Amazon Detective

管理ガイド

Amazon Detective: 管理ガイド

Table of Contents

Amazon Detective とは

Amazon Detective を使用すると、セキュリティに関する検出結果や疑わしいアクティビティの根本原因を簡単に分析、調査、および迅速に特定できます。Detective は、AWS リソースからログデータを自動的に収集します。その後、機械学習、統計分析、グラフ理論を使用して、セキュリティ調査をより迅速かつ効率的に行うのに役立つビジュアライゼーションを生成します。

Detective の事前に作成されたデータの集計、要約、およびコンテキストは、考えられるセキュリティ問題の性質と範囲を迅速に分析および特定するのに役立ちます。Detective は、最長 1 年間の履歴イベントデータを保持します。このデータは、選択した時間枠でのアクティビティのタイプと量の変化を示す一連のビジュアライゼーションを通じて簡単に利用できます。Detective は、それらの変更を GuardDuty の検出結果にリンクします。

Detective の仕組み

Detective は、ログイン試行、API コール、ネットワークトラフィックなどの時間ベースのイベントを AWS CloudTrail および Amazon VPC フローログから自動的に抽出します。また、GuardDuty によって検出された結果も取り込みます。

これらのイベントから、Detective は機械学習とビジュアライゼーションを使用して、リソースの動作と時間の経過に伴うそれらの間のインタラクションに関するインタラクティブな統合ビューを作成します。この動作グラフを詳しく確認して、失敗したログオン試行や疑わしい API コールなどのさまざまなアクションを調べることができます。また、これらのアクションが AWS アカウントや Amazon EC2 インスタンスなどのリソースにどのように影響するかを確認できます。さまざまなタスクの動作グラフのスコープとタイムラインを調整できます。

- 基準外のアクティビティを迅速に調査します。
- セキュリティの問題を示している可能性のあるパターンを特定します。
- 検出結果の影響を受けるすべてのリソースを理解します。

Detective に合わせたビジュアライゼーションは、アカウント情報のベースラインと概要を提供します。これらの検出結果は、「これはこのロールに対する異常な API コールですか?」などの質問に回答するのに役立ちます。あるいは、「このインスタンスからのトラフィックのこのスパイクは予想されるものですか?」という質問の回答にも役立ちます。

Detective を使用すると、データを整理したり、独自のクエリやアルゴリズムを開発、設定、調整したりする必要はありません。前払い費用はなく、分析されたイベントの料金のみをお支払いいただきます。追加のソフトウェアをデプロイしたり、他のフィードをサブスクライブしたりする必要はありません。

どのようなユーザーが Detective を使用しますか?

アカウントで Detective を有効にすると、そのアカウントが動作グラフの管理者アカウントになります。動作グラフは、1 つ以上の AWS アカウントから抽出および分析されたデータのリンクされたセットです。管理者アカウントは、メンバーアカウントを招待して、管理者アカウントの動作グラフにデータを提供します。

Detective はにも統合されていますAWS Organizations。組織の管理アカウントは、組織の Detective 管理者アカウントを指定します。Detective 管理者アカウントは、組織の行動グラフで組織アカウントをメンバーアカウントとして有効にします。

Detective が動作グラフアカウントのソースデータをどのように使用するかについては、動作グラフで使用されるソースデータ (p. 13) を参照してください。

管理者アカウントが動作グラフを管理する方法については、アカウントの管理 (p. 17) を参照してください。メンバーアカウントが動作グラフの招待とメンバーシップを管理する方法については、the section called “メンバーアカウントの場合: 招待とメンバーシップの管理” (p. 39) を参照してください。

管理者アカウントは、動作グラフから生成された分析とビジュアライゼーションを使用して、AWS リソースと GuardDuty の検出結果を調査します。Detective の GuardDuty および AWS Security Hub との統合により、これらのサービスの GuardDuty の検出結果から直接 Detective コンソールにピボットできます。

Detective の調査は、関係する AWS リソースに関連するアクティビティに焦点を当てています。Detective での調査プロセスの概要については、Detective ユーザーガイドの How Amazon Detective is used for investigation を参照してください。

Amazon Detective の用語と概念

以下の用語と概念は、Amazon Detective とその仕組みを理解する上で重要です。

管理者アカウント

動作グラフを所有し、調査に動作グラフを使用する AWS アカウント。

管理者アカウントは、メンバーアカウントを招待して、動作グラフにデータを提供します。を参照してくださいthe section called “動作グラフへのメンバーアカウントの招待” (p. 33)。

組織行動グラフの場合、管理者アカウントは、組織の管理アカウントが指定する Detective 管理者アカウントです。the section called “Detective 管理者アカウントの指定” (p. 21) を参照してください。Detective 管理者アカウントは、任意の組織アカウントを組織動作グラフのメンバーアカウントとして有効にできます。the section called “組織メンバーアカウントの管理” (p. 29) を参照してください。

管理者アカウントは、動作グラフのデータ使用量を表示したり、動作グラフからメンバーアカウントを削除したりすることもできます。

動作グラフ

1 つ以上の AWS アカウントに関連付けられている受信ソースデータから生成されたリンクされたデータセット。

各動作グラフは、検出結果、エンティティ、および関係の同じ構造を使用します。

グループを見つける

調査結果グループは、同じイベントまたはセキュリティ問題に関連する可能性のある関連する調査結果、エンティティ、および証拠のコレクションです。Detective は、組み込みの機械学習モデルに基づいて Finding グループを生成します。

委任管理者アカウント (AWS Organizations)

Organizations では、サービスの委任管理者アカウントが組織のサービスの使用を管理できます。

Detective では、Detective 管理者アカウントが組織管理アカウントでない限り、Detective 管理者アカウントが委任管理者アカウントとしての役割も担います。組織管理アカウントを委任管理者アカウントにすることはできません。

Detective 管理者アカウント

組織の管理アカウントによって、リージョンの組織行動グラフの管理者アカウントとして指定されたアカウント。the section called “Detective 管理者アカウントの指定” (p. 21) を参照してください。

組織管理アカウントは、アカウント以外のアカウントを選択することをお勧めします。

アカウントが組織管理アカウントでない場合、Detective 管理者アカウントが Organizations 内の Detective の委任管理者アカウントとしての役割も担います。

Detective のソースデータ

次のフィードタイプからの情報についての、処理および構造化されたバージョン:

- AWS CloudTrail ログや Amazon VPC フローログなどの AWS のサービスからのログ
- GuardDuty 調査結果

Detective は、動作グラフにデータを入力するために、Detective のソースデータを使用します。また、Detective は、分析をサポートするために Detective のソースデータのコピーを保存します。

エンティティ

受信データから抽出された項目。

各エンティティにはタイプがあり、それが表すオブジェクトのタイプを識別します。エンティティタイプの例には、IP アドレス、Amazon EC2 インスタンス、AWS ユーザーが含まれます。

エンティティは、管理する AWS リソース、またはリソースとインタラクションした外部 IP アドレスである場合があります。

各エンティティについて、ソースデータはエンティティのプロパティを入力するためにも使用されます。プロパティ値は、ソースレコードから直接抽出することも、複数のレコードに集約することもできます。

結果

Amazon が検出したセキュリティの問題 GuardDuty。

検出結果の概要

検出結果に関する情報の要約を提供する単一のページ。

検出結果の概要には、検出結果に関係するエンティティのリストが含まれています。リストから、エンティティのプロファイルにピボットできます。

検出結果の概要には、検出結果の属性を含む詳細パネルも含まれています。

大量のエンティティ

時間間隔中に非常に多数の他のエンティティとの接続があるエンティティ。例えば、EC2 インスタンスには、数百万の IP アドレスからの接続がある場合があります。接続数は、Detective が対応できるしきい値を超えています。

現在のスコープ時間が大量の時間間隔を含む場合、Detective はユーザーに通知します。

Amazon Detective ユーザーガイドの Viewing details for high-volume entities を参照してください。

調査

疑わしいアクティビティ、または関心のあるアクティビティに対してトリアージを実行し、スコープを決定し、その基盤となるソースまたは原因に到達し、次にどのように進めるかを決定するプロセス。

メンバーアカウント

管理者アカウントが動作グラフにデータを提供するために招待した AWS アカウント。組織の動作グラフでは、メンバーアカウントは、Detective 管理者アカウントがメンバーアカウントとして有効にした組織アカウントにすることができます。

招待されたメンバーアカウントは、動作グラフの招待に応答したり、動作グラフから自らのアカウントを削除したりできます。the section called “メンバーアカウントの場合: 招待とメンバーシップの管理” (p. 39) を参照してください。

組織アカウントは、組織行動グラフのメンバーシップを変更できません。

また、データの提供先である動作グラフ全体で、アカウントの使用量に関する情報を表示することもできます。

これらのメンバーアカウントには、動作グラフに対する他のアクセス権が付与されていません。

組織動作グラフ

Detective 管理者アカウントが所有する行動グラフ。組織管理アカウントは、Detective 管理者アカウントを指定します。the section called “Detective 管理者アカウントの指定” (p. 21) を参照してください。

組織の動作グラフでは、Detective 管理者アカウントが、組織アカウントがメンバーアカウントであるかどうかを制御します。組織アカウントは、組織行動グラフから自身を削除することはできません。

Detective、他のアカウントを組織動作グラフに招待することもできます。

Profile

エンティティのアクティビティに関連するデータのビジュアライゼーションを集めたものを提供する単一のページ。

検出結果については、プロファイルは、検出結果が真の懸念事項であるか、または誤検知であるかをアナリストが判断するのに役立ちます。

プロファイルは、検出結果の調査または疑わしいアクティビティの一般的な捕捉をサポートするための情報を提供します。

プロファイルのパネル

プロファイル上の単一のビジュアライゼーション。各プロファイルパネルは、アナリストによる調査を支援するために、特定の質問に対する回答をサポートすることを目的とするものです。

プロファイルパネルには、単純なキーバリューペア、テーブル、タイムライン、棒グラフ、またはジオロケーションチャートを含めることができます。

関係

個々のエンティティ間で生じるアクティビティ。関係は入力ソースデータからも抽出されます。

エンティティと同様に、関係にはタイプがあります。これは、関係するエンティティのタイプと接続の方向を識別します。関係のタイプの例として、Amazon EC2 インスタンスに接続する IP アドレスを挙げることができます。

