aws

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、チャネル AWS Marketplace パートナー (パートナー) およびチャージバック要件がある組織向けのカスタム請求サービスです。パートナーの場合、チャージバックは顧客から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 の 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 (アカウントの集合など) のコストを正しい内部予算または損益 (P&L) ステートメントに配分できます。

Billing Conductor を使用すると、これらのアクティビティを実現するために、お客様は 2 番目の見積りバージョンのコストを作成し、顧客またはアカウント所有者と共有できます。見積りコストは、Billing Conductor で定義された料金レートで、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 (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 請求書と一致) と見積りコスト (Billing Conductor 設定と一致) の使用上の違いを 1 か月間で観察します。ただし、 AWS 請求書が発行されると、使用量の値は毎月月末に一致します。

見積りコストを定義すると、お客様は次のいずれかのユースケースに合わせてコストを一様にモデル化できます。

1. 顧客契約。 の外部で交渉されたパートナーユースケースである場合があります。 AWS
2. 内部会計プラクティス。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 (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) からの顧客の既存の請求書には影響しません。

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りコストと請求対象コストの差) を分析する
- の見積りコストを表示する AWS Cost Explorer
- 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
- 見積りコストを反映した Reservation and Savings Plans のカバレッジと使用状況レポートを表示する

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、請求詳細ページの見積りコストを分析できます。マネージドアカウントは、予算を作成して見積り支出をモニタリングし、希望する見積り支出の上限を超えたとき、または超えると予測されるときにアラートを受け取ることもできます。

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。

# AWS Billing Conductor の機能

AWS Billing Conductor の機能を使用して、次の操作を実行できます。

アカウントをグループ化する

アカウントを請求グループに整理して、見積りコストを集計して表示します。グループごとに、クロスサービス割引や などの個々の顧客のメリット AWS 無料利用枠 をシミュレートします。

カスタム料金

グローバルまたは特定のマークアップ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

請求グループに 1 回限りまたは定期的な定額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。請求グループのアカウントは、見積りコストを反映した Reservation and Savings Plans のカバレッジと使用状況レポートを表示できます。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。

予算

請求グループのアカウントは、予算を作成して見積り支出をモニタリングし、希望する見積り支出の上限を超えたとき、または超えると予測されるときにアラートを受け取ることができます。

# AWS Billing Conductor の料金

料金の詳細については、「AWS Billing Conductor 料金」を参照してください。

# 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企業から大企業まで、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を表示したり、請求設定を管理したり、支払いに必要な請求アーティファクトにアクセスしたりできます AWS。 AWS 請求コンソールでは、アカウントの支出の概要も説明され、 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 ユーザーガイドをご参照ください。

AWS Cost Explorer

Cost Explorer インターフェイスを使用して、時間の経過に伴う AWS コストと使用状況を視覚化、理解、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、以下の各トピックを参照してください。

- での見積りコストの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、利用可能な最も包括的なコストと使用状況データの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、オペレーションの一意の組み合わせごとの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、ジョブを完了するために必要なアクセス量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 の製品とサービスは、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 の計算により、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、いくつかの根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なものです。これは AWS 請求書から分離され、毎月支払うべき実際の料金を反映していません。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 請求には影響しません。お客様またはお客様の組織の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、サービスを効果的に使用できるように、 AWS Billing Conductor 全体で使用される主要な用語を定義します。

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た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

支払うべき実際のコストを表す標準 AWS 請求書 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。

Billable

によって生成 AWS され、請求書の計算の基礎として使用される AWS 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を計算するために使用される入力。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。

# 見積り請求データについて

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。

## 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重要な違いがあります。

- 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によって購入された場合にのみ、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。空の料金プランを請求グループに適用すると、料金レートはデフォルトでパブリック AWS オンデマンド料金になります。

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？

支払者アカウントは、これらの料金を支払う責任を負うため、常に標準 AWS 請求を表示できます AWS。また、請求ページと で各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「請求グループ別のコストと使用状況レポートの設定」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。プロフォーマ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。指定された SKU の最初の有料オファーと交換されます。

常に無料利用枠

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、料金ルール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階層データがない場合、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 AWS 請求で生成されたコストを照合することはできません。たとえば、標準 AWS 請求書で請求されるプライベート割引と税金を差し引いて、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。

## プロフォーマドメインで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、利点はまず、購入請求グループアカウント内で発生する対象となる使用量に適用されます。残りの利点は、グループ内の他のアカウントに分散されます。

支払いレベルで行われた 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された 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、RIsと Savings Plans が見積りドメインにどのように適用されるかに影響を与える可能

