取り専用アクセスを許可します。ユーザーは、すべての AWS Billing Conductor リソースを表示および一覧表示できます。ユーザーがリソースを作成または削除することはできません。

```
{
```

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

AWS Billing Conductor の AWS マネージドポリシーの更新

AWS Billing Conductor の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更に関する自動通知については、 AWS Billing Conductor ドキュメント履歴ページの RSS フィードを購読してください。

変更	説明	日付
AWSBillingConductorReadOnlyAccess	をAWSBillingConductorReadOnlyAccess ポリシーGetBillingGroupCostReport に追加しました。	2024 年 2 月 8 日
AWSBillingConductorFullAccess	作成されるポリシー	2022 年 3 月 29 日
AWSBillingConductorReadOnlyAccess	作成されるポリシー	2022 年 3 月 29 日
AWS Billing Conductor の変更ログが公開されました	AWS Billing Conductor が AWS マネージドポリシーの変更の追跡を開始しました。	2022 年 3 月 29 日

AWS Billing Conductor リソースベースのポリシーの例

トピック

特定の IP アドレスへの Amazon S3 バケットアクセスの制限

次の例は、指定したバケット内のオブジェクトに対して任意の Amazon S3 オペレーションを実行するためのアクセス許可をユーザーに付与します。ただし、リクエストは条件で指定された IP アドレス範囲からのリクエストである必要があります。

このステートメントの条件では、54.240.143.* の範囲のインターネットプロトコルバージョン 4 (IPv4) IP アドレスが許可されています。ただし、54.240.143.188 を除きます。

Condition ブロックは、 IpAddressNotIpAddress条件と aws:SourceIp条件キーを使用します。これは、 AWS 幅広い条件キーです。これらの条件キーの詳細については、「ポリシーでの条件の指定」を参照してください。aws:sourceIpIPv4 値は標準の CIDR 表記を使用します。詳細については、IAM ユーザーガイドの IP アドレス条件演算子 を参照してください。

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

AWS Billing Conductor ID とアクセスのトラブルシューティング

次の情報は、 Billing Conductor と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Billing Conductor でアクションを実行する権限がない
- iam を実行する権限がありません。PassRole
- AWS アカウント外のユーザーに Billing Conductor リソースへのアクセスを許可したい

Billing Conductor でアクションを実行する権限がない

からアクションを実行する権限がないと AWS Management Console 通知された場合は、管理者に連絡してサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

次の例のエラーは、mateojackson IAM ユーザーがコンソールを使用して *Billing Conductor* の詳細を表示しようとしているとき、Billing Conductor:*GetWidget* のアクセス許可がない場合に発生します。

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

この場合、Mateo は、Billing Conductor:*GetWidget* アクションを使用して *my-example-Billing Conductor* リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行することを認可されていないというエラーが表示された場合は、ポリシーを更新して Billing Conductor にロールを渡せるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次のエラー例は、marymajor という名前の IAM ユーザーがコンソールを使用して、Billing Conductor でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが

実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

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

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

AWS アカウント外のユーザーに Billing Conductor リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Billing Conductor がこれらの機能をサポートするかどうかについては、「が IAM と AWS Billing Conductor 連携する方法」を参照してください。
- 所有している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの AWS アカウント「所有している別の の IAM ユーザーへのアクセスを提供する」を参照してください。AWS アカウント
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「外部で認証されたユーザー (ID フェデレーション) へのアクセス権限」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

AWS Billing Conductor でのログ記録とモニタリング

モニタリングは、 AWS アカウントの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS Billing Conductor の使用状況をモニタリングするためのツールがいくつかあります。

AWS コストと使用状況レポート

AWS コストと使用状況レポートは、 AWS 使用状況を追跡し、アカウントに関連する推定請求額を提供します。各レポートには、 AWS アカウントで使用する AWS 製品、使用タイプ、オペレーションの一意の組み合わせごとに明細項目が含まれます。 AWS コストと使用状況レポートをカスタマイズして、情報を時間単位または日単位で集計できます。