スコープ時間

プロファイルに表示されるデータのスコープ設定に使用される時間枠。

検出結果のデフォルトのスコープ時間は、疑わしいアクティビティが観察された最初と最後の時間を反映します。

エンティティプロファイルのデフォルトのスコープ時間は直近 24 時間です。

Amazon Detective のリージョンとクォータ

Amazon Detective を使用する場合は、これらのクォータに注意してください。

Detective のリージョンとエンドポイント

Detective が利用可能なリージョンのリストを表示するには、Detective のサービスエンドポイントを参照してください。

Detective のクォータ

Detective には以下のクォータがあります。これらのクォータは設定できません。

リソース	クォータ	コメント
メンバーアカウントの数	1,200	管理者アカウントが動作グラフに追加できるメンバーアカウントの数。
動作グラフのデータ量 — 量に関する警告	1 日あたり 3.24 TB	動作グラフのデータ量が 1 日あたり 3.24 TB より大きい場合、Detective は動作グラフが最大許容量に近づいていることを示す警告を表示します。
動作グラフのデータ量 — 新しいアカウントなし	1 日あたり 3.6 TB	動作グラフのデータ量が 1 日あたり 3.6 TB を超える場合、新しいメンバーアカウントを動作グラフに追加することはできません。
動作グラフのデータ量 — 動作グラフへのデータの取り込みを停止する	1 日あたり 4.5 TB	動作グラフのデータ量が 1 日あたり 4.5 TB を超える場合、Detective は動作グラフへのデータの取り込みを停止します。 1 日あたり 4.5 TB は、通常のデータ量とデータ量のスパイクの両方を反映しています。 データの取り込みを再度有効にするには、AWS Support に問い合わせてください。

Internet Explorer 11 はサポートされていません

Internet Explorer 11 では Detective をご利用いただけません。

Amazon Detective の設定

Amazon Detective を有効にすると、Detective は、自分のアカウントを管理者アカウントとするリージョン固有の動作グラフを作成します。最初は、動作グラフではこれが唯一のアカウントです。管理者アカウントは、他の AWS アカウントを招待して、動作グラフにデータを提供することができます。「アカウントの管理 (p. 17)」を参照してください。

あるリージョンで初めて Detective を有効にすると、動作グラフの 30 日間の無料トライアルも開始されます。アカウントが Detective を無効にしてから再度有効にした場合、無料トライアルは利用できません。「動作グラフの無料トライアル期間について (p. 12)」を参照してください。

無料トライアルが終了した後は、動作グラフの各アカウントには、提供するデータについての料金が請求されます。管理者アカウントは、動作グラフ全体について、使用量を追跡したり、通常の 30 日間の合計予測コストを表示したりできます。「the section called “管理者アカウントの使用量とコスト” (p. 45)」を参照してください。メンバーアカウントは、自らが属する動作グラフの使用量と予測コストを追跡できます。「the section called “メンバーアカウントの使用量の追跡” (p. 47)」を参照してください。

目次

Amazon Detective の前提条件と推奨事項

Amazon Detective を有効にするには、まず AWS アカウントが必要です。アカウントをお持ちでない場合は、この手順にしたがってアカウントを作成してください。

AWS 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用いて確認コードを入力するように求められます。

また、次の要件および推奨事項に注意する必要があります。

サポートされる AWS Command Line Interface バージョン

AWS CLI を使用して Detective タスクを実行するために必要な最小バージョンは 1.16.303 です。

アカウントが Amazon GuardDuty を有効にしている必要があります

Detective を有効にしようとすると、Detective は、アカウントのために GuardDuty が有効になってから 48 時間が経過しているかどうかを確認します。

GuardDuty をご利用のお客様ではない場合、または GuardDuty のお客様になってから 48 時間が経過していない場合、Detective を有効にすることはできません。GuardDuty を有効にするか 48 時間待つ必要があります。これにより、GuardDuty は、アカウントが生成するデータ量を評価できます。

アカウントのデータ量は Detective クォータの範囲内にある必要があります

動作グラフに流入するデータの量は、Detective が許容する最大値より小さい必要があります。

Detective を有効にしようとする際に、アカウントのデータ量が大き過ぎると、Detective を有効にできません。Detective コンソールには、データ量が大き過ぎることを示す通知が表示されます。

GuardDuty および AWS Security Hub との推奨アラインメント

GuardDuty および AWS Security Hub に登録している場合は、ご利用のアカウントをこれらのサービスの管理者アカウントにすることをお勧めします。管理者アカウントが 3 つのサービスすべてで同じである場合、次の統合ポイントはシームレスに機能します。

- GuardDuty または Security Hub では、GuardDuty の検出結果の詳細を表示する際に、検出結果の詳細から Detective の検出結果プロファイルにピボットできます。
- Detective では、GuardDuty の検出結果を調査するときに、その検出結果をアーカイブするオプションを選択できます。

GuardDuty と Security Hub の管理者アカウントが異なる場合は、より頻繁に利用するサービスに基づいて管理者アカウントを調整することをお勧めします。

- GuardDuty をより頻繁に使用する場合は、GuardDuty の管理者アカウントを使用して Detective を有効にします。

  !AWS Organizationsアカウントを管理するには、GuardDuty 管理者アカウントを組織の Detective 管理者アカウントとして指定します。
- Security Hub をより頻繁に使用する場合は、Security Hub の管理者アカウントを使用して Detective を有効にします。

  Organizations を使用してアカウントを管理する場合は、Security Hub 管理者アカウントを組織の Detective 管理者アカウントとして指定します。

すべてのサービスで同じ管理者アカウントを使用できない場合は、Detective を有効にした後、オプションでクロスアカウントロールを作成できます。このロールは、管理者アカウントに他のアカウントへのアクセス権を付与します。

IAM がこのタイプのロールをサポート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。

必要な Detective 権限の付与

Detective を有効にする前に、IAM プリンシパルに必要な Detective 権限があることを確認する必要があります。プリンシパルは、既に使用している既存のユーザーまたはロールにすることも、Detective で使用する新しいユーザーまたはロールを作成することもできます。

必要な権限をすべて付与する最も簡単な方法は、`AmazonDetectiveFullAccess`管理ポリシー (p. 71)。これにより、すべての Detective アクションへのアクセス許可を付与します。

GuardDuty CloudWatch の通知頻度に対する推奨される更新

GuardDuty では、ディテクターは、その後の検出結果の発生をレポートするために Amazon CloudWatch の通知頻度で設定されます。これには Detective への通知の送信が含まれます。

デフォルトでは、頻度は 6 時間です。これは、検出結果が何回も繰り返し発生しても、新しい発生は最長で 6 時間後まで Detective に反映されないことを意味します。

Detective がこれらの更新を受信するのにかかる時間を短縮するために、GuardDuty の管理者アカウントがディテクターの設定を 15 分に変更することをお勧めします。設定を変更しても GuardDuty の使用コストには影響しないことに注意してください。

通知頻度の設定については、を参照してください。Amazon CloudWatch Events での GuardDuty 結果のモニタリングのAmazon GuardDuty ユーザーガイド。

Amazon Detective の有効化

Detective は、Detective コンソール、Detective API、または AWS Command Line Interface から有効にできます。

Detective は、各リージョンで 1 回のみ有効にできます。自分のアカウントが既に該当のリージョンにある動作グラフの管理者アカウントである場合、そのリージョンで Detective を再度有効にすることはできません。

Detective を有効にする前に、アカウントが Amazon GuardDuty に登録されてから 48 時間以上が経過していることを確認してください。この要件を満たさない場合、Detective を有効にすることはできません。

GuardDuty の要件を満たしている場合、Detective を有効にするようにリクエストすると、Detective はデータ量が Detective のクォータ内にあるかどうかを確認します。データ量がクォータを超えている場合、Detective を有効にすることはできません。

Detective の有効化 (コンソール)

AWS Management Console から Amazon Detective を有効にできます。

Detective を有効にするには (コンソール)

1. AWS Management Console にサインインします。その後、https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. [Get started (開始方法)] を選択します。
3. [Enable Amazon Detective] (Amazon Detective を有効化) のページの [Align administrator accounts (recommended)] (管理者アカウントを調整 (推奨)) では、管理者アカウントを Detective と Amazon GuardDuty と AWS Security Hub の間で調整するためのレコメンデーションの説明が表示されます。「the section called “GuardDuty および AWS Security Hub との推奨アラインメント” (p. 8)」を参照してください。
4. IAM ポリシーのアタッチ (必須)Detective を有効にして動作グラフを管理するために必要なアクセス権限を持つ IAM ポリシーが含まれています。ポリシーは、既にプリンシパルにアタッチされている必要があります。

   まだアタッチされていない場合は、[Copy IAM policy] (IAM ポリシーをコピー) を選択してポリシーをコピーし、アタッチできるようにします。

   必要な IAM ポリシーが存在していることを確認します。

5. [Add tags] (タグを追加) のセクションでは、動作グラフにタグを追加できます。

   タグを追加するには、次の操作を行います。

   a. [新しいタグを追加] をクリックします。
   b. [Key] (キー) で、タグの名前を入力します。
   c. [Value] (値) で、タグの値を入力します。

   タグを削除するには、そのタグの [Remove] (削除) オプションを選択します。
6. [Enable Amazon Detective] (Amazon Detective を有効化) を選択します。
7. Detective を有効にすると、動作グラフにメンバーアカウントを招待できます。

   [Account management] (アカウント管理) のページに移動するには、[Add members now] (今すぐメンバーを追加) を選択します。メンバーアカウントの招待については、the section called “動作グラフへのメンバーアカウントの招待” (p. 33) を参照してください。

Detective の有効化 (Detective API、AWS CLI)

Detective API または AWS Command Line Interface から Amazon Detective を有効にできます。

Detective を有効にするには (Detective API、AWS CLI)

- Detective API: を使用する`CreateGraph`オペレーション.
- AWS CLI: コマンドラインで、`create-graph` コマンドを実行します。

```
aws detective create-graph --tags '{"tagName": "tagValue"}'
```

次のコマンドは、Detective を有効にし、`Department` タグの値を `Security` に設定します。

```
aws detective create-graph --tags '{"Department": "Security"}'
```

リージョン全体での Detective の有効化 (GitHub の Python スクリプト)

Detective は、次のことを実行するオープンソーススクリプトを GitHub で提供します。

- 指定されたリージョンのリストにある管理者アカウントのために Detective を有効にします
- 作成された各動作グラフに、提供されたメンバーアカウントのリストを追加します
- メンバーアカウントに招待メールを送信します
- メンバーアカウントになるための招待を自動的に承諾します