性がありますが、同じ RIsと Savings Plans が請求対象ドメインにどのように適用されるかには影響しません。

# 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。KPI はすべて過去 1 か月のものです。アカウントを作成または追加すると 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 – AWS 請求の推定請求額に従って、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month-to-dateまでの合計請求額。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の月次累計マージンです。マージンは、請求額から 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、「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

請求グループは、共通のエンドユーザーを共有する一括請求ファミリー内のアカウントのセットです。これは、見積り請求ドメインにのみ適用されます。そのエンドカスタマーはプライマリアカウントを維持し、 グループ全体で発生したコストと使用状況を確認できます。各請求グループの見積り使用量は、独自の一括請求ファミリーとして計算されます。使用量共有 RI と Savings Plans の特典は、グループ内でのみ提供され、ボリューム階層割引と Always Free Tier サービスが発生します。アカウントは、請求期間中に 1 つの請求グループにのみ関連付けることができます。

目次



## 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

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/billingconductor/ で AWS Billing Conductor 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。
   > - 現在 CloudTrail ログ記録証跡がある場合は、CloudTrail ログで自動アカウントの関連付けを確認できます。

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見積りコストと使用状況を表示する機能を継承し、請求グループの見積りコストと使用状況レポート (AWS CUR) を生成できます。

   当月に組織に参加したプライマリアカウントを選択した場合、その請求グループ内のすべてのアカウントの見積りコストには、プライマリアカウントが組織に参加してから蓄積されたコスト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と退出日が見積り請求にどのように影響するかを理解する」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。

# 請求グループの詳細の表示

このセクションを使用して、請求グループと料金プランの設定を確認するさまざまな方法と、作成後の出力を確認できます。

## 請求グループテーブルの表示

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。

## 請求グループ別の見積り設定の表示

請求グループの詳細を使用して、 AWS Billing Conductor で請求グループをモニタリング、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。

請求グループの詳細ページを表示するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/billingconductor/ で AWS Billing Conductor 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. 請求グループ テーブルで、請求グループ名を選択します。

## 連結アカウントによる見積り設定の表示

Billing Conductor コンソールのアカウントインベントリツールを使用して、連結アカウントごとに AWS 請求グループ設定を確認できます。

連結アカウントで請求グループ設定を表示するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/billingconductor/ で AWS Billing Conductor を開きます。
2. ナビゲーションペインで、アカウントインベントリを選択します。
3. アカウントインベントリテーブルで、アカウント ID を検索するか、フィルターを使用してアカウント ID を検索します。
4. アカウントを選択して、アカウントと請求グループの設定を表示します。

## 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. https://console.aws.amazon.com/costmanagement/ で AWS Billing and Cost Management コンソールを開きます。
2. ナビゲーションペインで [請求] 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。

Billing AWS Conductor で定義されているレートに従って、請求グループの使用状況をサービスおよび AWS リージョン別に分析して、その使用量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。

# 請求グループ別のコストと使用状況レポートの設定

作成した請求グループごとに見積り AWS コストと使用状況レポート (AWS CUR) を作成できます。見積り CUR AWS は、標準の CUR AWS と同じファイル形式、粒度、および列を持ち、特定の期間に利用可能な最も包括的なコストと使用状況データのセットが含まれています。

プロフォーマ CUR AWS 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 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。標準 CUR 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。

## AWS Billing Conductor CUR AWS と標準 CUR AWS 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のコストと使用状況レポートと見積り AWS CUR にはいくつかの違いがあります。

- 標準の CUR AWS 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り CUR AWS には、計算時に請求グループのアカウントのみが含まれます。

- 標準の CUR は 1 AWS 回請求書列に入力され、請求書は によって生成されます AWS。見積り AWS CUR は請求書列に入力されません。現在、見積り請求データ AWS に基づいて が生成または発行する請求書はありません。

次の手順を使用して、請求グループの見積り AWS CUR を生成します。

請求グループのプロフォーマコストと使用料レポートを作成するには

1. https://console.aws.amazon.com/costmanagement/ で AWS Billing and Cost Management コンソールを開きます。
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. [有効化] を選択します。
6. [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、請求書の確定後に AWS コストと使用状況の新しい変更で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. [次へ] を選択します。
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、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. [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。

    このステップは Amazon Redshift または 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. [時間粒度] で、次のいずれかを選択します。

    - 時間単位: 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。
    - 日単位: 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. [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. のレポートデータ統合を有効にする で、コストと使用状況レポートを Amazon Athena、Amazon Redshift、または QuickSight にアップロードするかどうかを選択します。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 QuickSight: .gz 圧縮
20. [次へ] を選択します。
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。

# 料金ルール

AWS Billing Conductor で料金ルールを作成して、請求グループ全体で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。

