aws

ユーザーガイド

Application Cost Profiler

Application Cost Profiler: ユーザーガイド

Table of Contents

AWS Application Cost Profiler は 2024 年 9 月 30 日までに廃止される予定で、現在、新規のお客様は受け付けていません。

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。

AWS Application Cost Profiler とは

AWS Application Cost Profiler は、AWS の請求とコストをサービスのテナント別に区別するのに役立ちます。テナントは、ユーザー、ユーザーのグループ、またはプロジェクトです。

リソースは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなど、ユーザーが AWS で操作できるエンティティです。選択したテナント別にリソース使用状況を特定できることを確認します。

一般的な AWS リソース使用状況には、組織内の複数のテナントをサポートする共有サービスが含まれます。特定のリソースは時間ベースのディメンションを使用します。リソースの 1 時間あたりの使用状況ではなく、テナント別にコスト情報と請求情報を取得するために、リソースを Application Cost Profiler と統合できます。このきめ細かなアプローチによって、共有のソフトウェアソリューション全体で AWS リソースがどのように消費されているかを把握できます。

Application Cost Profiler では、時間ベースのディメンションまたは 1 時間あたりの使用量のいずれかを使用できる以下のリソースが有効になっています。

- Amazon EC2 インスタンス (オンデマンドインスタンスとスポットインスタンスのみ)
- Amazon Simple Queue Service (Amazon SQS) キュー
- Amazon Simple Notification Service (Amazon SNS) のトピック
- Amazon DynamoDB の読み取りと書き込み

> **Note**
>
> Amazon SQS、Amazon SNS、DynamoDB の使用量は、ほとんどのリソースとは異なり、時間単位で課金されません。この場合、1 時間の使用量 (DynamoDB での読み取りと書き込みの数など) は、その 1 時間の中で読み取りまたは書き込みがいつ発生したのかに関係なく、異なるテナントに割り当てられた時間のパーセントで分類されます。

次の 3 つのステップで、サービスを Application Cost Profiler と統合します。

1. レポートを有効にして設定する — このステップでは、最終出力の外観を定義します。
2. テナントの使用状況データを Application Cost Profiler に送信する — このステップでは、テナントをテナントのリソース使用時間に関連付ける使用状況データを作成して、その使用状況データを Application Cost Profiler に送信する、サービスのコードが必要です。

3. レポートを取得する - Application Cost Profiler は、レポート設定に指定されている頻度でレポートを提供します。レポートには、各テナントの使用状況に関連付けられたコストが表示され、請求の詳細が表示されます。

これらのステップの詳細については、開始を参照してください。

Application Cost Profiler の使用開始

AWS Application Cost Profiler は、リソース使用状況をリソース全体ではなくテナント別にレポートできるため、AWS リソースに関するコスト情報を取得するのに役立ちます。テナントは、ユーザー、ユーザーのグループ、またはプロジェクトです。選択したテナント別にリソース使用状況を特定できることを確認します。テナントの使用状況に関するコストレポートを取得するには、レポートを設定し、使用状況データを Application Cost Profiler に送信します。このセクションでは、Application Cost Profiler を使用する前に完了する必要がある前提条件について説明します。

トピック

AWS アカウントへのサインアップ

AWS アカウントがない場合は、以下のステップを実行して作成します。

AWS アカウント にサインアップするには

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話のキーパッドを使用して検証コードを入力するように求められます。

   AWS アカウントにサインアップすると、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービスとリソースへのアクセス権があります。セキュリティのベストプラクティスとして、管理ユーザーに管理アクセスを割り当て、ルートユーザーアクセスが必要なタスクを実行する場合にのみ、ルートユーザーを使用してください。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の アカウント をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理ユーザーの作成

AWS アカウントにサインアップした後、日常的なタスクにルートユーザーを使用しないように、管理ユーザーを作成します。

AWS アカウントのルートユーザーをセキュリティで保護する

1. ルートユーザー を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、「AWS サインイン User Guide」の「Signing in as the root user」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の「AWS アカウント のルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理ユーザーを作成する

- 日常的な管理タスクのためには、AWS IAM Identity Center の管理ユーザーに管理アクセスを割り当てます。

  手順については、「AWS IAM Identity Center User Guide」の「Getting started」を参照してください。

管理ユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM アイデンティティセンターのユーザーを使用してサインインする方法については、「AWS サインイン ユーザーガイド」の「AWS アクセスポータルにサインイン」を参照してください。

プログラム的なアクセス権を付与する

AWS Management Console の外部で AWS を操作するには、プログラマチックアクセス権が必要です。プログラマチックアクセス権を付与する方法は、AWS にアクセスしているユーザーのタイプによって異なります。

ユーザーにプログラマチックアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラマチックアクセス権を必要とするユーザー	目的	方法
ワークフォースアイデンティティ (IAM Identity Center で管理されているユーザー)	一時的な認証情報を使用して、AWS CLI、AWS SDK、または AWS API へのプログラマチックリクエストに署名します。	使用するインターフェイス用の手引きに従ってください。 • AWS CLI については、AWS Command Line Interface ユーザーガイドの「AWS IAM Identity Center を使用するための AWS CLI の設定」を参照してください。 • AWS SDK、ツール、および AWS API については、AWS SDK とツールリファレンスガイドの「IAM Identity Center 認証」を参照してください。
IAM	一時的な認証情報を使用して、AWS CLI、AWS SDK、または AWS API へのプログラムによるリクエストに署名します。	IAM ユーザーガイドの「AWS リソースでの一時的な認証情報の使用」の指示に従ってください。
IAM	(非推奨) 長期的な認証情報を使用して、AWS CLI、AWS SDK、AWS API へのプログラ	使用するインターフェイス用の手順に従ってください。

プログラマチックアクセス権を必要とするユーザー	目的	方法
	ムによるリクエストに署名します。	• AWS CLI については、AWS Command Line Interface ユーザーガイドの「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDK とツールについては、AWS SDK とツールリファレンスガイドの「長期認証情報を使用して認証する」を参照してください。 • AWS API については、IAM ユーザーガイドの「IAM ユーザーのアクセスキーの管理」を参照してください。

Application Cost Profiler 固有の前提条件

Application Cost Profiler の使用を開始するには、以下の前提条件を満たす必要があります。

- Cost Explorer を有効にする

  AWS アカウントで AWS Cost Explorer を有効にします。Cost Explorer でアカウントを設定するには最大 24 時間かかります。Application Cost Profiler で日次レポートおよび月次レポートを生成するには、Cost Explorer の設定を完了する必要があります。

  詳細については、AWS Billing and Cost Management ユーザーガイドの Cost Explorer を有効にするを参照してください。
- S3 バケットを作成する

  Amazon Simple Storage Service (Amazon S3) バケットを少なくとも 2 つ作成します。Application Cost Profiler は、片方の S3 バケットを使用してレポートを提供します。もう片方の S3 バケット