GitHub スクリプトの設定方法と使用方法については、Amazon Detective Python スクリプトの使用 (p. 78) を参照してください。

データが抽出されていることの確認

Detective を有効にすると、AWS アカウントから動作グラフへのデータの取り込みと抽出が開始されます。

最初の抽出では、データは通常 24 時間以内に動作グラフで利用可能になります。

Detective がデータを抽出していることを確認する 1 つの方法は、Detective の [Search] (検索) ページでサンプルの値を探すことです。

[Search] (検索) ページでサンプルの値を確認するには

1. Detective コンソールを開きます。
2. ナビゲーションペインで、[Search (検索)] を選択します。
3. [Select type] (タイプを選択) のメニューから、項目のタイプを選択します。

   [Examples from your data] (データのサンプル) には、動作グラフのデータに存在する、選択したタイプの識別子のサンプルセットが含まれています。

   サンプルの値を表示できる場合は、データが取り込まれ、動作グラフに抽出されています。

動作グラフの無料トライアル期間について

Amazon Detective は、各リージョンの各アカウントに 30 日間の無料トライアルを提供します。アカウントの無料トライアルは、次のいずれかのアクションを初めて実行したときに開始します。

- アカウントで Detective を手動で有効化し、ある動作グラフの管理者アカウントになる。
- アカウントが組織の委任Detective アカウントとして委任されたAWS Organizations、Detective を初めて有効化した。
- Detective 管理者アカウントが指定される前にすでに Detective が有効になっていた場合、そのアカウントは新しい 30 日間の無料トライアルを開始しません。
- アカウントは、動作グラフのメンバーアカウントへの招待を承諾し、メンバーアカウントとして有効化されます。
- 組織アカウントは、Detective の管理者アカウントによってメンバーアカウントとして有効化されます。

無料トライアル期間はその時点から 30 日間です。その期間中に処理されたデータの料金については、アカウントに請求されません。トライアル期間が終了すると、Detective は、動作グラフに提供するデータについての料金をアカウントに請求し始めます。

リージョン内のすべての動作グラフに同じ 30 日間が使用されます。例えば、アカウントがある動作グラフのメンバーアカウントとして有効になったとします。これにより、30 日間の無料トライアル期間が開始します。10 日後、アカウントは同じリージョンの 2 番目の動作グラフのために有効になります。2 番目の動作グラフについては、そのアカウントの無料トライアル期間は 20 日間となります。

無料トライアルでは、次のような複数のメリットがあります。

- 管理者アカウントは、Detective の特長や機能を詳しく確認し、その価値を検証できます。
- 管理者アカウントとメンバーアカウントは、Detective がデータについての請求を開始する前に、データの量と推定コストをモニタリングできます。「the section called “管理者アカウントの使用量とコスト” (p. 45)」および「the section called “メンバーアカウントの使用量の追跡” (p. 47)」を参照してください。

オプションのデータソースの無料トライアル

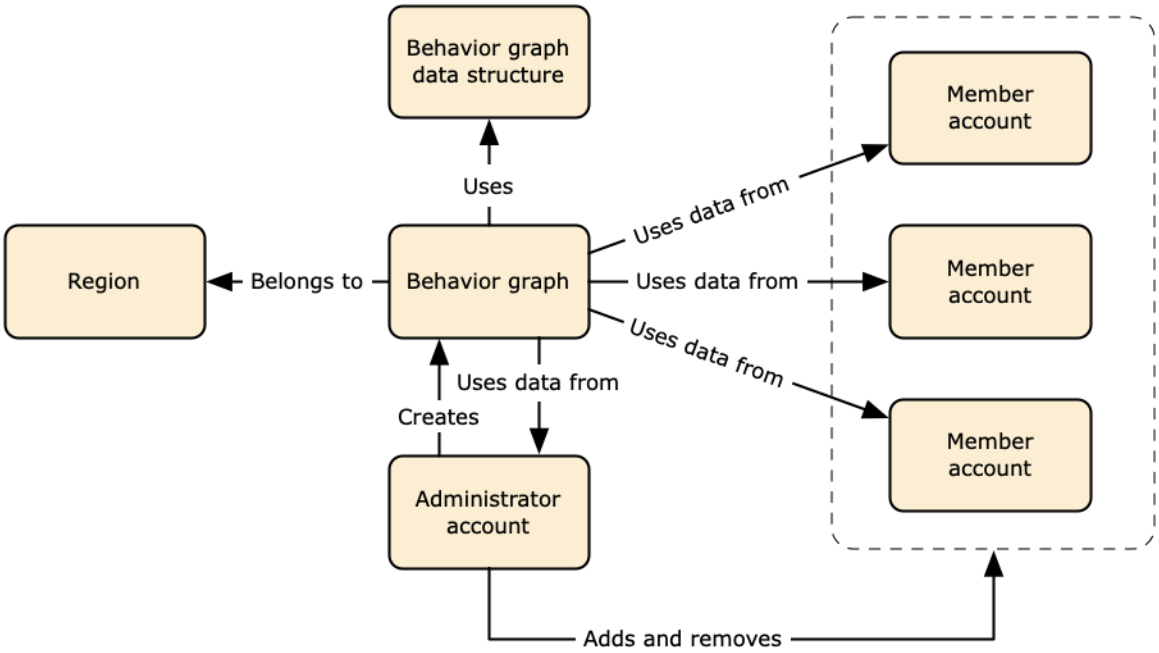
Detective は、オプションのデータソースの 30 日間の無料試用版も提供しています。この無料トライアルは、Detective が最初に有効になったときにコア Detective データソースに提供される無料トライアルとは別のものです。

> Note
>
> お客様がオプションのデータソースパッケージを有効にしてから 7 日以内に無効にすると、Detective はそのデータソースパッケージが再度有効になった場合に、そのデータソースパッケージの無料試用版を 1 回だけ自動リセットします。

オプションのデータソースを有効または無効にするには、「」を参照してください。Detective のオプションデータソースの種類 (p. 13)。

動作グラフで使用されるソースデータ

動作グラフにデータを入力するために、Amazon Detective は、動作グラフの管理者アカウントとメンバーアカウントのソースデータを使用します。



動作グラフのデータ構造の詳細については、Detective ユーザーガイドの Overview of the behavior graph data structure を参照してください。

Detective のコアデータソースのタイプ

Detective は、次のタイプの AWS ログからデータを取り込みます。

- AWS CloudTrail ログ
- Amazon Virtual Private Cloud (Amazon VPC) フローログ
- に登録されているアカウントの場合 GuardDuty、Detective も取り込んで GuardDuty 検出結果。

Detective は消費します。 CloudTrail および VPC フローログイベントをの独立した重複ストリームを使用して CloudTrail および VPC フローログに記録されます。これらのプロセスは、既存のプロセスに影響を与えたり、これらを使用したりすることはありません。 CloudTrail および VPC フローログ設定。また、これらのサービスのパフォーマンスに影響を与えたり、コストを増加させたりすることもありません。

Detective のオプションデータソースの種類

Detective は、Detective コアパッケージで提供される 3 つのデータソースに加えて、オプションのソースパッケージを提供します (コアパッケージにはAWS CloudTrailログ、VPC フローログ、 GuardDuty 検出結

果)。動作グラフのオプションのデータソースパッケージは、いつでも動作グラフ用に起動または停止できます。

Detective は、リージョンごとにすべてのオプションのソースパッケージに 30 日間の無料トライアルを提供します。

Note

データソースのすべてのログは、最長 1 年間保持されます。

現在、以下のオプションのソースパッケージが利用可能です。

- EKS 監査ログ

  このオプションのデータソースパッケージを使用すると、Detective は環境内の EKS クラスターに関する詳細情報を取り込み、そのデータを行動グラフに追加できます。詳細については、「Detective の Amazon EKS 監査ログ (p. 14)」を参照してください。

オプションのデータソースを開始または停止します。

1. でDetective コンソールを開きます。https://console.aws.amazon.com/detective/。
2. 下のナビゲーションパネルから設定、選択将軍。
3. []オプションのソースパッケージで、更新。次に、有効にするデータソースを選択するか、すでに有効になっているデータソースのボックスの選択を解除して、更新をクリックして、どのデータソースパッケージを有効にするかを変更します。

   Note

   オプションのデータソースを停止してから再起動すると、一部のエンティティプロファイルに表示されるデータにギャップが表示されます。このギャップは、コンソールの表示に表示され、データソースが停止した期間を表します。データソースが再起動されると、Detective は遡及的にデータを取り込むことはありません。

Detective の Amazon EKS 監査ログ

Amazon EKS 監査ログは、Detective Behavior Graph に追加できるオプションのデータソースパッケージです。利用可能なオプションのソースパッケージと、アカウント内のそれらのステータスは、設定コンソール、または Detective API を介してページを表示します。

このデータソースには 30 日間の無料試用版が提供されています。詳細については、次を参照してください。オプションのデータソースの無料トライアル (p. 12)。

Amazon EKS 監査ログを有効にすると、Detective は Amazon EKS で作成されたリソースに関する詳細な情報を行動グラフに追加できます。このデータソースは、次のエンティティタイプについて提供される情報を強化します。EKS クラスター、Kubernetes ポッド、コンテナイメージ、Kubernetes サブジェクト。

さらに、Amazon のデータソースとして EKS 監査ログを有効にしている場合 GuardDuty Kubernetesの調査結果の詳細は GuardDuty。このデータソースの有効化の詳細については GuardDuty 見るAmazon での Kubernetes 保護 GuardDuty。

Note

このデータソースは、2022 年 7 月 26 日以降に作成された新しい行動グラフではデフォルトで有効になっています。2022年7月26日より前に作成された行動グラフでは、手動で有効にする必要があります。

Amazon EKS 監査ログをオプションのデータソースとして追加または削除する:

1. でDetective コンソールを開きます。https://console.aws.amazon.com/detective/。
2. 下のナビゲーションパネルから設定、選択将軍。
3. []ソースパッケージで、EKS 監査ログをクリックして、このデータソース記録可能にします。すでに有効になっている場合は、もう一度選択して取り込みを停止しますEKS 監査ログあなたの行動グラフに。

Detective がソースデータを取り込み、保存する方法

Detective を有効にすると、Detective は、動作グラフの管理者アカウントからソースデータの取り込みを開始します。メンバーアカウントが動作グラフに追加されると、Detective は、それらのメンバーアカウントからのデータの使用も開始します。

Detective のソースデータは、元のフィードの構造化されたバージョンと処理されたバージョンで構成されています。Detective の分析をサポートするため、Detective は、Detective のソースデータのコピーを保存します。