目次



## 料金設定ルールの作成

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. AWS Billing Conductor を https://console.aws.amazon.com/billingconductor/ で開きます。
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。請求エンティティは、、その関連会社 AWS、またはサービスを販売するサードパーティープロバイダーによって提供されるサービスの販売者です 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。小数値を入力すると、小数点以下第 2 位に四捨五入されます。

> **Note**
>
> この割合は、メンバーアカウントの請求書ページに表示されます。例えば、`EC2 t3.micro on-demand (+20%)` と指定します。

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の表示

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

AWS Billing Conductor で料金プランを作成して、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。

目次



## 料金プランの作成

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. AWS Billing Conductor を https://console.aws.amazon.com/billingconductor/ で開きます。
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。

# 料金プランテーブルの表示

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

# カスタム明細項目

AWS Billing Conductor を使用して、パーソナライズされた明細項目を作成し、請求グループ内で指定された AWS アカウント に適用します。

カスタム明細項目を使用して、コスト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ト料金の値として計算できます。パーセンテージベースのカスタム明細項目を設定して、リソースを含めるか除外します。これらのリソースには、請求グループのコストと、請求期間中に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明細項目が含まれます。その後、カスタム明細項目を 1 か月間適用するか、複数か月間繰り返し実行するように設定できます。

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)。

- サポート 料金の割り当て
- 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. AWS Billing Conductor を https://console.aws.amazon.com/billingconductor/ で開きます。
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) 割り当てられたアカウントでは、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の定額料金を選択します。
10. 請求タイプを選択し、入力量を入力します。

    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. [Create] (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/ で AWS Billing Conductor 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) 割り当てられたアカウントでは、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の料金の割合を選択します。
10. 請求タイプを選択し、入力量を入力します。

    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. [Create] (作成) を選択します。

# カスタム明細項目テーブルの表示

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/ で AWS Billing Conductor 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 (フラットまたはパーセンテージ ) 、または請求値タイプ (クレジットまたは料金) を変更することはできません。

7. [Save changes] (変更の保存) 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/ で AWS Billing Conductor 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。

# マージンの分析

AWS Billing Conductor でマージンの概要とマージンの詳細を使用して、マージンを集計および特定の請求グループの両方で分析できます。

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。

目次



## マージンの概要でマージンの集計を表示する

### 請求グループのマージンの概要の表示

請求グループのマージンの概要を表示するには

1. AWS Billing Conductor を https://console.aws.amazon.com/billingconductor/ で開きます。
2. ナビゲーションペインの分析で、マージンの概要を選択します。
3. レポートタイプで、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. 請求グループの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. Month-to-dateの概要セクションでは、請求額、AWS コスト、マージンを表示できます。
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。
   - マージン分析テーブルのテーブルとして。

   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。

## マージン分析テーブルについて

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。

# マージンの詳細 AWS のサービス を使用してマージンを表示する

## サービス別の請求グループのマージンの表示

サービスごとに請求グループのマージンを表示するには

1. AWS Billing Conductor を https://console.aws.amazon.com/billingconductor/ で開きます。
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 つのサービスによるマージントレンドセクションの折れ線グラフとして。
    - マージン分析テーブルのテーブルとして。

## マージンの傾向グラフについて

マージンの詳細には、選択した請求期間の上位 5 つのサービスをマージンで表示する折れ線グラフが表示されます。折れ線グラフには、比較のために過去 3 か月間の各サービスのマージンが表示されます。

このグラフには、選択した請求期間の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、次の列が含まれます。

- サービス名
- 平均
- マージン

請求グループが過去 3 か月間にわたって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。

## マージン分析テーブルについて

請求グループのマージン分析テーブルには、次の列が含まれます。

- サービス名
- 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

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。

# Billing and Cost Management での見積りデータの表示

このセクションでは、請求情報とコスト管理コンソールで見積りデータを表示する方法を示します。AWS Billing Conductor の請求ページ統合について説明します。Cost Explorer で見積りコストを分析、予測、レポートすることもできます。見積りコストをサポートするすべてのクラウド財務管理サービスのコンパイル済みリストは参照できます。見積りコストをサポートし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レートでコスト AWS アカウント を使用します。

目次



## 請求ページで見積りコストを表示する

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. https://console.aws.amazon.com/costmanagement/ で AWS Billing and Cost Management コンソールを開きます。
2. ナビゲーションペインで [請求] 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。

Billing AWS Conductor で定義されているレートに従って、請求グループの使用状況をサービスおよび AWS リージョン別に分析して、その使用量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。

## での見積りコストの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。

請求グループマネージドアカウント (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、見積りデータを利用できます。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。履歴データが必要な場合は、 サポート センターに連絡して支払いアカウントがバックフィルをリクエストできます。データは、請求グループ設定に合わせて見積り形式で表示されます。