を使用して、使用状況データを Application Cost Profiler にアップロードします。通常、使用状況データをアップロードするために必要な S3 バケットは 1 つだけです。ただし、セキュリティのために必要な場合は、複数のS3 バケットを使用し、異なるアクセス許可を用いて別々の S3 バケットで異なるサービスの使用状況を保持できます。Application Cost Profiler に対して、これらの S3 バケットへのアクセス許可を付与する必要があります。

Application Cost Profiler 用の Amazon S3 バケットの設定の詳細については、Application Cost Profiler 用の Amazon S3 バケットの設定を参照してください。

- タグを有効にする

  リソース別ではなくタグ別に使用状況をレポートするには、AWS Billing and Cost Management コンソールでこれらのタグを有効にする必要があります。

  AWS 生成タグのアクティブ化の詳細については、AWS Billing and Cost Management ユーザーガイドの AWS 生成コスト配分タグのアクティブ化を参照してください。ユーザー定義タグのアクティブ化の詳細については、AWS Billing and Cost Management ユーザーガイドのユーザー定義のコスト配分タグのアクティブ化を参照してください。

次のステップ

これらの前提条件を満たしたら、以下を行うことができます。

- レポートを設定して、使用状況データを Application Cost Profiler に送信する。詳細については、「レポートの作成」を参照してください。
- 生成されたレポートを取得して分析する。詳細については、「Application Cost Profiler レポートの使用」を参照してください。

Application Cost Profiler 用の Amazon S3 バケットの設定

AWS Application Cost Profiler に対して使用状況データを送信し、Application Cost Profiler からレポートを受信するためには、データを保存するために AWS アカウントに少なくとも 1 つの Amazon Simple Storage Service (Amazon S3) バケットが必要であり、レポートを受信するために 1 つの S3 バケットが必要です。

> **Note**
>
> AWS Organizations のユーザーの場合、Amazon S3 バケットは、管理アカウントまたは個々のメンバーアカウントのいずれかで使用します。管理アカウントが所有する S3 バケット内のデータは、組織全体のレポートを生成するために使用できます。個々のメンバーアカウントの場合、S3 バケット内のデータは、そのメンバーアカウントのみのレポートを生成するために使用できます。

作成した S3 バケットは、それらのバケットを作成した AWS アカウントによって所有されます。S3 バケットには、標準の Amazon S3 料金が課金されます。Amazon S3 バケットの作成方法の詳細については、Amazon Simple Storage Service ユーザーガイドのバケットの作成を参照してください。

Application Cost Profiler で S3 バケットを使用するためには、バケットに対する読み取りまたは書き込み、あるいはその両方のアクセス許可を Application Cost Profiler に付与するポリシーをバケットにアタッチする必要があります。レポートの設定後にポリシーを変更すると、Application Cost Profiler によって使用状況データの読み取りやレポートの配信を行うことができなくなる可能性があります。

以下のトピックでは、Amazon S3 バケットの作成後に、これらのバケットのアクセス許可を設定する方法について説明します。オブジェクトの読み取り機能と書き込み機能に加えて、バケットを暗号化する場合は、Application Cost Profiler に各バケットの AWS Key Management Service (AWS KMS) キーへのアクセス許可が必要です。

トピック

- Application Cost Profiler にレポート配信 S3 バケットへのアクセス許可を付与する
- Application Cost Profiler に使用状況データ S3 バケットへのアクセス許可を付与する
- Application Cost Profiler に SSE-KMS で暗号化された S3 バケットへのアクセス許可を付与する

Application Cost Profiler にレポート配信 S3 バケットへのアクセス許可を付与する

レポート配信のために Application Cost Profiler に設定する S3 バケットには、Application Cost Profiler に対してレポートオブジェクトの作成を許可するポリシーがアタッチされている必要があります。さらに、暗号化を有効にするように S3 バケットを設定する必要があります。

> **Note**
>
> バケットを作成するときに、バケットの暗号化を選択する必要があります。Amazon S3 によって管理されるキーでバケットを暗号化するのか (SSE-S3)、または AWS KMS で管理される独自のキーでバケットを暗号化するのか (SSE-KMS) を選択できます。暗号化なしでバケットを既に作成した場合、暗号化を追加するためにバケットを編集する必要があります。

Application Cost Profiler にレポート配信 S3 バケットへのアクセス許可を付与するには

1. Amazon S3 コンソールに移動してサインインします。
2. 左側のナビゲーションで [Buckets] (バケット) を選択し、リストからバケットを選択します。
3. [Permissions] (アクセス許可) タブをクリックし、[Bucket policy] (バケットポリシー) をクリックして、[Edit] (編集) をクリックします。
4. [Policy] (ポリシー) セクションで、次のポリシーを挿入します。*<bucket_name>* をユーザーのバケットの名前に、*<AWS #####>* をユーザーの AWS アカウントの ID に置き換えます。

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

```
            }
          }
        }
      ]
    }
```

このポリシーでは、Application Cost Profiler サービスプリンシパル (`application-cost-profiler.amazonaws.com`) に、指定されたバケットにレポートを配信するためのアクセス許可を付与します。この処理はユーザーに代わって実行され、ヘッダーにユーザーの AWS アカウントとレポート配信バケットに固有の ARN が含められます。Application Cost Profiler がユーザーに代わって動作する場合にのみバケットにアクセスできるように、`Condition` はそれらのヘッダーをチェックします。

5. [Save changes] (変更の保存) を選択して、バケットにアタッチされるポリシーを保存します。

   SSE-S3 暗号化を使用してバケットを作成した場合は、完了です。SSE-KMS 暗号化を使用した場合、Application Cost Profiler にバケットへのアクセス許可を付与するために、次の手順が必要です。

6. (オプション) バケットの [プロパティ] タブを選択し、[デフォルトの暗号化] の下で、AWS KMS キーの Amazon リソースネーム (ARN) を選択します。このアクションにより、AWS Key Management Service コンソールが表示されてキーが表示されます。

7. (オプション) Application Cost Profiler に AWS KMS キーへのアクセス許可を付与するためのポリシーを追加します。このポリシーの追加手順については、「Application Cost Profiler に SSE-KMS で暗号化された S3 バケットへのアクセス許可を付与する」を参照してください。

Application Cost Profiler に使用状況データ S3 バケットへのアクセス許可を付与する

使用状況データの読み取り元として Application Cost Profiler に設定する S3 バケットには、Application Cost Profiler に対して使用状況データオブジェクトの読み取りを許可するポリシーがアタッチされている必要があります。

> **Note**
>
> Application Cost Profiler に使用状況データへのアクセス許可を付与することにより、レポート処理中は、これらの使用状況データオブジェクトを米国東部 (バージニア北部) の AWS リージョンに一時的にコピーすることに同意するものとします。これらのデータオブジェク