Detective の取り込みプロセスは、Detective のソースデータストアの Amazon Simple Storage Service (Amazon S3) バケットにデータをフィードします。新しいソースデータが到着すると、他の Detective コンポーネントがデータを取得し、抽出および分析プロセスを開始します。詳細については、Detective ユーザーガイドの How Detective uses source data to populate a behavior graph を参照してください。

Detective が動作グラフのデータ量のクォータを適用する方法

Detective には、各動作グラフで許可されるデータの量に関する厳密なクォータがあります。データ量は、Detective の動作グラフにフローする 1 日あたりのデータ量です。

管理者アカウントが Detective を有効にし、メンバーアカウントが動作グラフにデータを提供するための招待を承諾すると、Detective はこれらのクォータを適用します。

- 管理者アカウントのデータ量が 1 日あたり 3.6 TB を超える場合、管理者アカウントは Detective を有効にできません。
- メンバーアカウントからデータ量が追加されることにより、動作グラフが 1 日あたり 3.6 TB を超えることになる場合、メンバーアカウントを有効にすることはできません。

動作グラフのデータ量は、時間が経過するにつれて自然に増加することもあります。Detective は、クォータを超えることのないよう、動作グラフのデータ量を毎日チェックします。

動作グラフのデータ量がクォータに近づいている場合、Detective はコンソールに警告メッセージを表示します。クォータを超えないように、メンバーアカウントを削除できます。

動作グラフのデータ量が 1 日あたり 3.6 TB を超える場合、動作グラフに新しいメンバーアカウントを追加することはできません。

動作グラフのデータ量が 1 日あたり 4.5 TB を超える場合、Detective は動作グラフへのデータの取り込みを停止します。1 日あたり 4.5 TB は、通常のデータ量とデータ量のスパイクの両方を反映しています。このクォータに達すると、新しいデータは動作グラフに取り込まれませんが、既存のデータは削除されませ

ん。引き続きその履歴データを調査に使用することはできます。コンソールには、動作グラフのデータ取り込みが一時停止されていることを示すメッセージが表示されます。

データの取り込みが一時停止されている場合は、AWS Support を使用してデータを再度有効にする必要があります。可能であれば、AWS Support に問い合わせる前に、メンバーアカウントを削除して、データ量がクォータを下回るように試みてください。これにより、動作グラフのデータ取り込みを再度有効にすることが容易になります。

アカウントの管理

各行動グラフには、1 つ以上の勘定科目からのデータが含まれます。アカウントで Detective を有効にすると、そのアカウントが動作グラフの管理者アカウントになり、動作グラフのメンバーアカウントが選択されます。動作グラフは、最大 1,200 のメンバーアカウントを持つことができます。

と統合されている場合AWS Organizationsの順に選択し、組織管理アカウントは、その組織の Detective 管理者アカウントを指定します。その Detective 管理者アカウントは、組織の動作グラフの管理者アカウントになります。Detective 管理者アカウントは、組織の行動グラフで任意の組織アカウントをメンバーアカウントとして有効にできます。組織アカウントは、組織の行動グラフから自分自身を削除することはできません。

管理者アカウントは、行動グラフに参加するようにアカウントを招待することもできます。アカウントが招待を承認すると、Detective はアカウントをメンバーアカウントとして有効にします。招待によって追加されたメンバーアカウントは、行動グラフから自分自身を削除できます。

アカウントがメンバーアカウントとして有効になると、Detective は、メンバーアカウントのデータを取り込み、その動作グラフに抽出し始めます。

Detective は、各動作グラフに提供するデータについて各アカウントに料金を請求します。動作グラフでの各アカウントのデータ量の追跡については、を参照してください。the section called “管理者アカウントの使用量とコスト” (p. 45)。

目次

Detective のアカウント制限と推奨事項

Amazon Detective でアカウントを管理する場合は、以下の制約と推奨事項に注意してください。

メンバーアカウントのの最大数

Detective は、各動作グラフで最大 1,200 のメンバーアカウントを許可します。

アカウントとリージョン

を使用した場合AWS Organizationsアカウントを管理するには、組織管理アカウントは、組織の Detective 管理者アカウントを指定します。Detective 管理者アカウントは、組織の動作グラフの管理者アカウントになります。

Detective 管理者アカウントは、すべてのリージョンで同じである必要があります。組織管理アカウントは、各リージョンで Detective 管理者アカウントを個別に指定します。Detective 管理者アカウントは、各リージョンで組織の行動グラフとメンバーアカウントも個別に管理します。

招待によって作成されたメンバーアカウントの場合、管理者とメンバーの関連付けは、招待の送信元のリージョンでのみ作成されます。管理者アカウントは、各リージョンで Detective を有効にする必要があり、各リージョンに個別の動作グラフがあります。次に、管理者アカウントは、各アカウントをそのリージョンのメンバーアカウントとして関連付けるよう招待します。

1 つのアカウントは、同じリージョン内の複数の動作グラフのメンバーアカウントになることができます。1 つのアカウントが管理者アカウントになることができるのは、リージョンごとに 1 つの動作グラフについてのみです。1 つのアカウントは、異なるリージョンの管理者アカウントになることができます。

管理者アカウントとSecurity Hub と GuardDuty のアライメント

との統合を確実にするためAWS Security HubAmazon GuardDuty はスムーズに動作するため、これらすべてのサービスで同じアカウントが管理者アカウントであることを推奨します。

「the section called “GuardDuty および AWS Security Hub との推奨アラインメント” (p. 8)」を参照してください。

管理者アカウントに必要なアクセス許可の付与

管理者アカウントがその動作グラフを管理するために必要な権限を持っていることを確認するには、`AmazonDetectiveFullAccess`管理ポリシー (p. 71)IAM プリンシパルに。

Detective で組織の更新を反映する

組織への変更は、Detective にすぐには反映されません。

新規および削除された組織アカウントなど、ほとんどの変更では、Detective が通知されるまでに最大 1 時間かかる場合があります。

Organizations 内の指定された Detective 管理者アカウントを変更すると、伝播にかかる時間が短縮されます。

Organizations を使用して行動グラフ勘定科目を管理するための移行を行う

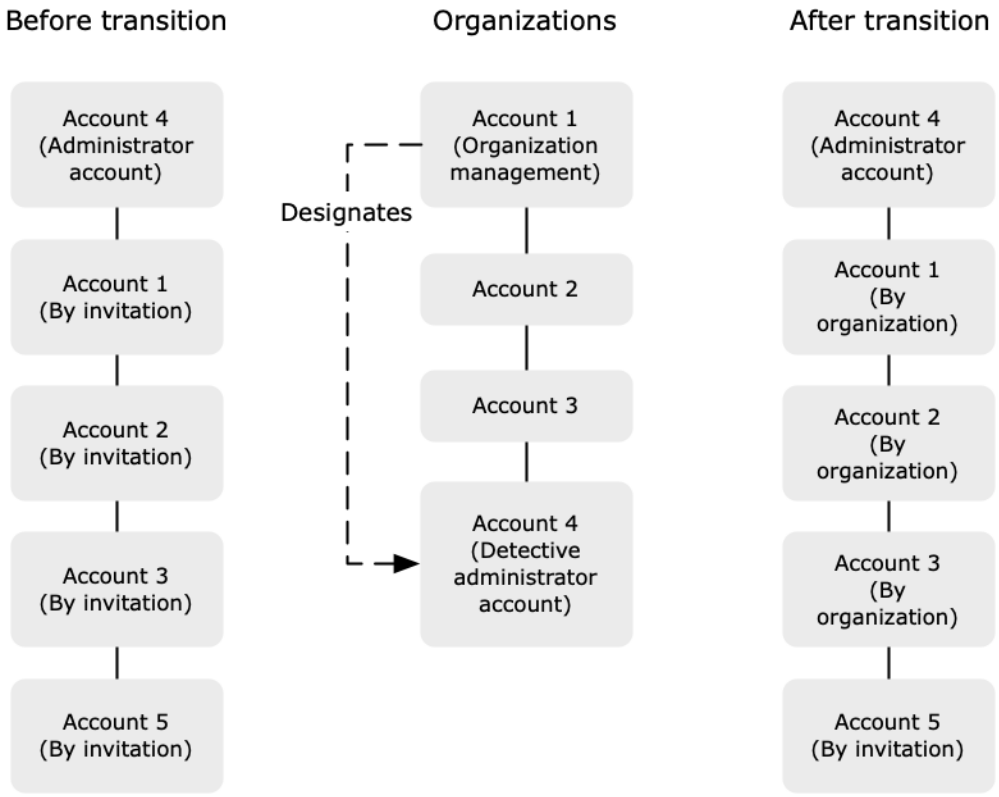
手動招待を受け入れたメンバーアカウントを含む既存の行動グラフがある可能性があります。に在籍している場合AWS Organizationsでは、手動招待プロセスを使用する代わりに、Organizations を使用してメンバーアカウントを有効化および管理するには、次の手順を使用します。

1. 組織の Detective 管理者アカウントを指定します。 (p. 19)これにより、組織行動グラフが作成されます。

   Detective 管理者アカウントに既に動作グラフがある場合、その動作グラフが組織の動作グラフになります。
2. 組織の行動グラフで、組織アカウントをメンバーアカウントとして有効にします。 (p. 19)

   組織行動グラフに組織アカウントである既存のメンバーアカウントがある場合、それらのアカウントは自動的に有効になります。

次の図は、移行前の動作グラフ構造、Organizations 内の構成、および移行後の動作グラフ勘定構造の概要を示しています。



組織の Detective 管理者アカウントを指定する

組織の管理アカウントは、組織の Detective 管理者アカウントを指定します。「the section called “Detective 管理者アカウントの指定” (p. 21)」を参照してください。

移行を簡単にするために、Detective は、組織の Detective 管理者アカウントとして現在の管理者アカウントを選択することをお勧めします。

Organizations 内の Detective に委任された管理者アカウントがある場合、そのアカウントまたは組織管理アカウントを Detective 管理者アカウントとして使用する必要があります。

それ以外の場合は、組織の管理アカウントではない Detective 管理者アカウントを初めて指定するときに、Detective は Organizations を呼び出して、そのアカウントを Detective の委任された管理者アカウントにします。

組織アカウントをメンバーアカウントとして有効にする

Detective 管理者アカウントは、組織の動作グラフの管理者アカウントです。Detective 管理者アカウントは、組織の行動グラフでメンバーアカウントとして有効にする組織アカウントを選択します。「the section called “組織メンバーアカウントの管理” (p. 29)」を参照してください。