> **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 で見積りコストを確認できます。
> - Cost Explorer では、時間単位の詳細度データは見積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 見積りコストをサポートする。

## Savings Plans、予約カバレッジ、使用状況レポートの分析

Billing Conductor 請求グループ AWS アカウント で、 の Savings Plans、予約カバレッジ、使用状況レポートを分析できます。レポートは請求グループごとに生成されます。プライマリ請求グループアカウントは、グループ内のすべてのアカウントの見積りコストに基づいて、カバレッジと使用率の

データを表示できます。見積りドメインでは、Savings Plans と予約は、請求対象ドメインの設定にかかわらず、請求グループ内でのみ共有されます。つまり、見積りカバレッジと使用率レポートは、見積り予約と Savings Plans の共有設定に基づいて請求グループレベルで計算されます。これは、請求グループ内のすべてのアカウントでデフォルトで有効になっています。

請求グループ管理アカウントまたは請求グループメンバーは、そのアカウントに Savings Plans の購入または予約がある場合、見積りコストに基づいてカバレッジと使用率データを表示できます。請求対象のカバレッジと使用率の履歴データを表示することはできません。プロフォーマデータは、2024 年 2 月までのみバックフィルできます。

分析には、次のグラフを使用できます。

Savings Plans 使用率グラフ

これは、オンデマンド支出に相当する見積りコストと純削減額の合計を示しています。

Savings Plans カバレッジグラフ

これは、オンデマンド支出の見積りコストがカバーされていないことと、オンデマンドと比較して月額削減の可能性を示しています。

予約使用率グラフ

これは、有効な予約コスト、オンデマンドコスト同等額、純削減額の合計、および潜在的な削減額の合計に基づく見積りコストを示しています。

予約カバレッジグラフ

これは、オンデマンドコストと年間削減額の合計に対する見積りコストを示しています。

> **Note**
>
> - 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。この機能は、請求グループのアカウントでのみ使用できます。
> - 合計コミットメント値は、見積りドメインの影響を受けません。
> - 予測使用率レポートとカバレッジレポートは、最適化の決定を行うためのリファレンスとして使用しないでください。例えば、ワークロード、Savings Plans、予約購入の変更などです。最適化の決定については、請求可能な使用率レポートとカバレッジレポートを参照してください。

- 見積りデータに基づいて予約や Savings Plans の購入を行う前に、請求管理者または組織と相談することをお勧めします。Savings Plans および予約購入の推奨事項は、請求可能な共有設定、請求可能なオンデマンド支出、および請求可能なドメイン内の既存の Savings Plans や予約のパフォーマンスに基づいて、正確なレコメンデーションを提供します。Savings Plans と予約のレコメンデーションには、請求グループのプライマリアカウントと連結アカウントの請求可能な使用率とカバレッジレポートで報告されたインサイトが反映されます。Savings Plans と予約購入のレコメンデーションページを請求グループ内のアカウントとして参照すると、推奨されるコミットメント値に請求可能な使用率とカバレッジレポートが正確に反映されます。これは、組織の最適化に関する意思決定の信頼できる情報源です。

## 請求グループ設定と Savings Plans 共有設定の影響を理解する

割引特典は Billing Conductor 内の請求グループ内で共有されます。このため、Savings Plans のカバレッジと使用率のメトリクスは、請求対象ドメインの請求グループ設定または Savings Plans の共有設定に基づいて変更される場合があります。

例

- Savings Plans の共有が請求対象ドメイン内の組織内のすべてのアカウントで有効になっており、組織内のすべてのアカウントを含む請求グループが 1 つある場合、請求対象ドメインと見積りドメイン間のカバレッジと使用率のメトリクスに差異はありません。
- 請求対象ドメイン内の組織内のすべてのアカウントで Savings Plans 共有が有効になっているが、Billing Conductor プロフォーマドメインが組織内のアカウントのサブセットを含む請求グループが 1 つあるか、複数の請求グループがそれぞれアカウントのサブセットを含むように設定されている場合、プロフォーマドメインと請求対象ドメインのカバレッジメトリクスと使用率メトリクスに差異が生じます。差異の性質は、請求グループの設定と、Savings Plans が請求グループ内外のアカウントに存在するかどうかによって異なります。ただし、見積りドメインでは請求対象ドメインと比較して使用率メトリクスが低く、見積りドメインでは請求対象ドメインと比較してカバレッジが高くなる可能性があります。
- Savings Plans の共有が請求対象ドメイン内の特定の連結アカウントに制限されており、請求グループに Savings Plans を購入したアカウントが含まれている場合、使用率とカバレッジのメトリクスは請求対象ドメインと比較して按分的に高くなる可能性があります。これは、見積り Savings Plans の共有動作が、制限付きの請求可能な共有設定よりも優先されるためです。これにより、より多くのアカウント (請求グループである場合) が Savings Plans の恩恵を受けることができます。