トは、毎月のレポート生成が完了するまで、米国東部 (バージニア北部) リージョンに保持されます。

Application Cost Profiler に使用状況データ S3 バケットへのアクセス許可を付与するには

1. Amazon S3 コンソールに移動してサインインします。
2. 左側のナビゲーションで [Buckets] (バケット) を選択し、リストからバケットを選択します。
3. [Permissions] (アクセス許可) タブをクリックし、[Bucket policy] (バケットポリシー) をクリックして、[Edit] (編集) をクリックします。
4. [Policy] (ポリシー) セクションで、次のポリシーを挿入します。*<bucket-name>* をユーザーのバケットの名前に、*<AWS #####>* をユーザーの AWS アカウントの ID に置き換えます。

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

このポリシーでは、Application Cost Profiler サービスプリンシパル (`application-cost-profiler.amazonaws.com`) に、指定されたバケットからデータを取得するためのアクセス許可を付与します。この処理はユーザーに代わって実行され、ヘッダーにユーザーの AWS アカウントと使用状況バケットに固有の ARN が含められます。Application Cost Profiler がユーザーに代わって動作する場合にのみバケットにアクセスできるように、`Condition` はそれらのヘッダーをチェックします。

5. [Save changes] (変更の保存) を選択して、バケットにアタッチされるポリシーを保存します。

AWS KMS マネージドキーでバケットを暗号化する場合、次のセクションの手順に従って、Application Cost Profiler にバケットへのアクセス許可を付与する必要があります。

Application Cost Profiler に SSE-KMS で暗号化された S3 バケットへのアクセス許可を付与する

Application Cost Profiler 用に設定した S3 バケット (レポートバケットとして必要) を AWS KMS (SSE-KMS) に保存されたキーで暗号化する場合、Application Cost Profiler にこれらのバケットを復号するためのアクセス許可も付与する必要があります。これを行うには、データの暗号化に使用した AWS KMS キーへのアクセス許可を付与します。

> **Note**
>
> バケットが Amazon S3 マネージドキーで暗号化される場合は、この手順を実行する必要はありません。

SSE-KMS で暗号化された S3 バケット用に Application Cost Profiler に AWS KMS へのアクセス許可を付与する

1. AWS KMS コンソールに移動してサインインします。
2. 左側のナビゲーションで [Customer managed keys] (カスタマーマネージドキー) を選択し、リストからバケットの暗号化に使用するキーを選択します。
3. [Switch to policy view] (ポリシービューへの切り替え) を選択し、[Edit] (編集) をクリック」します。
4. [Policy] (ポリシー) セクションで、次のポリシーステートメントを挿入します。

```
{
```

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

5. [Save changes] (変更の保存) を選択して、キーにアタッチされるポリシーを保存します。
6. Application Cost Profiler がアクセスする必要がある S3 バケットを暗号化する各キーに対して手順を繰り返します。

> **Note**
>
> データは、インポート時に S3 バケットから (暗号化されている) Application Cost Profiler マネージドバケットにコピーされます。キーへのアクセス許可を取り消すと、Application Cost Profiler はバケットから新しいオブジェクトを取得できなくなります。ただし、インポート済みのデータは引き続きレポートの生成に使用できます。

レポートの作成

前提条件を満たしたら、AWS アカウントのレポートを設定して使用状況データを AWS Application Cost Profiler に送信する準備をします。このセクションでは、レポートを設定する方法、および使用状況データを Application Cost Profiler に送信する方法について説明します。

Application Cost Profiler レポートの設定

次の手順で、使用状況データに基づいて生成するレポートを設定する方法を示します。レポートを生成する頻度などの詳細を設定します。

> **Note**
>
> AWS アカウントが AWS 組織に含まれている場合、管理アカウントまたは個々のメンバーアカウントのいずれかを使用してレポートを設定できます。個々のアカウントに対して設定されたレポートには、そのアカウントのデータのみが含まれます。管理アカウントを使用して設定されたレポートには、組織全体のデータを含めることができます。
> レポート出力に使用される Amazon S3 バケットは、レポート設定を作成するアカウントに属している必要があります。

Application Cost Profiler レポートを設定するには

1. Web ブラウザを開き、Application Cost Profiler コンソールにサインインします。
2. [Get started now] (今すぐ始める) をクリックして、レポートを設定または変更します。
3. レポートの [レポート名] および [レポートの説明] を入力します。
4. [S3 バケット名を入力] フィールドに S3 バケットの名前を入力し、[S3 プレフィックスを入力] フィールドに S3 プレフィックスを入力します。S3 バケットの作成および Application Cost Profiler へのアクセス許可の付与の詳細については、「Application Cost Profiler 用の Amazon S3 バケットの設定」を参照してください。
5. レポートに使用するオプションを選択します。

   - [時間頻度] — レポートを生成する頻度として [毎日]、[毎月]、[両方] のいずれかを選択します。
   - [レポート出力形式] — Amazon S3 バケット内に作成するファイルのタイプを選択します。[CSV] を選択すると、Application Cost Profiler によって、レポートに gzip 圧縮を使用し

たカンマ区切り値のテキストファイルが作成されます。[Parquet] を選択すると、レポートに Parquet ファイルが生成されます。

6. [Configure] (設定) を選択してレポート設定を保存します。

> **Note**
>
> AWS Application Cost Profiler API を使用してレポートを設定することもできます。

[今すぐ始める] をクリックして現在のレポート設定を表示し、レポート設定を確認します。

> **Note**
>
> 設定できるレポートは 1 つのみです。設定ページに戻ると、既存のレポートが編集されます。

レポートを設定した後で、データの取り込みが有効になります。サービスを Application Cost Profiler と統合して、リソースの使用状況データを提供できます。

サービスのテナント使用状況データのレポート

レポートを設定したら、アカウントのリソースまたはサービスのテナント使用状況データを送信する準備ができます。リソースが特定のテナントで使用されている場合は、Application Cost Profiler に通知する必要があります。例えば、異なるテナントからの API コールをサービスが受け入れる場合、そのテナントからの API コールを開始および終了するときに、各テナントの開始時刻と終了時刻を記録します。Application Cost Profiler は、そのデータを使用して、各テナントの作業に費やされた時間ごとにサービスのコストに関するレポートを生成します。

Application Cost Profiler に使用状況データを提供するには、次の操作を行います。

- リソース使用状況データの準備 — 特定のテナントでリソースがいつ使用されるかを説明するテーブルを作成します。
- 使用状況データのアップロード — Application Cost Profiler にアクセス許可を付与した Amazon S3 バケットにテーブルをアップロードします。
- 使用状況データのインポート — `ImportApplicationUsage` API オペレーションを呼び出して、Application Cost Profiler にデータの処理準備が整ったことを通知します。