リポジトリの []アカウントページで、Detective 管理者アカウントは、組織内のすべてのアカウントを表示します。

Detective 管理者アカウントが既に動作グラフの管理者アカウントであった場合、その動作グラフが組織の動作グラフになります。その動作グラフで既にメンバーアカウントであった組織アカウントは、自動的にメンバーアカウントとして有効になります。他の組織アカウントのステータスはメンバーではない。

組織アカウントには、次のタイプがあります。組織別、以前に招待によるメンバーアカウントであっても。

組織に属さないメンバーアカウントには、次のタイプがあります。招待により。

-アカウント管理ページにはオプションもあり、新しい組織アカウントを自動的に有効にするをクリックして、組織に追加された新しいアカウントを自動的に有効にします。「the section called “新しい組織アカウントを自動的に有効にする” (p. 29)」を参照してください。このオプションは最初はオフになっています。

Detective 管理者アカウントが最初に表示されるときアカウント管理ページには、次のメッセージが表示されます。すべての組織アカウントを有効にするボタンを使用します。選択した場合すべての組織アカウントを有効にする、Detective は以下のアクションを実行します。

- 現在の組織アカウントをすべてメンバーアカウントとして有効にします。
- 新しい組織アカウントを自動的に有効にするオプションをオンにします。

また、すべての組織アカウントを有効にするメンバーアカウントリストのオプション。

アカウントに許可されるアクション

管理者アカウントとメンバーアカウントは、次の Detective アクションにアクセスできます。テーブルの値の意味は次のとおりです。

- 任意— アカウントは、同じ Detective 管理者アカウントのすべてのアカウントに対してアクションを実行できます。
- 自分 - アカウントは、自分のアカウントでのみアクションを実行できます。
- ダッシュ (—)-アカウントはアクションを実行できません。

この表は、管理者およびメンバーアカウントのデフォルトの許可を示しています。カスタム IAM ポリシーを使用することで、Detective の機能へのアクセスをさらに制限できます。

アクション	管理者アカウント (組織)	管理者アカウント (招待)	メンバー (組織)	メンバー (招待)
アカウントを表示する	すべて	すべて	自己 (管理者アカウントの表示)	自己 (管理者アカウントの表示)
メンバーアカウントを削除する	すべて 招待されたアカウントは削除されます 組織アカウントは関連付け解除されます	すべて	–	自分
オプションのデータソースパッケージを追加または削除する	任意 (設定はすべてのメンバーアカウントに適用されます)	任意 (設定はすべてのメンバーアカウントに適用されます)	–	–
Detective	自分	自分	–	–

アクション	管理者アカウント (組織)	管理者アカウント (招待)	メンバー (組織)	メンバー (招待)
動作グラフのデータの表示	すべて	すべて	–	–

組織のDetective 管理者アカウントの指定

組織の行動グラフでは、Detective 管理者アカウントが、すべての組織アカウントの動作グラフメンバーシップを管理します。

Detective 管理者アカウントの管理方法

組織管理アカウントは、各リージョンの組織の Detective 管理者アカウントを指定します。

Detective 管理者アカウントを委任された管理者アカウントとして設定する

Detective 管理者アカウントは、組織のDetective の委任管理者アカウントにもなります。例外は、組織管理アカウントが Detective 管理者アカウントとして自身を指定する場合です。組織管理アカウントは、Organizations の委任管理者になることはできません。

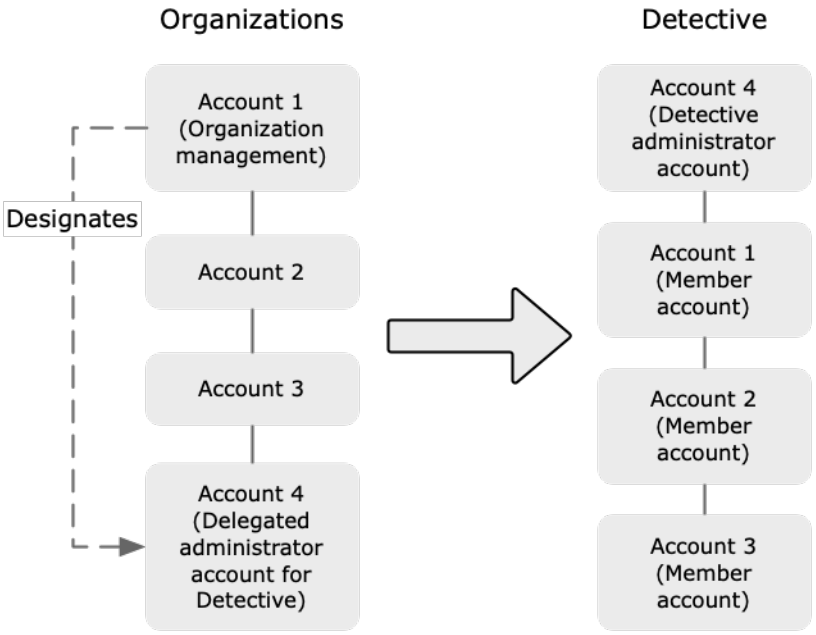
委任された管理者アカウントを Organizations で設定すると、組織管理アカウントは Detective 管理者アカウントとして委任された管理者アカウントまたは独自のアカウントのみを選択できます。委任管理者アカウントは、すべてのリージョンで選択することをお勧めします。

組織行動グラフの作成と管理

組織管理アカウントが Detective 管理者アカウントを選択すると、Detective はそのアカウントの新しい動作グラフを作成します。その行動グラフは組織行動グラフです。

Detective 管理者アカウントが既存の行動グラフの管理者アカウントである場合、その動作グラフは組織の行動グラフになります。

Detective 管理者アカウントは、組織の行動グラフでメンバーアカウントとして有効にする組織アカウントを選択します。



Detective 管理者アカウントは、組織に属していないアカウントに招待を送信することもできます。「the section called “組織メンバーアカウントの管理” (p. 29)」および「the section called “招待されたアカウントの管理” (p. 32)」を参照してください。

Detective 管理者アカウントの削除

組織管理アカウントは、リージョン内の現在の Detective 管理者アカウントを削除できます。Detective 管理者アカウントを削除すると、Detective は現在のリージョンからのみ削除されます。Organizations の委任された管理者アカウントは変更されません。

組織管理アカウントがリージョン内の Detective 管理者アカウントを削除すると、Detective は組織の動作グラフを削除します。削除された Detective 管理者アカウントに対して Detective は無効になっています

Detective の現在の委任された管理者アカウントを削除するには、Organizations API を使用します。Organizations 内の Detective の委任された管理者アカウントを削除すると、Detective は、委任された管理者アカウントが Detective 管理者アカウントである組織の動作グラフをすべて削除します。Detective 管理者アカウントとして組織管理アカウントを持つ組織の動作グラフは影響を受けません。

Detective 管理者アカウントを設定するために必要な権限

組織の管理アカウントが Detective 管理者アカウントを設定できるようにするには、IAM プリンシパルに次のアクセス権限を付与します。

- [] のアタッチAmazonDetectiveFullAccess管理ポリシー (p. 71)。
- 次のOrganizations に権限を付与します。

```
{
    "Effect": "Allow",
    "Action": "organizations:EnableAWSServiceAccess",
    "Resource": "*"
},
{
```

```
    "Effect": "Allow",
    "Action": [
        "organizations:RegisterDelegatedAdministrator".
        "organizations:DescribeAccount"
    ],
    "Resource": "arn:aws:organizations::*:account/o-*/*"
}
```

OrganizationsDeregisterDelegatedAdministratorオペレーションは、すべてのリージョンから同時にDetective 管理者アカウントを削除するために使用されます。実行できるようにするにはDeregisterDelegatedAdministratorでは、IAM プリンシパルも付与する必要がありますorganizations:DeregisterDelegatedAdministrator。