Savings Plans と予約レポートの詳細については、「 Savings Plans ユーザーガイド」の「Savings Plans のモニタリング」およびAWS Cost Management 「 ユーザーガイド」のCost Explorer での予約の理解」を参照してください。 Savings Plans

## 予約と Savings Plans インベントリを表示する

Billing Conductor 請求グループ AWS アカウント で の Savings Plans と予約インベントリを表示できます。プライマリ請求グループアカウントは、請求グループ内のアカウントのインベントリを表示できます。Savings Plans と予約は、請求対象ドメインの設定にかかわらず、請求グループ内でのみ共有されます。

請求グループ管理アカウントまたは請求グループメンバーは、そのアカウントで購入された場合、予約と Savings Plans インベントリを表示できます。

Savings Plans と予約インベントリを表示するには (請求グループのプライマリアカウントのみ )

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/costmanagement/ で AWS Billing and Cost Management コンソールを開きます。
2. ナビゲーションペインで、インベントリの下の Savings Plans を選択します。

を使用している場合 AWS Organizations、管理アカウントは Savings Plans と予約インベントリを表示できます。

> **Note**
>
> - 請求グループメンバーアカウントの場合、キューに登録された Savings Plans はSavings Plans AWS アカウント の購入のアカウントインベントリページにのみ表示されます (プライマリアカウントの Organizations インベントリには表示されません )。

# での見積りデータの表示 AWS Budgets

AWS アカウント AWS Billing Conductor 請求グループの は、 を使用して見積り支出をモニタリングできます AWS Budgets。Billing Conductor 請求グループ AWS アカウント で によって作成された予算は、見積り請求データをキャプチャし、見積り支出制限を超えたときにアラートを有効にします。予算予測も見積りデータに基づいており、使用制限を超過するとアラートも表示されます。

請求グループのプライマリアカウントは、全体的な請求グループの見積り支出と、特定の請求グループメンバーアカウントの支出をモニタリングできます。請求グループ管理アカウントまたは請求グループメンバーは、独自の見積り予算を作成および表示できます AWS アカウント。これらのアカウントは、請求グループのメンバーであった請求期間の予算履歴を表示できます。請求データは、請求グループに参加する前の日付の予算履歴からは共有されません。

アカウントが請求グループに参加すると、既存の予算情報が見積りデータのキャプチャを開始します。予算履歴と予測は、見積りデータに基づいています。アカウントが請求グループを離れると、予算は請求対象データのキャプチャを開始します。予算履歴と予測は、今後請求可能なデータに基づいて行われます。

> **Note**
>
> 請求可能なデータに対して以前に予算アラートが設定されていた請求グループの連結アカウントは、見積りデータビューに合わせてしきい値を予算アラートに更新することをお勧めします。

詳細については AWS Budgets、「 AWS Cost Management ユーザーガイド」の「 によるコストの管理 AWS Budgets」を参照してください。

## AWS のサービス 見積りコストをサポートする

次の Cloud Financial Management サービスとその機能は、見積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 | あり | あり | あり |
| 分割コストの配分 | いいえ | いいえ | いいえ |
| AWS Billing | なし | あり | あり |
| ダッシュボード | いいえ | あり | あり |

| 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 | | |
|---|---|---|---|
| 請求の詳細 | あり | あり | あり |
| CSV をダウンロードする | いいえ | いいえ | いいえ |
| AWS Cost Explorer | なし | あり | あり |
| 予測 | いいえ | あり | あり |
| レポートを保存する | いいえ | あり | あり |
| 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 | あり | あり |
| Savings Plans カバレッジレポート | いいえ | あり | あり |
| 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 | あり | あり |
| 予約カバレッジレポート | いいえ | あり | はい |
| AWS Budgets | なし | あり | あり |
| 予算レポート | いいえ | あり | あり |

見積りコストをサポートしていないサービスや機能の場合、 AWS アカウント は AWS 請求書と一致する請求可能な料金でコストを確認します。

## 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、「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 Billing and Cost Explorer 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 の概念と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について説明します。

## AWS Billing Conductor へのアクセスの制御

AWS Billing Conductor は、支払者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、Billing and Cost Management コンソールで AWS Billing Conductor の重要業績評価指標 (KPIs) を表示するアクセス許可を 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 ID とアクセスの管理 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ときは、プログラムによるアクセスを許可する一意の 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について、より正確なアクセスコントロールを定義できます。 AWS Billing Conductor API へのクエリアクセスを複数の IAM ユーザーに許可するには、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。