以下のセクションで、これらの各手順について詳しく説明します。

トピック

ステップ 1: リソース使用状況データの準備

サービスでリソースが使用されているときに、どのテナントがそのリソースを使用しているかを追跡します。このデータをテーブルに記録します。このテーブルを後でアップロードして、Application Cost Profiler にインポートできるようにします。テーブル内の各行に、リソース、そのリソースを使用しているテナント、およびその使用の開始時刻と終了時刻が示されます。リソースの例としては、使用されている Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなどがあります。

このステップでは、使用状況に関する正しい情報を出力するために、コードをサービスに統合する必要があります。

次の表に、リソース使用状況テーブル内のフィールドの一覧を示します。

フィールド	説明
ApplicationId	システム内の使用されているアプリケーションまたは製品を識別します。テナントメタデータの範囲を定義します。
TenantId	指定されたリソースを消費するテナントのシステム内の識別子。Application Cost Profiler は、ApplicationId 内でこのレベルに集計します。
TenantDesc	(オプション) 独自の追加レポートのテナントに関する追加データ。
UsageAccountId	リソースを実行するアカウント (組織に含まれているアカウントの場合に重要)。

フィールド	説明
StartTime	エポックからのミリ秒およびマイクロ秒単位のタイムスタンプ (UTC)。指定されたテナントによる使用期間の開始時刻を示します。
EndTime	エポックからのミリ秒およびマイクロ秒単位のタイムスタンプ (UTC)。指定されたテナントによる使用期間の終了時刻を示します。
ResourceId	使用されているリソースの Amazon リソースネーム (ARN)。
名前	(オプション) [ResourceId] を指定する代わりに、[Name] (名前) リソースタグを指定して、コストがリソースセットに帰属させることができるようになります (フィールドに、[Name] (名前) タグに使用する値が含まれている必要あり)。リソースタグは、コストと使用状況レポートの一部として有効になります。リソースタグの詳細については、コストと使用状況レポートユーザーガイドの「リソースタグの詳細」を参照してください。

出力は、次の例に示すように、見出し行を含むカンマ区切り値 (.csv) ファイルに含まれている必要があります。

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

データを .csv 拡張子のファイルとして保存します (gzip で圧縮する場合は .csv.gzip)。このデータを Application Cost Profiler にアップロードすると、各タイムスライスは関連付けられたテナントに割り当てられます。この例では、レポートには、そのテナントの Amazon EC2 インスタンスコストのタイムスライスが含まれます。Amazon EC2 インスタンスの場合にのみ、特定のテナントに関連付けられていないスライスは属性なしのテナントに追加されます。オーバーラップするタイムスライスは複数回カウントされます。使用状況テーブルのデータが正確であることを確認するのは、ユーザーの責任です。

> **Note**
>
> ファイルは 1 時間に相当する必要があります。リソースが数時間使用される場合は、1 時間で使用状況が終了し、それと同時に次のファイルで新しいレコードが開始されます。
> 1 時間分のデータを含む 1 つのファイルを送信する必要があります。同じ時間のデータに対して複数のファイルが送信された場合、Application Cost Profiler は最新のファイルのデータのみを考慮します。

例えば、次の表は、指定されたタイムスライスに基づいて、1 時間 (3,600,000 ミリ秒) における 3 つのテナントの使用状況を Application Cost Profiler が計算する方法を示しています。

テナント	指定されたタイムスライス	計算された 1 時間あたりのコストのパーセント
Tenant1	1,200,000 ms	33.34%
Tenant2	600,000 ms	16.66%
<unattributed>		50.00%

この例では、Tenant1 には 1 時間の 3 分の 1 が割り当てられ、Tenant2 には 1 時間の 6 分の 1 が割り当てられています。1 時間の 50% である残りの 30 分 (1,800,000 ミリ秒) は、どちらのクライアントにも帰属しません。

現在、Application Cost Profiler では以下のリソースが有効になっています。

- Amazon EC2 インスタンス (オンデマンドインスタンスとスポットインスタンスのみ)
- Lambda 関数 (Lambda 関数のデータを送信する場合は、`ResourceId` として非修飾リソース ARN を送信する必要があります)

- Amazon Elastic Container Service (Amazon ECS) インスタンス
- Amazon Simple Queue Service (Amazon SQS) キュー
- Amazon Simple Notification Service (Amazon SNS) のトピック
- Amazon DynamoDB の読み取りと書き込み

> **Note**
>
> Amazon SQS、Amazon SNS、DynamoDB の使用量は、ほとんどのリソースとは異なり、時間単位で課金されません。この場合、1 時間の使用量 (DynamoDB での読み取りと書き込みの数など) は、その 1 時間の中で読み取りまたは書き込みがいつ発生したのかに関係なく、異なるテナントに割り当てられた時間のパーセントで分類されます。

ステップ 2: リソース使用状況のアップロード

テナントごとの使用状況のファイルを取得したら、データファイルを Amazon S3 にアップロードし、Application Cost Profiler がそのファイルへのアクセス許可を持っていることを確認します。

S3 バケットの作成の詳細については、「Application Cost Profiler 固有の前提条件」を参照してください。

Application Cost Profiler が S3 バケットにアクセスできることを確認する必要があります。これは S3 バケットごとに 1 回だけ行う必要があります (同じバケットを再利用して複数の使用状況ファイルをアップロードできます)。バケットへのアクセス許可の付与については、Application Cost Profiler に使用状況データ S3 バケットへのアクセス許可を付与するを参照してください。バケットが暗号化されている場合は、「Application Cost Profiler に SSE-KMS で暗号化された S3 バケットへのアクセス許可を付与する」を参照してください。

> **Note**
>
> 使用状況データに使用する S3 バケットを暗号化する必要はありません。

データを .csv 拡張子 (gzip で圧縮する場合は .csv.gzip) のファイルとして S3 バケットに 1 時間間隔でアップロードします。新しいファイルをアップロードした後、ファイルをレポートにインポートできるように、アップロードしたことを Application Cost Profiler に通知する必要があります。

> **Note**
>
> Application Cost Profiler に使用状況データへのアクセス許可を付与することにより、レポート処理中は、これらの使用状況データオブジェクトを米国東部 (バージニア北部) の AWS リージョンに一時的にコピーすることに同意するものとします。これらのデータオブジェクトは、毎月のレポート生成が完了するまで、米国東部 (バージニア北部) リージョンに保持されます。

ステップ 3: Application Cost Profiler への使用状況データのインポート

Application Cost Profiler がアクセスできる Amazon S3 バケットに使用状況データをアップロードしたら、そのデータが存在すること、および最終レポートにインポートするように Application Cost Profiler に通知します。そのためには、Application Cost Profiler API で `ImportApplicationUsage` オペレーションを使用します。

`ImportApplicationUsage` オペレーションを含め、AWS Application Cost Profiler API の詳細については、「AWS Application Cost Profiler API リファレンス」を参照してください。