- サービスにリンクされたロールに対する ARN に対する次の IAM アクセス権限を付与します。

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "<service-linked role ARN>",
}
```

組織の管理アカウントに必要なアクセス許可を含む IAM ポリシーを表示するには

1. Detective コンソールを開きます。
2. ナビゲーションペインで [Settings] の [General] を選択します。
3. []必要な IAM ポリシーで、組織管理 IAM ポリシーを表示する。

Detective 管理者アカウントの指定 (コンソール)

組織管理アカウントは、Detective コンソールを使用して Detective 管理者アカウントを指定できます。

Detective 管理者アカウントを管理するために Detective を有効にする必要はありません。Detective 管理者アカウントは、Detectiveページで.

Detective 管理者アカウントを指定するには (Detectiveページで)

1. Detective コンソールを開きます。
2. [Get started (開始方法)] を選択します。
3. []委任された管理者で、Detective 管理者アカウントを選択します。

   使用できるオプションは、Organizations 内の Detective の委任管理者アカウントを持っているかどうかによって異なります。

   - Organizations 内の Detective の委任された管理者アカウントがない場合は、アカウントのアカウント ID を入力して、Detective 管理者アカウントとして指定します。

     手動招待プロセスの既存の管理者アカウントと動作グラフがある場合があります。その場合は、Detective はそのアカウントを Detective 管理者アカウントとして指定することをお勧めします。

     Amazon GuardDuty のOrganizations に委任された管理者アカウントがある場合、AWS Security Hub、または Amazon Macie の場合、Detective はそれらのアカウントのいずれかを選択するように求められます。別のアカウントを入力することもできます。
   - 組織のDetective in Organizationsに委任された管理者アカウントがある場合は、そのアカウントまたはアカウントを選択するように求められます。Detective は、すべてのリージョンで委任された管理者アカウントを選択することをお勧めします。

4. [Delegate] (委任) を選択します。

Detective が有効になっている場合、または既存の動作グラフのメンバーアカウントである場合は、将軍ページで.

Detective 管理者アカウントを指定するには (将軍ページで)

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Settings] (設定) の [General] (一般) を選択します。
3. []委任された管理者で、編集。
4. []委任された管理者で、Detective 管理者アカウントを選択します。

   使用できるオプションは、Organizations 内の Detective の委任管理者アカウントを持っているかどうかによって異なります。

   - Organizations 内の Detective の委任された管理者アカウントがない場合は、アカウントのアカウント ID を入力して、Detective 管理者アカウントとして指定します。

     手動招待プロセスの既存の管理者アカウントと動作グラフがある場合があります。その場合は、Detective はそのアカウントを Detective 管理者アカウントとして指定することをお勧めします。

     Amazon GuardDuty のOrganizations に委任された管理者アカウントがある場合、AWS Security Hub、または Amazon Macie の場合、Detective はそれらのアカウントのいずれかを選択するように求められます。別のアカウントを入力することもできます。
   - 組織のDetective in Organizationsに委任された管理者アカウントがある場合は、そのアカウントまたはアカウントを選択するように求められます。委任管理者アカウントは、すべてのリージョンで選択することをお勧めします。
5. [Delegate] (委任) を選択します。

探偵管理者アカウントの指定 (Detective API、AWS CLI)

Detective 管理者アカウントを指定するには、API 呼び出しまたはAWS Command Line Interface。組織管理アカウントの認証情報を使用する必要があります。

組織に Detective の委任管理者アカウントをすでに持っている場合は、そのアカウントまたはアカウントを選択する必要があります。Detective は、委任管理者アカウントを選択することをお勧めします。

Detective 管理者アカウントを指定するには (Detective API,AWS CLI)

- Detective API: を使用する`EnableOrganizationAdminAccount`オペレーション. 以下の情報が必要です。AWSDetective 管理者アカウントのアカウント識別子。アカウント ID を取得するには、`ListOrganizationAdminAccounts`オペレーション.
- AWS CLI: コマンドラインで、`enable-organization-admin-account` コマンドを実行します。

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

例

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Detective 管理者アカウントの削除 (コンソール)

Detective コンソールから、Detective 管理者アカウントを削除できます。

Detective 管理者アカウントを削除すると、そのアカウントの Detective が無効になり、組織の動作グラフが削除されます。

Detective 管理者アカウントは、現在のリージョンでのみ削除されます。

Detective 管理者アカウントを削除しても、Organizations の委任された管理者アカウントには影響しません。

Detective 管理者アカウントを削除するには (Detectiveページで)

1. Detective コンソールを開きます。
2. [Get started (開始方法)] を選択します。
3. []委任管理者で、アカウントの削除。
4. 確認ダイアログで、次のように入力します。**`disable`**[] の順に選択します。Amazon Detective。

Detective 管理者アカウントを削除するには (将軍ページで)

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Settings] (設定) の [General] (一般) を選択します。
3. []委任管理者で、アカウントの削除。
4. 確認ダイアログで、次のように入力します。**`disable`**[] の順に選択します。Amazon Detective。

Detective 管理者アカウントの削除 (Detective APIAWS CLI)

Detective 管理者アカウントを削除するには、API 呼び出しまたはAWS CLI。組織管理アカウントの認証情報を使用する必要があります。

Detective 管理者アカウントを削除すると、そのアカウントの Detective が無効になり、組織の動作グラフが削除されます。

Detective API を使用して Detective 管理者アカウントを削除すると、API 呼び出しまたはコマンドが発行されたリージョンでのみ削除されます。Detective 管理者アカウントを削除しても、Organizations 委任された管理者アカウントには影響しません。

Detective 管理者アカウントを削除するには (Detective API、AWS CLI)

- Detective API: を使用する`DisableOrganizationAdminAccount`オペレーション.
- AWS CLI: コマンドラインで、`disable-organization-admin-account` コマンドを実行します。

```
aws detective disable-organization-admin-account
```

委任管理者アカウントの削除 (Organizations API、AWS CLI)

Detective 管理者アカウントを削除すると、そのリージョンでのみ削除されます。Detective 管理者アカウントを削除しても、Organizations 委任された管理者アカウントには影響しません。

Organizations API では、Detective の委任された管理者アカウントを削除できます。これにより、委任された管理者アカウントが Detective 管理者アカウントである組織の動作グラフもすべて削除され、それらのリージョンのアカウントの Detective が無効になります。

委任された管理者アカウント (Organizations API) を削除するにはAWS CLI)

- Organizations API: を使用するDeregisterDelegatedAdministratorオペレーション. Detective 管理者アカウントのアカウント ID と Detective のサービスプリンシパルを指定する必要があります。detective.amazonaws.com。
- AWS CLI: コマンドラインで、deregister-delegated-administrator コマンドを実行します。

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

例

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --service-
principal detective.amazonaws.com
```

アカウントのリストの表示

管理者アカウントは、Detective コンソールまたは API を使用して、アカウントのリストを表示できます。リストには、次のものを含めることができます。

- 管理者アカウントが動作グラフに参加するように招待したアカウント。これらのアカウントには、次のタイプがあります。招待により。
- 組織動作グラフでは、組織内のすべてのアカウント。これらのアカウントには、次のタイプがあります。組織別。

結果には、招待を辞退した招待メンバーアカウントや、動作グラフから削除された管理者アカウントは含まれません。以下のステータスのアカウントのみが含まれます。

[Verification in progress] (検証を実行中)

招待アカウントの場合、Detective は招待を送信する前にアカウントのメールアドレスを検証しています。

組織アカウントの場合、Detective はアカウントが組織に属していることを確認しています。Detective は、アカウントを有効にしたのは Detective 管理者アカウントであることも確認します。

[Verification failed] (検証に失敗しました)

検証に失敗しました。招待が送信されなかったか、組織アカウントがメンバーとして有効になっていませんでした。

[招待済み]

招待されたアカウントの場合。招待は送信されましたが、メンバーアカウントはまだ応答していません。

メンバーではない

組織行動グラフの組織アカウントの場合。組織アカウントは現在、メンバーアカウントではありません。組織動作グラフにデータを提供しません。

有効

招待アカウントの場合、メンバーアカウントは招待を承諾し、動作グラフにデータを提供します。

組織行動グラフの組織アカウントの場合、Detective 管理者アカウントによってアカウントがメンバーアカウントとして有効になりました。アカウントは、組織行動グラフにデータを寄与します。

が有効ではない

招待アカウントの場合、メンバーアカウントは招待を承諾しましたが、有効にできません。

組織の動作グラフの組織アカウントの場合、Detective 管理者アカウントはアカウントを有効にしようとしましたが、アカウントを有効にできません。

このステータスは、次のいずれかの理由で発生します。

- メンバーアカウントが Amazon GuardDuty のお客様になってから 48 時間が経過していません。
- メンバーアカウントのデータにより、動作グラフのデータ量が Detective のクォータを超えることになります。

アカウントのリスト作成 (コンソール)

♪AWS Management Consoleをクリックすると、アカウントのリストを表示してフィルタリングできます。

アカウントのリストを表示するには (コンソール)

1. AWS Management Console にサインインします。その後、https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。

   メンバーアカウントリストには、次のアカウントが含まれています。

   - アカウント
   - 動作グラフにデータを提供するように招待したアカウント
   - 組織行動グラフでは、すべての組織勘定科目

   各アカウントについて、リストには次の情報が表示されます。

   - AWS アカウント識別子。
   - 組織アカウントの場合、アカウント名。
   - アカウントの種類 (招待によりまたは組織別).
   - 招待アカウントの場合、アカウントのルートユーザーの電子メールアドレス。
   - アカウントのステータス。
   - アカウントの日次データ量。Detective は、メンバーアカウントとして有効化されていないアカウントのデータ量を取得できません。
   - アカウントステータスが最後に更新された日付。

テーブルの上部にあるタブを使用して、メンバーアカウントのステータスに基づいてリストをフィルタリングできます。各タブでは、一致するメンバーアカウントの数が表示されます。

- すべてのメンバーアカウントを表示するには、[All] (すべて) を選択します。
- 選択[Enabled (有効)]ステータスが「」のアカウントを表示するには[Enabled (有効)]。
- 選択が有効ではない以外のステータスのアカウントを表示するには[Enabled (有効)]。

メンバーアカウントのリストに他のフィルターを追加することもできます。

動作グラフのアカウントのリストにフィルターを追加するには (コンソール)

1. フィルターボックスを選択します。
2. リストのフィルタリングに使用する列を選択します。
3. 指定した列で、フィルタリングに使用する値を選択します。
4. フィルターを削除するには、右上にある x アイコンを選択します。
5. 最新のステータス情報でリストを更新するには、右上にある更新アイコンを選択します。

メンバーアカウントの一覧表示 (Detective API、AWS CLI)

API 呼び出しを使用することも、AWS Command Line Interfaceをクリックして、動作グラフ内のメンバーアカウントのリストを表示します。

リクエストで使用する動作グラフの ARN を取得するには、`ListGraphs` 操作を使用します。

メンバーアカウントのリストを取得するには (Detective API、AWS CLI)

- Detective API: を使用する`ListMembers`オペレーション. 目的の動作グラフを識別するには、動作グラフ ARN を指定します。

  組織行動グラフの場合、`ListMembers`は、メンバーアカウントとして有効になっていない組織勘定科目、または行動グラフから関連付けを解除した組織アカウントを返しません。
- AWS CLI: コマンドラインで、`list-members` コマンドを実行します。

```
aws detective list-members --graph-arn <behavior graph ARN>
```

例:

```
aws detective list-members --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

動作グラフで特定のメンバーアカウントに関する詳細を取得するには (Detective API、AWS CLI)

- Detective API: を使用する`GetMembers`オペレーション. 動作グラフ ARN とメンバーアカウントのアカウント識別子のリストを指定します。
- AWS CLI: コマンドラインで、`get-members` コマンドを実行します。

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior graph
 ARN>
```

例:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

組織アカウントをメンバーアカウントとして管理する

組織の動作グラフでは、Detective 管理者アカウントは、メンバーアカウントとして有効にする組織アカウントを決定します。

Detective を設定して、新しい組織アカウントをメンバーアカウントとして自動的に有効化したり、組織アカウントを手動で有効にしたりできます。

Detective 管理者アカウントは、組織行動グラフから組織アカウントの関連付けを解除することもできます。

目次

新しい組織アカウントをメンバーアカウントとして自動的に有効にする

Detective 管理者アカウントは、組織の行動グラフで新しい組織アカウントをメンバーアカウントとして自動的に有効にするように Detective を設定できます。

新しいアカウントが組織に追加されると、そのアカウントはアカウント管理ページで. 組織アカウントの場合、タイプです組織別。

デフォルトでは、新しい組織アカウントはメンバーアカウントとして有効になりません。彼らのステータスはです。メンバーではない。

組織アカウントを自動的に有効にすることを選択すると、Detective は新しいアカウントが組織に追加されると、メンバーアカウントとして有効になります。Detective は、まだ有効になっていない既存の組織アカウントを有効にしません。

Detective が組織アカウントをメンバーアカウントとして有効にできるかどうかは、以下によって異なります。

- 動作グラフのメンバーアカウントの最大数は 1,200 です。行動グラフにすでに 1,200 のメンバーアカウントが含まれている場合、新しいアカウントを有効にすることはできません。
- Detective は Amazon GuardDuty が有効になってから 48 時間以上が経過していないアカウントを有効にすることはできません。
- Detective は、動作グラフのデータ量が許容される最大値を超えることになる場合、アカウントを有効にできません。

新しい組織アカウントを自動的に有効にする (コンソール)

リポジトリの []アカウント管理[] ページで次の操作を行います。新しい組織アカウントを自動的に有効にする設定では、組織に追加されたアカウントを自動的に有効にするかどうかを決定します。

新しい組織アカウントをメンバーアカウントとして自動的に有効にするには

1. Detective コンソールを開きます。

2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. 切り替え新しい組織アカウントを自動的に有効にするをオンの位置にします。

新しい組織アカウントを自動的に有効化する (Detective API、AWS CLI)

新しい組織アカウントをメンバーアカウントとして自動的に有効にするかどうかを決定するには、管理者アカウントは Detective API またはAWS Command Line Interface。

設定を表示および管理するには、動作グラフ ARN を指定する必要があります。ARN を取得するには、`ListGraphs`オペレーション.