## プライマリアカウントの参加日と退出日が見積り請求にどのように影響するかを理解する

プライマリアカウントが Organization に参加した日付は、その請求グループの見積りコストの過去の境界を定義します。月の途中で Organization に参加したアカウントを請求グループのプライマリアカウントとして選択した場合、その請求グループ内のすべてのアカウントは、その月の前半の見積り請求データを表示できません。これは、プライマリアカウントが、その時点で Organization の一部ではなかったためです。同様に、プライマリアカウントが月の途中で Organization を離れた場合、請求グループ内のアカウントは、プライマリアカウントが Organization を離れた日付からの見積り請求を確認できません。

> **Note**
>
> 請求グループは、プライマリアカウントが Organization を離れた翌月に削除対象としてマークされます。この請求グループのアカウントの見積り請求を今後数か月間維持するには、請求グループを削除して新しいグループを作成することをお勧めします。新しい請求グループは、新しいプライマリアカウントで作成することも、Organization に再参加した場合は元のアカウントを使用して作成することもできます。

例えば、プライマリアカウントが 10 月 15 日に組織に加わり、10 月 28 日に退出したとします。請求グループ内のすべてのアカウントの見積り請求データには、10 月 15 日から 28 日までのコストと使用状況のみが含まれます。これは、他のアカウントが 10 月全体の請求グループの一部である場合にも当てはまります。

請求可能な見積りドメイン全体でコストデータセットと使用状況データセットの不一致を回避するには、プライマリアカウントとして選択されたアカウントが 1 か月間にわたって Organization の一部であることを確認してください。

## 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 日に 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。以前の請求期間に適用されるように生成されたカスタム明細項目は、請求グループの AWS コストと使用状況レポート、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 の計算ロジックについて

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、特定の月に加え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。

メンバーアカウントのスタンスから、新しい請求グループの設定は、月の途中で が新しい請求グループから別の請求グループAccount 3に移動すると、その月のアカウントの使用に適用されます。これは、アカウントが月初から新しい請求グループと異なっているかのように Cost Explorer と請求書に反映されます。

| 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。お客様は AWS 、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を活用できます。

セキュリティは、 AWS とお客様の間の責任共有です。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 AWS 責任があります。 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。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。 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AWS による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。
- クラウド内のセキュリティ – 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、ユーザーは、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 を使用する際に責任共有モデルを適用する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ように AWS Billing Conductor を設定する方法について説明します。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 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 ID とアクセスの管理 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

AWS Billing Conductor でのデータ保護には、 AWS 責任共有モデルが適用されます。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。ユーザーは、このインフラストラクチャでホストされ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に関する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 AWS 責任共有モデルおよび GDPR のブログ記事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 が必須で、TLS 1.3 をお勧めします。
- で 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。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- 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 などの高度な管理された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 140-3 検証済み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) 140-3」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を、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含め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 タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

# の ID とアクセスの管理 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、追加料金なしで使用できる AWS のサービス 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すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。 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、「AWS Billing Conductor が IAM と連携する方法」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 ロールを引き受けることによって、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 認証情報は、フェデレーション ID の例です。フェデレーティッド ID 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、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」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を暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」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。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS 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「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」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 ID 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、一時的な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許可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 ユーザーに関するユースケース」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 ID 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。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 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「ロールを引き受けるための各種方法」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 ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID は

ロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可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。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」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、(プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。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 でのクロスアカウントのリソースへのアクセス」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許可、サービスロール、またはサービスリンク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アクションを実行すると AWS、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 へのリクエストをリクエストする 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「AWS のサービスに許可を委任するロールを作成する」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、サービスリンクロールのアクセス許可を表示できますが、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。EC2 インスタンスに AWS ロールを割り当て、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 ロールを使用して許可を付与する」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、ID AWS 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 JSON AWS 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対してどのような条件下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受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。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 ユーザーグループ、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 許可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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、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、 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「管理ポリシーとインラインポリシーのいずれかを選択する」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許可を持つかを制御します。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。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」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) の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、ビジネスが所有する複数の AWS アカウント 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「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- 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。が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。

# AWS Billing Conductor が IAM と連携する方法

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については、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、また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 JSON AWS 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対してどのような条件下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許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数の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アクセス許可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。