次の例は、`ImportApplicationUsage` を呼び出す方法を示しています。`##########`を、S3 バケットの値およびアップロードされたオブジェクトの値に置き換えてください。

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

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

> **Note**
>
> `region` パラメータが必要になるのは、デフォルトで無効になっている AWS リージョンにバケットがある場合のみです。詳細については、「AWS 全般のリファレンス」の「Managing AWS リージョン」を参照してください。

`ImportApplicationUsage` でインポートしたデータを使用し、レポートを設定したときにリクエストした頻度で、Application Cost Profiler によって新しいレポートが生成されます。

レポートを設定し、Application Cost Profiler への使用状況データのインポートを自動化したら、生成されたレポートを表示できます。レポートの詳細については、「Application Cost Profiler レポートの使用」を参照してください。

Application Cost Profiler レポートの使用

使用状況データを AWS Application Cost Profiler と統合し、1 時間ごとにデータを送信すると、Application Cost Profiler によって自動的にレポートが生成されます。

レポートは、レポートを設定したときに選択したオプションに基づいて、毎日または毎月のいずれかで生成されます。レポートは、レポートを設定したときに選択した Amazon Simple Storage Service (Amazon S3) バケットに配信されます。

毎月 1 日に生成される日次レポートには、前月のデータが含まれます。

Application Cost Profiler レポートで使用可能なデータ

使用状況レポートに作成される列を次の表に示します。

列名	説明
PayerAccountId	組織内の管理アカウント ID。アカウントが AWS Organizations に属していない場合は、アカウント ID。
UsageAccountId	使用のあるアカウントのアカウント ID。
LineItemType	レコードのタイプ。常に Usage になります。
UsageStartTime	エポックからのミリ秒単位のタイムスタンプ (UTC)。指定されたテナントによる使用期間の開始時刻を示します。
UsageEndTime	エポックからのミリ秒単位のタイムスタンプ (UTC)。指定されたテナントによる使用期間の終了時刻を示します。
ApplicationIdentifier	Application Cost Profiler に送信される使用状況データに指定される ApplicationId。
TenantIdentifier	Application Cost Profiler に送信される使用状況データに指定される TenantId。使用状況デー

列名	説明
	タ内のレコードのないデータは、unattributed で収集されます。
TenantDescription	Application Cost Profiler に送信される使用状況データに指定される TenantDesc 。
ProductCode	請求対象の AWS 製品 (例: AmazonEC2)。
UsageType	請求対象の使用タイプ (例: BoxUsage:c5.large)。
操作	請求対象のオペレーション (例: RunInstances)。
ResourceId	請求対象のリソースのリソース ID または Amazon リソースネーム (ARN)。
ScaleFactor	リソースが 1 時間の割り当て超過である場合、例えば、レポートされる使用状況データが 1 時間ではなく 2 時間である場合、合計が実際の請求額と等しくなるようにスケール係数が適用されます (この場合は 0.5)。この列は、その 1 時間に特定のリソースに使用されたスケール係数をレポートします。スケール係数は常にゼロ (0) より大きく、1 以下です。
TenantAttributionPercent	指定されたテナントに帰属する使用の割合 (ゼロ (0) ~ 1)。
UsageAmount	指定されたテナントに帰属する使用量。
CurrencyCode	レートとコストに使用する通貨 (例: USD)。
Rate	ユニットあたりの使用量の請求レート。
TenantCost	指定されたテナントでのそのリソースの合計コスト。

列名	説明
[Region] (リージョン)	リソースの AWS リージョン。
名前	コストと使用状況レポートまたはリソース使用状況データを使用して、リソースのリソースタグを作成した場合、Name タグはここに表示されます。リソースタグの詳細については、コストと使用状況レポートユーザーガイドの「リソースタグの詳細」を参照してください。

以下は、2 時間での 1 リソースの出力レポートの例です。

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

この例では、最初の 1 時間のうち半分の時間が Tenant1 に割り当てられています。残りの半分の時間は unattributed のままになっています。2 番目の 1 時間では、4 つのテナントすべてに 1 時間すべてが割り当てられています。この場合、スケール係数はそれらすべてを 0.25 ずつスケールダウンし、すべてに 1 時間の 4 分の 1 が割り当てられています。最終コストは、TenantCost 列で確認できます。

AWS Application Cost Profiler のクォータとエンドポイント

AWS アカウントには、AWS のサービスごとにデフォルトのクォータ (以前は制限と呼ばれていました) があります。特に明記されていない限り、各クォータは AWS リージョン固有です。一部のクォータについては引き上げをリクエストできますが、その他のクォータについてはリクエストできません。

次の表は、アカウントあたりのService Quotas および Application Cost Profiler の AWS リージョンエンドポイントを示しています。

Service Quotas

リソース	デフォルト値	説明
PutReportDefinition リクエストのレート	5	アカウントあたり、1 秒あたりの最大 PutReportDefinition リクエスト数。
UpdateReportDefinition リクエストのレート	5	アカウントあたり、1 秒あたりの最大 UpdateReportDefinition リクエスト数。
GetReportDefinition リクエストのレート	5	アカウントあたり、1 秒あたりの最大 GetReportDefinition リクエスト数。
DeleteReportDefinition リクエストのレート	5	アカウントあたり、1 秒あたりの最大 DeleteReportDefinition リクエスト数。
ListReportDefinitions リクエストのレート	5	アカウントあたり、1 秒あたりの最大 ListRepor

リソース	デフォルト値	説明
		tDefinitions リクエスト数。
ImportApplicationUsage リクエストのレート	5	アカウントあたり、1 秒あたりの最大 ImportApplicationUsage リクエスト数。
使用状況データファイルの最大サイズ	10 MB	時間単位の使用状況データファイルの最大サイズ。

サービスエンドポイント

Application Cost Profiler はグローバルサービスです。すべての API コールを米国東部 (バージニア北部) エンドポイントに対して行う必要があります。

- 米国東部 (バージニア北部) – application-cost-profiler.us-east-1.amazonaws.com

AWS Application Cost Profiler でのセキュリティ

AWS では、クラウドのセキュリティが最優先事項です。AWS の顧客は、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利点を得られます。

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 は、AWS クラウドで AWS の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を負います。また、AWS は、使用するサービスを安全に提供します。AWS 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が定期的にセキュリティの有効性をテストおよび検証しています。Application Cost Profiler 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 – お客様の責任範囲は、ご使用の AWS のサービスに応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、AWS Application Cost Profiler 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。ここでは、セキュリティとコンプライアンスの目標を満たすように Application Cost Profiler を設定する方法について説明します。また、Application Cost Profiler リソースのモニタリングや安全性の確保に役立つ他の AWS サービスの使用方法についても説明します。