組織アカウントを自動的に有効にする現在の構成を表示するには

- Detective API: を使用する`DescribeOrganizationConfiguration`オペレーション.

  応答で、新しい組織アカウントが自動的に有効になっている場合は、`AutoEnable`です`true`。
- AWS CLI: コマンドラインで、`describe-organization-configuration` コマンドを実行します。

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

例

```
aws detective describe-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

新しい組織アカウントを自動的に有効にするには

- Detective API: を使用する`UpdateOrganizationConfiguration`オペレーション. 新しい組織アカウントを自動的に有効にするには、`AutoEnable`に`true`。
- AWS CLI: コマンドラインで、`update-organization-configuration` コマンドを実行します。

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN> --auto-
enable | --no-auto-enable
```

例

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

組織アカウントをメンバーアカウントとして有効化する

新しい組織アカウントを自動的に有効にしない場合は、それらのアカウントを手動で有効にできます。また、関連付けを解除したアカウントを手動で有効にする必要があります。

アカウントを有効にできるかどうかの判別

組織行動グラフの有効アカウントが最大 1,200 の場合、組織アカウントをメンバーアカウントとして有効にすることはできません。この場合、組織のアカウントのステータスは残ります。メンバーではない。

組織のアカウントを有効にすると、Detective は、アカウントが Amazon GuardDuty のお客様になってから 48 時間以上が経過しているかどうかを確認します。設定されている場合、Detective は、アカウントデータによって動作グラフのデータレートがクォータを超えていないかどうかを確認します。このチェックには 24 時間から 48 時間かかることがあります。

Detective がデータレートを検証している間、メンバーアカウントのステータスは有効ではありません。

メンバーアカウントがこれらの両方のチェックに合格すると、メンバーアカウントのステータスが [] に更新されます。[Enabled (有効)]。Detective は、メンバーアカウントから動作グラフへのデータの取り込みを開始します。

アカウントがこれらのいずれかのチェックに失敗すると、メンバーアカウントのステータスは残ります。有効ではありません。アカウントは、動作グラフにデータを提供しません。

メンバーアカウントが有効になることが確認されるとすぐに、Detective はメンバーアカウントのステータスを自動的に[Enabled (有効)]。

メンバーアカウントとしての組織アカウントの有効化 (コンソール)

[] からアカウント管理ページでは、組織アカウントをメンバーアカウントとして有効にできます。

組織アカウントをメンバーアカウントとして有効にするには

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. 現在有効になっていないアカウントのリストを表示するには、有効ではありません。
4. 特定の組織アカウントを選択するか、すべての組織アカウントを有効にすることができます。

   選択した組織アカウントを有効にするには、次の手順に従います。

   a. 有効にする各組織アカウントを選択します。
   b. [Enable accounts] (アカウントを有効化) を選択します。

   すべての組織アカウントを有効にするには、すべての組織アカウントを有効にする。

メンバーアカウントとしての組織アカウントの有効化 (Detective API、AWS CLI)

Detective API またはAWS Command Line Interfaceをクリックして、組織の動作グラフで組織アカウントをメンバーアカウントとして有効化します。リクエストで使用する動作グラフの ARN を取得するには、`ListGraphs` 操作を使用します。

メンバーアカウントとして組織アカウントを有効にするには (Detective API、AWS CLI)

- Detective API: を使用する`CreateMembers`オペレーション. グラフ ARN を入力する必要があります。

  アカウントごとに、アカウント ID を指定します。組織行動グラフの組織アカウントには、招待状が届きません。電子メールアドレスやその他の招待情報を入力する必要はありません。
- AWS CLI: コマンドラインで、`create-members` コマンドを実行します。

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-arn <behavior
 graph ARN>
```

例

```
aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012 --
graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

組織アカウントをメンバーアカウントとして関連付け解除する

組織行動グラフで組織アカウントからのデータの取り込みを停止するには、アカウントの関連付けを解除します。そのアカウントの既存のデータは、動作グラフに残ります。

組織アカウントの関連付けを解除すると、ステータスが [] に変わります。メンバーではない。Detective はそのアカウントからのデータの取り込みを停止しますが、アカウントはリストに残ります。

組織アカウントの関連付け解除 (コンソール)

[] からアカウント管理ページでは、組織アカウントをメンバーアカウントとして関連付け解除できます。

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. 有効なアカウントのリストを表示するには、[Enabled (有効)]。
4. 関連付けを解除する各アカウントのチェックボックスをオンにします。
5. [Actions] を選択します。次に [] を選択します。アカウントを無効化する。

   関連付け解除されたアカウントのアカウントステータスがに変わります。メンバーではない。

組織アカウントの関連付け解除 (DDetective API、AWS CLI)

Detective API またはAWS Command Line Interface動作グラフ内の組織アカウントのメンバーアカウントとしての関連付けを解除します。

リクエストで使用する動作グラフの ARN を取得するには、`ListGraphs` 操作を使用します。

組織動作グラフから組織アカウントの関連付けを解除するには (Detective API、AWS CLI)

- Detective API: を使用する`DeleteMembers`オペレーション. グラフ ARN と関連付けを解除するメンバーアカウントのアカウント識別子のリストを指定します。
- AWS CLI: コマンドラインで、`delete-members` コマンドを実行します。

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior graph
 ARN>
```

例

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

招待されたメンバーアカウントの管理

管理者アカウントは、動作グラフにアカウントをメンバーアカウントに招待できます。メンバーアカウントが招待を承諾して有効になると、Amazon Detective は、メンバーアカウントのデータを取り込み、その動作グラフに抽出し始めます。

組織行動グラフ以外の行動グラフでは、すべてのメンバーアカウントが招待アカウントになります。

Detective 管理者アカウントは、組織アカウントではないアカウントを組織行動グラフに招待することもできます。

管理者アカウントは、動作グラフから招待メンバーアカウントを削除できます。

目次

動作グラフへのメンバーアカウントの招待

管理者アカウントは、動作グラフにデータを提供するようにアカウントを招待できます。動作グラフには、最大 1,200 のメンバーアカウントを含めることができます。

動作グラフにデータを提供するようにアカウントを招待するプロセスの概要は次のとおりです。

1. 追加する各メンバーアカウントについて、管理者アカウントは AWS アカウント識別子とルートユーザーのメールアドレスを提供します。
2. Detective は、メールアドレスがアカウントのルートユーザーのメールアドレスであることを検証します。

   Detective は、AWS GovCloud (米国東部) または AWS GovCloud (米国西部) リージョンではこの検証を実行しません。
3. アカウント情報が有効な場合、Detective はメンバーアカウントに招待を送信します。

   Detective は、AWS GovCloud (米国東部) または AWS GovCloud (米国西部) リージョンのメンバーアカウントに招待メールを送信することはありません。

   他のリージョンについては、Detective API には、メンバーアカウントへの招待を送信しないオプションが含まれています。

   このオプションは、一元的に管理されるアカウントに有益です。
4. メンバーアカウントは招待を承諾または辞退します。

   管理者アカウントが招待メールを送信しない場合でも、メンバーアカウントはなお招待に応答する必要があります。
5. メンバーアカウントが招待を承諾すると、Detective は、メンバーアカウントが Amazon GuardDuty のお客様になってから 48 時間以上が経過しているかどうかを確認します。

   48 時間以上が経過している場合、Detective は、メンバーアカウントのデータによって、動作グラフのデータレートがクォータを超えていないかどうかを確認します。

   このチェックには 24 ~ 48 時間かかることがあります。

   Detective がデータレートを検証している間、メンバーアカウントのステータスは有効ではありません。
6. メンバーアカウントがこれらの両方のチェックに合格すると、メンバーアカウントのステータスが自動的に[Enabled (有効)]。Detective は、メンバーアカウントから動作グラフへのデータの取り込みを開始します。

   これらのチェックのいずれかに合格しなかった場合、メンバーアカウントのステータスは残ります有効ではありません。メンバーアカウントは、動作グラフにデータを提供しません。

7. メンバーアカウントが有効になる資格があるとすぐに、Detective はメンバーアカウントのステータスを自動的に[Enabled (有効)]。

   たとえば、メンバーアカウントのステータスは[Enabled (有効)]メンバーアカウントは GuardDuty を有効にし、Detective はデータ量が過多ではないことを検証した場合、または管理者アカウントは、アカウントのためのスペースを確保するために、他のメンバーアカウントを削除します。

   複数のアカウントが有効ではありません[] (Detective) を選択すると、Detective は招待された順にアカウントを有効にします。いずれかを有効にするかどうかをチェックするプロセス有効ではありませんアカウントは 1 時間ごとに実行されます。

   管理者アカウントは、自動プロセスを待つ代わりに、手動でアカウントを有効にすることもできます。例えば、管理者アカウントで、有効にするアカウントを選択できます。「the section called “有効でないメンバーアカウントの有効化” (p. 36)」を参照してください。

   Detective は、以下のアカウントを自動的に有効にするようになったことに注意してください有効ではありません2021 年 5 月 12 日. だったアカウント有効ではありませんそれ以前は自動的に有効になりません。管理者アカウントは、手動で有効にする必要があります。

個々のアカウントの動作グラフへの招待 (コンソール)

動作グラフにデータを提供するように招待するメンバーアカウントを手動で指定できます。

招待するメンバーアカウントを手動で選択するには (コンソール)

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. [Actions] を選択します。その後、[Invite accounts] (アカウントを招待) を選択します。
4. [Add accounts] (アカウントを追加) で、[Add individual accounts] (個別のアカウントを追加) を選択します。
5. 招待リストにメンバーアカウントを追加するには、次のステップを実行します。

   a. [Add account] (アカウントを追加) を選択します。

   b. を使用する場合AWSアカウント IDに、「」と入力します。AWSアカウント ID。

   c. [Email address] (メールアドレス) で、アカウントのルートユーザーのメールアドレスを入力します。
6. リストからアカウントを削除するには、そのアカウントの [Remove] (削除) を選択します。
7. [Personalize invitation email] (招待メールをパーソナライズ) で、招待メールに含めるカスタマイズされたコンテンツを追加します。

   例えば、この領域を使用して、連絡先情報を指定します。または、これを使用して、招待を承諾する前に、必要な IAM ポリシーをユーザーまたはロールにアタッチする必要があることをメンバーアカウントに注意喚起します。
8. [Member account IAM policy] (メンバーアカウントの IAM ポリシー) には、メンバーアカウントに必要な IAM ポリシーのテキストが含まれます。招待メールには、このポリシーテキストが含まれます。ポリシーテキストをコピーするには、[Copy] (コピー) を選択します。
9. [Invite] (招待) を選択します。

メンバーアカウントリストの動作グラフへの招待 (コンソール)

Detective コンソールから、動作グラフに招待するメンバーアカウントのリストを含む `.csv` ファイルを提供できます。

ファイルの最初の行はヘッダー行です。その後、各アカウントは個別の行にリストされます。各メンバーアカウントのエントリには、AWS アカウント ID とアカウントのルートユーザーのメールアドレスが含まれています。

例:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Detective がファイルを処理する際に、アカウントのステータスが [Verification failed] (検証に失敗しました) でない限り、すでに招待されているアカウントは無視されます。このステータスは、アカウント用に提供されたメールアドレスがアカウントのルートユーザーのメールアドレスと一致しなかったことを示唆するものです。その場合、Detective は元の招待を削除し、メールアドレスの検証と招待の送信を再試行します。

このオプションは、アカウントのリストを作成するために使用できるテンプレートも提供します。

.csv リストからメンバーアカウントを招待するには (コンソール)

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. [Actions] を選択します。その後、[Invite accounts] (アカウントを招待) を選択します。
4. [Add accounts] (アカウントを追加) で、[Add from .csv] (.csv から追加) を選択します。
5. 作業するテンプレートファイルをダウンロードするには、[Download .csv template] (.csv テンプレートをダウンロード) を選択します。
6. アカウントのリストを含むファイルを選択するには、[Choose .csv file] (.csv ファイルを選択) を選択します。
7. [Review member accounts] (メンバーアカウントを確認) で、Detective がファイルで見つけたメンバーアカウントのリストを検証します。
8. [Personalize invitation email] (招待メールをパーソナライズ) で、招待メールに含めるカスタマイズされたコンテンツを追加します。

   例えば、連絡先情報を提供したり、メンバーアカウントに必要な IAM ポリシーについて注意喚起したりできます。
9. [Member account IAM policy] (メンバーアカウントの IAM ポリシー) には、メンバーアカウントに必要な IAM ポリシーのテキストが含まれます。招待メールには、このポリシーテキストが含まれます。ポリシーテキストをコピーするには、[Copy] (コピー) を選択します。
10. [Invite] (招待) を選択します。

動作グラフへのメンバーアカウントの招待 (Detective API、AWS CLI)

Detective API または AWS Command Line Interface を使用して、動作グラフにデータを提供するようにメンバーアカウントを招待できます。リクエストで使用する動作グラフの ARN を取得するには、`ListGraphs` 操作を使用します。

動作グラフにメンバーアカウントを招待するには (Detective API、AWS CLI)

- Detective API: を使用する`CreateMembers`オペレーション. グラフ ARN を入力する必要があります。各アカウントについて、アカウント識別子とルートユーザーのメールアドレスを指定します。

  メンバーアカウントに招待メールを送信しないようにするには、`DisableEmailNotification` を true に設定します。デフォルトでは、`DisableEmailNotification` は false です。

招待メールを送信する場合は、オプションで、招待メールに追加するカスタムテキストを入力できます。

- AWS CLI: コマンドラインで、`create-members` コマンドを実行します。

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --message "<Custom message text>"
```