単一のステートメントに複数のアクションを指定するには次のようにコンマで区切ります。

```
"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 JSON AWS 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対してどのような条件下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、アマゾン 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、リソースレベルの許可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 ARNs、IAM ユーザーガイドの AWS Billing Conductor で定義されるリソースを参照してください。各リソースの ARN を指定できるアクションについては、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 JSON AWS 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対してどのような条件下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して、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 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では 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」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。

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。アクセス権が付与される 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 ロールと、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制御するには`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 役割を引き受ける、またはクロスアカウント役割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 GetFederationToken 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。

サービスにリンクされた役割

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。

サービス役割

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役割を引き受けることが許可されます。この役割により、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。サービス役割は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 管理者はこの役割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「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

- ポリシーに関するベストプラクティス
- Billing Conductor アイデンティティベースのポリシーの例

## ポリシーに関する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の付与を開始するには、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することで、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「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。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、最小特権アクセス許可とも呼ばれています。IAM を使用して許可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 でのポリシーとアクセス許可」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、サービスアクションが などの特定の を通じて使用されている場合に 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 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 でポリシーを検証する」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、MFA をオンにしてセキュリティを強化します。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 を使用した安全な API アクセス」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 アクセスの許可
- 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
- 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 Billing and Cost Explorer 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 アクセスの許可

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、IAM エンティティは、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を持ちます。OU のインポート機能は AWS Billing 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": "*"
        }
    ]
}
```

### 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 Billing and Cost Explorer 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。チームに必要な権限のみを提供する 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 管理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損なわ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ジョブ関数の マネージドポリシー AWS をサポートしています。例えば、ReadOnlyAccess 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 への完全なアクセスを許可します。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 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始してからの AWS Billing Conductor の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、AWS Billing Conductor ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

| 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 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| AWSBillingConductorReadOnlyAccess | 作成されるポリシー | 2022 年 3 月 29 日 |
| AWS Billing Conductor 変更ログが公開されました | AWS Billing Conductor は、AWS 管理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

## 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、 IpAddress および NotIpAddress条件と、 AWS ワイドaws:SourceIp条件キーである 条件キーを使用します。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:::amzn-s3-demo-bucket1/*",
```

```
      "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:PassRole を実行する権限がない
- 自分の AWS アカウント以外のユーザーに 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

で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* リソースにアクセスできるように、管理者にポリシーの更新を依頼します。

## iam:PassRole を実行する権限がない

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。メアリーには、ロールをサービスに渡す許可がありません。

```
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。

## 自分の AWS アカウント以外のユーザーに 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、「AWS Billing Conductor が IAM と連携する方法」を参照してください。
- 所有 AWS アカウント 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「所有 AWS アカウント 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。
- 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) へのアクセスの許可」を参照してください。

- 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使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」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、時間単位または日単位で情報を集計できます。

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 AWS CloudTrail、 AWS Billing Conductor のユーザー、ロール、または 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。CloudTrail は AWS Billing Conductor のすべての API コールをイベントとしてキャプチャします。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 のイベントなど、Amazon S3 バケットへの CloudTrail 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。CloudTrail で収集された情報を使用して、 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。

CloudTrail の詳細については、「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ています。

| イベント名 | 定義 |
| --- | --- |
| AssociateAccounts | 請求グループへのアカウントの関連付けをログに記録します。 |
| AssociatePricingRules | 料金プランへの料金ルールの関連付けをログに記録します。 |
| 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 | 次の請求期間中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ログに記録します。 |
| BatchAssociateResourcesToCustomLineItem | リソースのバッチ関連付けをパーセンテージのカスタム明細項目にログに記録します。 |
| BatchDisassociateResourcesFromCustomLineItem | パーセンテージの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ログに記録します。 |
| 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ログに記録します。 |
| DeleteCustomLineItem | カスタム明細項目の削除をログに記録します。 |

| イベント名 | 定義 |
| --- | --- |
| DeletePricingPlan | 料金プランの削除をログに記録します。 |
| DeletePricingRule | 料金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ログに記録します。 |
| DisassociatePricingRules | 料金プランからの料金ルールの関連付け解除をログに記録します。 |
| ListAccountAssociations | 請求グループのアカウント ID へのアクセスをログに記録します。 |
| 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ログに記録します。 |
| ListCustomLineItemVersions | カスタム明細項目のバージョンへのアクセスをログに記録します。 |
| 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 | 請求期間中の料金ルールへのアクセスをログに記録します。 |

| イベント名 | 定義 |
| --- | --- |
| 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ログに記録します。 |
| 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ログに記録します。 |
| ListTagsForResource | リソースのタグへのアクセスをログに記録します。 |
| TagResource | リソース上のタグの関連付けをログに記録します。 |
| UpdateBillingGroup | 請求グループの更新をログに記録します。 |
| UpdateCustomLineItem | カスタム明細項目の更新をログに記録します。 |
| UpdatePricingPlan | 料金プランの更新をログに記録します。 |
| UpdatePricingRule | 料金ルールの更新をログに記録します。 |

## AWS CloudTrail の Billing Conductor 情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。 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イベント履歴の他の AWS サービスイベントとともに CloudTrail 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、「CloudTrail イベント履歴でのイベントの表示」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さらに分析して処理するように、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:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

すべての AWS Billing Conductor アクションは CloudTrail によってログに記録され、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 エレメント」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

「トレイル」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するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、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の情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出し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

- AutoAssociateAccount
- CreateBillingGroup

### AutoAssociateAccount

以下の例は、AutoAssociateAccount アクションを示す CloudTrail ログエントリです。