目次

AWS Application Cost Profiler でのデータ保護

AWS 責任共有モデルは、AWS Application Cost Profiler 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 には、AWS クラウド のすべて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。ユーザーには、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。このコンテンツには、使用される AWS のサービスのセキュリティ構成と管理タスクが含まれます。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「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。

データを保護するため、AWS アカウント の認証情報を保護し、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セットアップ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を各ユーザーに付与できます。また、次の方法でデータを保護することをおすすめします。

- 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 が必須です。TLS 1.3 が推奨されます。
- AWS CloudTrail で API とユーザーアクティビティロギングをセットアップします。
- AWS のサービス内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- 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 により AWS にアクセスするときに FIPS 140-2 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) 140-2」を参照してください。

お客様の E メールアドレスなどの機密情報やセンシティブ情報は、タグや名前フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これには、コンソール、API、AWS CLI、または AWS SDK を用いた Application Cost Profiler またはその他 AWS のサービスの使用時が含まれます。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。

保管中の暗号化

AWS Application Cost Profiler は、追加の設定なしに、サービスに保管されるすべてのデータを常に保管時に暗号化します。この暗号化は、Application Cost Profiler を使用する場合は自動的に行われます。

提供する Amazon S3 バケットに対して、レポートバケットを暗号化する必要があります。使用状況データバケットを暗号化し、Application Cost Profiler にアクセス許可を付与できます。詳細については、「Application Cost Profiler 用の Amazon S3 バケットの設定」を参照してください。

転送中の暗号化

AWS Application Cost Profiler は、転送時の暗号化のために、Transport Layer Security (TLS) とクライアント側の暗号化を使用します。Application Cost Profiler との通信は常に HTTPS を介して行われるため、データは転送時に常に暗号化されます。この暗号化は、Application Cost Profiler を使用する場合はデフォルトで設定されます。

AWS Application Cost Profiler の Identity and Access Management

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するために役立つ AWS のサービス です。IAM 管理者は、Application Cost Profiler リソースの使用についてどのユーザーを認証し(サインインさせ)、許可する (アクセス許可を持たせる) かを制御します。IAM は、追加費用なしで使用できる 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、Application Cost Profiler で行う作業によって異なります。

サービスユーザー – 業務を行うために Application Cost Profiler サービスを使用する場合は、管理者から必要な認証情報とアクセス許可が与えられます。作業を行うためにさらに多くの Application Cost Profiler 機能を使用する場合は、追加のアクセス許可が必要になることがあります。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。Application

Cost Profiler の機能にアクセスできない場合は、AWS Application Cost Profiler の Identity and Access 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 – 社内で Application Cost Profiler リソースを担当している場合は、おそらく Application Cost Profiler へのフルアクセスがあります。サービスユーザーが Application Cost Profiler のどの機能とリソースにアクセスする必要があるかを決定するのは、サービス管理者の仕事です。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 Application Cost Profiler で IAM を使用する方法の詳細については、AWS Application Cost Profiler で IAM を使用する方法を参照してください。

IAM 管理者 – IAM 管理者である場合は、Application Cost Profiler 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 Application Cost Profiler のアイデンティティベースのポリシーの例を確認するには、AWS Application Cost Profiler の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。

アイデンティティによる認証

認証とは、アイデンティティ認証情報を使用して AWSにサインインする方法です。ユーザーは、AWS アカウントのルートユーザー として、または IAM ロールを引き受けることによって、認証済み (AWS にサインイン済み) である必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。 AWS IAM Identity Centerフェデレーティッドアイデンティティの例としては、IAM アイデンティティセンターユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報などがあります。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。フェデレーションを使用して AWSにアクセスする場合、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。AWS へのサインインの詳細については、『AWS サインイン ユーザーガイド』の「AWS アカウント にサインインする方法」を参照してください。

プログラムで AWS にアクセスする場合、AWS は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) を提供し、認証情報で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。リクエストに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「AWS API 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、追加のセキュリティ情報の提供が求めら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高めることを推奨しています。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「AWS での多要素認証 (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

AWS アカウント を作成する場合、このアカウントのすべての AWS のサービス とリソースに対して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。このアイデンティティは AWS アカウントの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によってアクセスできます。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を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行してください。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、1 人のユーザーまたは 1 つのアプリケーションに対して特定の許可を持つ AWS アカウント 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、特定の許可を持つ、AWS アカウント 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ことにより、AWS Management Console で一時的に IAM ロールを引き受けることができます。ロールを引き受けるには、AWS CLI または AWS API 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、次のような状況で役立ちます。

- フェデレーティッドユーザーアクセス - 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「サードパーティアイデンティティプロバイダー用のロールの作成」を参照してください。IAM Identity Center を使用する場合、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 アイデンティティセンターは、アクセス許可セットを 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へのアクセスを別のアカウントの人物 (信頼できるプリンシパル) 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 AWS のサービスでは、(ロールをプロキシとして使用する代わりに) リソースにポリシーを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 AWS のサービスでは、他の AWS のサービスの機能を使用します。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、またはサービスリンクロールを使用してこれを行う場合があります。
  - プリンシパル権限 - IAM ユーザーまたはロールを使用して AWS でアクションを実行する場合、そのユーザーはプリンシパルと見なされます。ポリシーによって、プリンシパルに権限が付与されます。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により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。この場合、両方のアクションを実行するための権

限が必要です。アクションにポリシーで追加の依存アクションが必要かどうかを確認するには、サービス認証リファレンスの AWS のサービスのアクション、リソース、および条件キー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 に権限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、AWS のサービス にリンクされたサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの許可を表示できますが、編集はできません。

- Amazon EC2 で実行されているアプリケーション - EC2 インスタンスで実行され、AWS CLI または AWS API 要求を行っているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用できます。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、インスタンスに添付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 ロールを使用してアクセス許可を付与する」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権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS アイデンティティまたはリソースにアタッチします。ポリシーは AWS のオブジェクトであり、アイデンティティやリソースに関連付けて、これらのアクセス許可を定義します。AWS 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、これらのポリシーを評価します。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。大半のポリシーは JSON ドキュメントとして AWS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 AWSJSON ポリシーを使用して、だれ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アクセス許可をユーザーに付与するため、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。このポリシーがあるユーザーは、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、および条件を制御します。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ます。管理ポリシーは、AWS アカウント 内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。マネージドポリシーには、AWS マネージドポリシーとカスタマー管理ポリシーがあります。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の例には、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあります。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、フェデレーションユーザー、または AWS のサービス を含めることができます。

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は使用できません。

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、ACL をサポートするサービスの例です。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 では、他の一般的ではないポリシータイプをサポートしています。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る最大の許可を設定できます。