AWS コストと使用状況レポートの詳細については、「 コストと使用状況レポートガイド」を参照してください。

を使用した AWS Billing Conductor API コールのログ記録 AWS CloudTrail

AWS Billing Conductor は、ユーザー AWS CloudTrail、ロール、または Billing Conductor の サービスによって実行されたアクションを記録する AWS サービスである と統合されています。 AWS は、Billing Conductor のすべての API AWS コールをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、 AWS Billing Conductor コンソールからの呼び出しと、 AWS Billing Conductor API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、AWS Billing Conductor の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、 AWS Billing Conductor に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

AWS Billing Conductor CloudTrail イベント

このセクションでは、請求情報とコスト管理に関連する CloudTrail イベントの完全なリストを示します。

イベント名	定義
`AssociateAccounts`	アカウントの請求グループへの関連付けを記録します。

イベント名	定義
AssociatePricingRules	料金設定ルールと料金プランの関連付けを記録します。
AutoAssociateAccount	アカウントと請求グループの自動関連付けを記録します。
AutoDisassociateAccount	次の請求期間の請求グループからのアカウントの自動関連付け解除を記録します。
BatchAssociateResourcesToCustomLineItem	リソースのバッチ関連付けをパーセンテージカスタム明細項目に記録します。
BatchDisassociateResourcesFromCustomLineItem	パーセンテージカスタム明細項目からのリソースのバッチ関連付け解除を記録します。
CreateBillingGroup	請求グループの作成をログに記録します。
CreateCustomLineItem	カスタム明細項目の作成をログに記録します。
CreatePricingPlan	料金プランの作成をログに記録します。
CreatePricingRule	料金設定ルールの作成をログに記録します。
DeleteBillingGroup	請求グループの削除を記録します。
DeleteCustomLineItem	カスタム明細項目の削除をログに記録します。
DeletePricingPlan	料金プランの削除を記録します。

イベント名	定義
DeletePricingRule	料金設定ルールの削除をログに記録します。
DisassociateAccounts	請求グループからのアカウントの関連付け解除を記録します。
DisassociatePricingRules	料金プランからの料金ルールの関連付け解除を記録します。
ListAccountAssociations	請求グループのアカウント ID へのアクセスを記録します。
ListBillingGroupCostReports	請求グループの実際の AWS 料金へのアクセスを記録します。
ListBillingGroups	請求期間中の請求グループへのアクセスを記録します。
ListCustomLineItems	請求期間中のカスタム明細項目へのアクセスを記録します。
ListCustomLineItemVersions	カスタム明細項目のバージョンへのアクセスを記録します。
ListPricingPlans	請求期間中の料金プランへのアクセスを記録します。
ListPricingPlansAssociatedWithPricingRule	料金設定ルールに関連付けられた料金プランへのアクセスをログに記録します。
ListPricingRules	請求期間の料金設定ルールへのアクセスを記録します。
ListPricingRulesAssociatedToPricingPlan	料金プランに関連付けられた料金ルールへのアクセスを記録します。

イベント名	定義
ListResourcesAssociatedToCustomLineItem	カスタム明細項目に関連付けられたリソースへのアクセスを記録します。
ListTagsForResource	リソースのタグへのアクセスを記録します。
TagResource	リソース上のタグの関連付けを記録します。
UpdateBillingGroup	請求グループの更新を記録します。
UpdateCustomLineItem	カスタム明細項目の更新を記録します。
UpdatePricingPlan	料金プランの更新を記録します。
UpdatePricingRule	料金設定ルールの更新を記録します。

AWS の Billing Conductor 情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 で が有効になります。 AWS Billing Conductor でアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他の AWS サービスイベントとともにイベントに記録されます。 で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「イベント履歴で CloudTrail イベントを表示する」を参照してください。

AWS Billing Conductor のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」

- CloudTrail がサポートするサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

すべての AWS Billing Conductor アクションは によってログに記録 CloudTrail され、AWS 「 Billing Conductor API リファレンス」に記載されています。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザーの認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail userIdentity 要素」を参照してください。

AWS Billing Conductor ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

トピック

- AutoAssociateアカウント
- CreateBillingグループ

AutoAssociateアカウント

次の例は、 `AutoAssociateAccount`アクションを示す CloudTrail ログエントリを示しています。

```
{
```

```
    "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"
}
```