```
{
    "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"
}
```


### CreateBillingGroup

以下の例は、CreateBillingGroup アクションを示す CloudTrail ログエントリです。


```
{
```

```
    "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AWS プログラムによる対象範囲内のサービスコンプライアンス」を参照してください。一般的な情報については、AWS 「 Compliance ProgramsAssurance」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、「AWS Artifact でのレポートのダウンロード」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。 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、リソース設定が内部プラクティス、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、冗長性の高い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で保護されています。 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、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された 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 が必須で、TLS 1.3 をお勧めします。
- 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 Service (AWS 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。

## インターフェイスエンドポイント (AWS PrivateLink) AWS Billing Conductor を使用した へのアクセス

を使用して AWS PrivateLink 、VPC と の間にプライベート接続を作成できます AWS Billing Conductor。インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を使用せずに、VPC 内にあるかのように Billing Conductor にアクセスできます。VPC 内のインスタンスは、Billing Conductor にアクセスするためにパブリック IP アドレスを必要としません。

このプライベート接続を確立するには、 AWS PrivateLinkを利用したインターフェイスエンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、Billing Conductor 宛てのトラフィックのエントリポイントとして機能するリクエスタ管理のネットワークインターフェイスです。

詳細については、「 AWS PrivateLink ガイド」の「Access AWS のサービス through AWS PrivateLink」を参照してください。

## Billing Conductor に関する考慮事項

Billing Conductor のインターフェイスエンドポイントを設定する前に、「 AWS PrivateLink ガイド」の「考慮事項」を参照してください。

Billing Conductor は、インターフェイスエンドポイントを介したすべての API アクションの呼び出しをサポートしています。

VPC エンドポイントポリシーは Billing Conductor ではサポートされていません。デフォルトでは、Billing Conductor へのフルアクセスはインターフェイスエンドポイントを介して許可されます。または、セキュリティグループをエンドポイントネットワークインターフェイスに関連付けて、インターフェイスエンドポイントを介して Billing Conductor へのトラフィックを制御することもできます。

## Billing Conductor のインターフェイスエンドポイントを作成する

Billing Conductor のインターフェイスエンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface () を使用して作成できますAWS CLI。詳細については、「AWS PrivateLink ガイド」の「インターフェイスエンドポイントを作成」を参照してください。

次のサービス名を使用して Billing Conductor のインターフェイスエンドポイントを作成します。

```
com.amazonaws.region.service-name
```

インターフェイスエンドポイントのプライベート DNS を有効にすると、デフォルトのリージョン DNS 名を使用して Billing Conductor に API リクエストを行うことができます。例えば、`service-name.us-east-1.amazonaws.com`。

## インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイントを介して Billing Conductor へのフルアクセスを許可します。VPC から Billing Conductor に許可されるアクセスを制御するには、カスタムエンドポイントポリシーをインターフェイスエンドポイントにアタッチします。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。

- このアクションを実行できるリソース。

詳細については、AWS PrivateLink ガイドのControl access to services using endpoint policies (エンドポイントポリシーを使用してサービスへのアクセスをコントロールする)を参照してください。

例: Billing Conductor アクションの VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。このポリシーをインターフェイスエンドポイントにアタッチすると、すべてのリソースのすべてのプリンシパルに対して、リストされている Billing Conductor アクションへのアクセスが許可されます。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": "billingconductor:*",
         "Resource":"*"
      }
   ]
}
```

# クォータと制限

次の表は、 AWS Billing Conductor 内のクォータと制限について説明しています。

## 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<br>• 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<br>• space を含めることはできません<br>• 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<br>• space を含めることはできません<br>• 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ドキュメントをまとめたものです。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新版 | 予約プランと Savings Plans は Billing Conductor と統合されています。Savings Plans」のトピックを参照してください。 | 2024 年 10 月 10 日 |
| 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 管理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。AWS の 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 | 請求グループのマージンの詳細 AWS のサービス を で表示できます。「請求グループあたりのマージンの分析」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の選択が請求グループの見積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重要性を理解する」を参照してください。 | 2023 年 10 月 26 日 |
| 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。<br>• 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<br>• AWS のサービス 見積りコストをサポートする<br>• IAM ポリシーの例: 見積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 |

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。