- 権限の境界 - 権限の境界は、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) に付与できる許可の上限を設定する高度な機能です。エンティティに権限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権限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、権限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。権限の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの権限の境界」を参照してください。
- サービスコントロールポリシー (SCP) - SCP は、AWS Organizations で組織や組織単位 (OU) の最大許可を指定する JSON ポリシーです。AWS Organizations は、ユーザーの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、一元的に管理するサービスです。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 はメンバーアカウントのエンティティに対する権限を制限します (各 AWS アカウントのルートユーザー など)。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ティッド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の範囲は、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」をご参照ください。

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連するとき、リクエストを許可するかどうかを AWS が決定する方法の詳細については、『IAM ユーザーガイド』の「ポリシーの評価ロジック」を参照してください。

AWS Application Cost Profiler で IAM を使用する方法

IAM を使用して Application Cost Profiler へのアクセスを管理するには、Application Cost Profiler で使用できる IAM 機能を理解しておく必要があります。Application Cost Profiler およびその他の AWS のサービスと IAM との連携の概要については、IAM ユーザーガイドの IAM と連携する AWS のサービスを参照してください。

トピック

- Application Cost Profiler のアイデンティティベースのポリシー
- Application Cost Profiler のリソースベースのポリシー
- Application Cost Profiler タグに基づいた許可
- Application Cost Profiler の IAM ロール

Application Cost Profiler のアイデンティティベースのポリシー

IAM のアイデンティティベースのポリシーでは、アクションを許可または拒否する条件に加えて、許可または拒否するアクションとリソースを指定できます。Application Cost Profiler は、特定のアクション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、関連する 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。

Application Cost Profiler のポリシーアクションは、アクションの前にプレフィックス `application-cost-profiler:` を使用します。例えば、Application Cost Profiler レポート定義の詳細を表示するアクセス許可を他のユーザーに付与するには、ポリシーに `application-cost-profiler:GetReportDefinition` 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` 要素を含める必要があります。Application Cost Profiler は、このサービスで実行できるタスクを記述する、独自の一連のアクションを定義します。

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

以下に、Application Cost Profiler で使用できるアクションを示します。それぞれが、同じ名前の API アクションを許可します。Application Cost Profiler API の詳細については、「AWS Application Cost Profiler API リファレンス」を参照してください。

- `application-cost-profiler:ListReportDefinitions` — AWS アカウントのレポート定義 (存在する場合) の一覧表示を許可します。
- `application-cost-profiler:GetReportDefinition` – Application Cost Profiler レポートのレポート定義詳細の取得を許可します。
- `application-cost-profiler:PutReportDefinition` – 新しいレポート定義の作成を許可します。
- `application-cost-profiler:UpdateReportDefinition` – レポート定義の更新を許可します。
- `application-cost-profiler:DeleteReportDefinition` – レポートの削除を許可します (Application Cost Profiler API でのみ使用可能)。
- `application-cost-profiler:ImportApplicationUsage` — 指定された Amazon S3 バケットからの使用状況データのインポートを Application Cost Profiler にリクエストすることを許可します。

リソース

Application Cost Profiler では、ポリシーでリソースの Amazon リソースネーム (ARN) を指定することはできません。

条件キー

Application Cost Profiler にはサービス固有の条件キーがありませんが、いくつかのグローバル条件キーの使用がサポートされています。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。

例

Application Cost Profiler のアイデンティティベースのポリシーの例については、AWS Application Cost Profiler の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。

Application Cost Profiler のリソースベースのポリシー

Application Cost Profiler は、リソースベースのポリシーをサポートしていません。

Application Cost Profiler タグに基づいた許可

Application Cost Profiler は、リソースのタグ付けやタグに基づいたアクセスの制御をサポートしていません。

Application Cost Profiler の IAM ロール

IAM ロールは AWS アカウント内のエンティティで、特定の許可を持っています。

Application Cost Profiler 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 GetFederationToken などの AWS STS API オペレーションを呼び出します。

Application Cost Profiler は、一時的な認証情報の使用をサポートしています。

サービスにリンクされたロール

サービスリンクロールは、AWS サービスが他のサービスのリソースにアクセスしてお客様の代わりにアクションを完了することを許可します。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。 管理者は、サービスにリンクされた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。

Application Cost Profiler は、サービスにリンクされたロールをサポートしていません。

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、 管理者は、このロールのアクセス許可を変更できます。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。

Application Cost Profiler は、サービスロールをサポートしていません。

AWS Application Cost Profiler の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、AWS Application Cost Profiler リソースを作成または変更するためのアクセス許可はありません。また、AWS Management Console や AWS Command Line Interface (AWS CLI)、AWS API を使用してタスクを実行することもできません。管理者は、必要な特定の API 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
- Application Cost Profiler コンソールの使用
- ユーザーが自分の許可を表示できるようにする
- 1 つの Amazon S3 バケットへのアクセス

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、ユーザーのアカウントで誰かが Application Cost Profiler リソースを作成、アクセス、または削除できるどうかを決定します。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の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 マネージドポリシーを使用して開始し、最小特権の権限に移行する – ユーザーとワークロードへの権限の付与を開始するには、多くの一般的なユースケースのために権限を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに応じた AWS カスタマー管理ポリシーを定義することで、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 ポリシーで許可を設定するときは、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、最小特権権限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。また、AWS のサービス など特定の AWS CloudFormation を介して使用する場合、条件を使用して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。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 アクセスアナライザーを使用して IAM ポリシーを検証し、安全で機能的な許可を確保する - IAM アクセスアナライザーは、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 アクセスアナライザーによるポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する - AWS アカウント で IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。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。

Application Cost Profiler コンソールの使用

AWS Application Cost Profiler コンソールにアクセスするには、一連の最小限のアクセス許可が必要です。これらのアクセス許可により、AWS アカウントの Application Cost Profiler リソースの詳細をリストおよび表示できます。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 Application Cost Profiler コンソールを使用して AWS アカウントの Application Cost Profiler レポート定義を表示できるようにするには、次のアクセス許可をエンティティにアタッチします。

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

例えば、読み取り専用ユーザーに対して次のポリシーを作成できます。

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

詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

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。

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を、IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了する権限が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

1 つの Amazon S3 バケットへのアクセス

この例では、AWS アカウントの IAM ユーザーに Amazon S3 バケットの 1 つである examplebucket へのアクセスを付与します。また、ユーザーがオブジェクトを追加、更新、および削除できるようにします。

このポリシーでは、ユーザーに s3:PutObject、s3:GetObject、s3:DeleteObject のアクセス許可を付与するだけでなく、s3:ListAllMyBuckets、s3:GetBucketLocation、および s3:ListBucket のアクセス許可も付与します。これらが、コンソールで必要とされる追加のアクセス許可です。またコンソール内のオブジェクトのコピー、カット、貼り付けを行うためには、s3:PutObjectAcl および s3:GetObjectAcl アクションが必要となります。コンソールを使用して、ユーザーにアクセス許可を付与し、テストする例の解説については、「チュートリアル例: ユーザーポリシーを使用したバケットへのアクセスのコントロール」を参照してください。