CreateBillingグループ

次の例は、 CreateBillingGroupアクションを示す CloudTrail ログエントリを示しています。


```
{
    "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 Billing Conductor のコンプライアンス検証

サードパーティーの監査者は、複数の コンプライアンスプログラムの一環として AWS サービスのセキュリティと AWS コンプライアンスを評価します。 AWS Billing Conductor は AWS コンプライアンスプログラムの対象ではありません。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」「コンプライアンスプログラム」を参照してください。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、Downloading Reports in AWS および を参照してください。

AWS Billing Conductor を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- 「セキュリティ & コンプライアンスクイックリファレンスガイド」 – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、 AWSでセキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイするための手順が記載されています。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

AWS Billing Conductor の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

AWS Billing Conductor のインフラストラクチャセキュリティ

マネージドサービスである AWS Billing Conductor は、 AWS グローバルネットワークセキュリティによって保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS が公開した API コールを使用して、ネットワーク経由で Billing Conductor にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token ServiceAWS STS を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

クォータと制限

次の表に、AWS Billing Conductor 内のクォータと制約を示します。

クォータ

支払者アカウントごとの請求グループの数	5,000
請求グループごとのアカウント数	1,000
料金プランの数	5,000
料金設定ルールの数	50,000
料金プランに関連付けることができる料金設定ルールの数	500
料金設定ルールに関連付けることができる料金プランの数	1,000
カスタム明細項目の数	50,000
パーセンテージカスタム明細項目に関連付けられるソース値の数	100
フラットカスタム明細項目に関連付けられるパーセンテージカスタムの数	100

制限事項

次の表のその他の制約は、引き上げることができません。

請求グループあたりの請求グループの Cost and Usage Report の数	10
請求グループ名	• 128 文字以内でなければなりません • space を含めることはできません

	• 特殊文字は使用できません
請求グループの説明	1,024 文字以内でなければなりません
料金プラン名	• 128 文字以内でなければなりません • space を含めることはできません • 特殊文字は使用できません
料金プランの説明	1,024 文字以内でなければなりません
カスタム明細項目の名前	• 128 文字以内でなければなりません • space を含めることはできません • 特殊文字は使用できません

ドキュメント履歴

次の表は、 AWS Billing Conductor の今回のリリースの内容をまとめたものです。

変更	説明	日付
更新版	「 AWS Billing Conductorとは」トピックを更新しました。	2024 年 3 月 7 日
AWS マネージドポリシーのドキュメントを更新しました	AWSBillingConductorReadOnlyAccess ポリシーGetBillingGroupCostReport に を追加しました。「 の AWS マネージドポリシー AWS Billing Conductor」を参照してください。	2024 年 2 月 8 日
マージンの概要に関するドキュメントを追加	AWS のサービス 請求グループのマージンの詳細は、 で表示できます。「請求グループごとのマージンの分析」を参照してください。	2023 年 12 月 14 日
カスタム明細項目に関するドキュメントを追加	請求グループ内の特定の連結アカウントにカスタム明細項目を適用できます。「請求グループごとのカスタム明細項目の作成」を参照してください。	2023 年 12 月 4 日
プライマリアカウントに関するドキュメントを追加しました	プライマリアカウントを選択すると、請求グループの見積もりコストにどのように影響するかを理解します。「プライマリアカウントの参加日の	2023 年 10 月 26 日

	重要性を理解する」を参照してください。	
カスタム明細項目フィルターのサポートを追加しました	カスタム明細項目に対して、明細項目フィルターを指定できるようになりました。詳細については、「割合料金のカスタム明細項目の作成」を参照してください。	2023 年 9 月 5 日
見積もりコストに関するドキュメントを追加	以下のトピックを参照してください。 • での見積りコストに対するアドホック分析の実行 AWS Cost Explorer • AWS のサービス 見積もりコストをサポートする • IAM ポリシーの例: 見積もりコストへのアクセスを拒否する	2023 年 8 月 22 日
自動アカウント関連付けのサポートが追加されました	請求グループの自動アカウント関連付けを有効にできるようになりました。詳細については、請求グループ、料金設定、およびカスタム明細項目の作成を参照してください。	2023 年 7 月 26 日
CSV ダウンロードサポートを追加	請求グループのマージン分析テーブルの CSV ファイルをダウンロードできます。詳細については、「請求グループごとのマージン分析」を参照してください。	2023 年 6 月 6 日

初回リリース	AWS Billing Conductor ユーザーガイドと API リファレンスの初回リリース。	2022 年 3 月 16 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。