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

```
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

AWS Application Cost Profiler の Identity and Access のトラブルシューティング

次の情報は、AWS Application Cost Profiler および AWS Identity and Access Management (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

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

Application Cost Profiler でアクションを実行する権限がありません

AWS Management Console から、アクションを実行する権限がないと通知された場合は、管理者に問い合わせてサポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当者です。

以下のエラー例は、`mateojackson` IAM ユーザーがコンソールを使用して Application Cost Profiler レポートの詳細を表示しようとする際に `application-cost-profiler:ListReportDefinitions` 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:
 application-cost-profiler:ListReportDefinitions on resource: Report Definition
```

この場合、Mateo は、`application-cost-profiler:ListReportDefinitions` アクションを使用してレポート定義リソースにアクセスできるように、ポリシーの更新を管理者に依頼します。

iam を実行する権限がない：PassRole

`iam:PassRole` アクションを実行する権限が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 Application Cost Profiler 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やサービスリンクロールを作成せずに、既存のロールをサービスに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。

以下のエラー例は、marymajor という名前の IAM ユーザーがコンソールを使用して Application Cost Profiler でアクションを実行しようと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 Mary 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 管理者に問い合わせてください。管理者とは、サインイン認証情報を提供した担当者です。

自分の AWS アカウント以外のユーザーに Application Cost Profiler 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制御リスト (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:

- Application Cost Profiler がこれらの機能をサポートしているかどうかについては、AWS Application Cost Profiler で IAM を使用する方法を参照してください。
- 所有している AWS アカウント 全体のリソースへのアクセス権を提供する方法については、『IAM ユーザーガイド』の「所有している別の AWS アカウント アカウントへのアクセス権を IAM ユーザーに提供」を参照してください。
- サードパーティーの AWS アカウント にリソースへのアクセス権を提供する方法については、「IAM ユーザーガイド」の「サードパーティーが所有する AWS アカウント にアクセス権を提供する」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 Application Cost Profiler のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「コンプライアンスプログラム別の範囲」の「AWS のサービス」と「」の「AWS のサービス」を参照し、関心のあるコンプライアンスプログラムを選択してください。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。

AWS Artifact 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。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

AWS のサービスを使用する際のユーザーのコンプライアンス責任は、ユーザーのデータの機密性や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。AWS では、コンプライアンスに役立つ次のリソースを提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド - これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、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 AWS にデプロイするための手順を示します。
- 「Amazon Web Services での HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ」 - このホワイトペーパーは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法を説明しています。

> **Note**
>
> すべての AWS のサービスが HIPAA 適格であるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスのリソース - このワークブックおよびガイドのコレクションは、顧客の業界と拠点に適用されるものである場合があります。
- 「AWS Config デベロッパーガイド」の「ルールでのリソースの評価」 - AWS Config サービスは、リソース設定が社内慣行、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 Security Hub - この AWS のサービスは、AWS 内のセキュリティ状態の包括的なビューを提供します。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セ

キュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。

- AWS Audit Manager - この AWS のサービスは、AWS の使用状況を継続的に監査して、リスクの管理方法や、規制および業界標準へのコンプライアンスの管理方法を簡素化するために役立ちます。

AWS Application Cost Profiler での耐障害性

AWS の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として構築されます。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。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、耐障害性、および拡張性が優れています。

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 Application Cost Profiler で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 Application Cost Profiler 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 AWS がインフラストラクチャ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「インフラストラクチャ保護」を参照してください。

ユーザーは、AWS が公開している API コールを使用して、ネットワーク経由で Application Cost Profiler 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 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、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。

EventBridge での Application Cost Profiler イベントの監視

Amazon EventBridge を使用すると、AWS のサービスを自動化し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に対応できます。AWS サービスからのイベントは、ほぼリアルタイムで EventBridge に配信されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。詳細については、Amazon EventBridge ユーザーガイドを参照してください。

EventBridge で AWS Application Cost Profiler イベントを監視できます。EventBridge は、そのデータを AWS Lambda や Amazon Simple Notification Service (Amazon SNS) などのターゲットにルーティングします。これらのイベントは、Amazon CloudWatch Events に表示されるイベントと同じで、AWS リソースの変更を示すシステムイベントのほぼリアルタイムのストリームを提供します。

EventBridge によるレポート生成の監視

EventBridge を使用すると、生成されるレポートの通知を Application Cost Profiler が送信するときに実行するアクションを定義するルールを作成できます。例えば、レポートが生成されるたびに E メールメッセージを送信するルールを作成できます。

レポート生成を監視するには

1. EventBridge と Application Cost Profiler の両方を使用するアクセス許可を持つアカウントを使用して AWS にログインします。
2. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
3. 次の値を使用して、レポート生成時に作成されるイベントを監視する EventBridge ルールを作成します。

   - [ルールタイプ] では、[イベントパターンを持つルール] を選択します。
   - [Event source] (イベントソース) では、[Other] (その他) を選択します。
   - [Event pattern] (イベントパターン) セクションで [Custom patterns (JSON editor)] (カスタムパターン (JSONエディター)) を選択し、次のイベントパターンをテキストエリアに貼付けます。

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

- [ターゲットタイプ] で、AWS サービスを選択します。[ターゲットの選択] で、選択した種類のイベントを Eventbridge が検出したときに対応する AWS サービスを選択します。ターゲットは、ルールで定義したイベントパターンに一致するイベントが返されたときにトリガーされます。

ルールの作成に関する詳細については、「Amazon EventBridge ユーザーガイド」の「イベントに反応する Amazon EventBridge ルールの作成」を参照してください。

レポート生成イベントの例

このイベントは、レポートが生成されて取得する準備ができたことを通知します。message フィールドに、Amazon Simple Storage Service (Amazon S3) バケットと、レポートが保存されている Amazon S3 オブジェクトのキーが表示されます。

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

ドキュメント履歴

次の表に、AWS Application Cost Profiler のドキュメントリリースを示します。

変更	説明	日付
サービス廃止の通知	AWS Application Cost Profiler は 2024 年 9 月 30 日までに廃止される予定で、現在、新規のお客様は受け付けていません。	2023 年 8 月 11 日
イベントのモニタリング	EventBridge コンソールの変更により、Application Cost Profiler のイベントを監視するルールの作成方法が変更されました。詳細については、「EventBridge での Application Cost Profiler イベントの監視」を参照してください。	2022 年 7 月 5 日
S3 バケットポリシーの例の更新	S3 バケットポリシーの例に対するドキュメントのみの更新。詳細については、「Application Cost Profiler 用の Amazon S3 バケットの設定」を参照してください。	2021 年 12 月 6 日
一般提供	Application Cost Profiler の初回一般リリース。	2021 年 5 月 13 日