例

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This is Paul
 Santos. I need to add your account to the data we use for security investigation in
 Amazon Detective. If you have any questions, contact me at psantos@example.com."
```

メンバーアカウントに招待メールを送信しないことを示すには、`--disable-email-notification` を含めます。

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --disable-email-notification
```

例

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-notification
```

複数のリージョンにまたがるメンバーアカウントのリストの追加 (GitHub の Python スクリプト)

Detective は、GitHub でオープンソーススクリプトを提供します。これにより、次のことが可能になります。

- 指定リストの複数のリージョンにおける管理者アカウントの動作グラフに、メンバーアカウントの指定リストを追加します。
- あるリージョンで管理者アカウントが動作グラフを有していない場合、スクリプトは Detective を有効にし、そのリージョンに動作グラフを作成します。
- メンバーアカウントに招待メールを送信します。
- メンバーアカウントになるための招待を自動的に承諾します。

GitHub スクリプトの設定方法と使用方法については、Amazon Detective Python スクリプトの使用 (p. 78) を参照してください。

有効でないメンバーアカウントの有効化

メンバーアカウントが招待を承諾した後、Amazon Detective はメンバーアカウントを有効にできるかどうかを確認します。Detective がメンバーアカウントを有効にできない場合は、メンバーアカウントのステータスを有効ではありません。これは、次のいずれかの理由で発生します。

- メンバーアカウントが Amazon GuardDuty のお客様になってから 48 時間が経過していません。

- Detective はメンバーアカウントのデータ量を検証しています。
- メンバーアカウントのデータにより、動作グラフのデータレートがクォータを超えることになります。

メンバーアカウントは有効ではありません動作グラフにデータを提供しないでください。

動作グラフがアカウントに対応できるため、Detective はアカウントを自動的に有効にします。

メンバーアカウントを手動で有効化しようとすることもできます有効ではありませんメンバーアカウント。例えば、既存のメンバーアカウントを削除して、データ量を減らすことができます。自動プロセスでアカウントが有効になるのを待つ代わりに、有効化を試みることができます有効ではありませんメンバーアカウント。

有効ではありません (コンソール) のメンバーアカウントの有効化

メンバーアカウントリストには、選択したメンバーアカウントを有効にするオプションが含まれています有効ではありません。

有効でないメンバーアカウントを有効にするには

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. [My member accounts] (自分のメンバーアカウント) で、有効にする各メンバーアカウントのチェックボックスをオンにします。

   ステータスがのメンバーアカウントのみを有効にできます有効ではありません。
4. [Enable accounts] (アカウントを有効化) を選択します。

Detective は、メンバーアカウントを有効にできるかどうかを判断します。メンバーアカウントを有効にできる場合、ステータスは[Enabled (有効)]。

有効ではありません (Detective API、) のメンバーアカウントの有効化AWS CLI)

API 呼び出しを使用することも、AWS Command Line Interface単一のメンバーアカウントを有効にするには有効ではありません。リクエストで使用する動作グラフの ARN を取得するには、`ListGraphs` 操作を使用します。

有効でないメンバーアカウントを有効にするには

- Detective API: `StartMonitoringMember` API オペレーションを使用します。動作グラフ ARN を指定する必要があります。メンバーアカウントを識別するには、AWS アカウント識別子を使用します。
- AWS CLI:コマンドラインから、`start-monitoring-member`コマンド:

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account ID>
```

例:

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

動作グラフからの招待メンバーアカウントの削除

管理者アカウントは、いつでも動作グラフからメンバーアカウントを削除できます。

Detective は、AWS GovCloud (米国東部) and AWS GovCloud (米国西部) リージョンを除き、AWS で終了したメンバーアカウントを自動的に削除します。

動作グラフから招待メンバーアカウントが削除されると、次のようになります。

- メンバーアカウントが [My member accounts] (自分のメンバーアカウント) から削除されます。
- Amazon Detective は、削除されたアカウントからのデータの取り込みを停止します。

Detective は、メンバーアカウント全体のデータを集約する動作グラフから既存のデータを削除しません。

動作グラフからの招待メンバーアカウントの削除 (コンソール)

♪AWS Management Console[] をクリックして、動作グラフから招待メンバーアカウントを削除します。

メンバーアカウントを削除するには (コンソール)

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. アカウントリストから、削除する各メンバーアカウントのチェックボックスをオンにします。

   リストから自分のアカウントを削除することはできません。
4. [Actions] を選択します。次に [] を選択します。アカウントを無効化する。

動作グラフからの招待メンバーアカウントの削除 (Detective API、AWS CLI)

Detective API またはAWS Command Line Interface[] をクリックして、動作グラフから招待メンバーアカウントを削除します。リクエストで使用する動作グラフの ARN を取得するには、`ListGraphs` 操作を使用します。

動作グラフから招待メンバーアカウントを削除するには (Detective API、AWS CLI)

- Detective API: を使用する`DeleteMembers`オペレーション. グラフ ARN と削除するメンバーアカウントのアカウント識別子のリストを指定します。
- AWS CLI: コマンドラインで、`delete-members` コマンドを実行します。

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior graph
 ARN>
```

例:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

複数のリージョンにまたがる招待メンバーアカウントのリストの削除 (GitHub の Python スクリプト)

Detective は GitHub でオープンソースのスクリプトを提供しています。このスクリプトを使用して、指定されたリージョンのリスト全体で、管理者アカウントの動作グラフから、指定されたメンバーアカウントのリストを削除できます。

GitHub スクリプトの設定方法と使用方法については、Amazon Detective Python スクリプトの使用 (p. 78) を参照してください。

メンバーアカウントの場合: 動作グラフの招待とメンバーシップの管理

Amazon Detective は、データを提供する各動作グラフの取り込みデータについて、各メンバーアカウントに課金します。

-アカウント管理ページでは、メンバーアカウントがメンバーである動作グラフの管理者アカウントを表示できます。

行動グラフに招待されたメンバーアカウントは、招待を表示して返信できます。動作グラフからアカウントを削除することもできます。

組織行動グラフの場合、組織アカウントは、自分のアカウントがメンバーアカウントであるかどうかを制御しません。Detective 管理者アカウントは、メンバーアカウントとして有効または無効にする組織アカウントを選択します。

目次

メンバーアカウントに必要な IAM ポリシー

メンバーアカウントが招待を表示および管理するためには、まず必要な IAM ポリシーをプリンシパルにアタッチする必要があります。プリンシパルは、既存のユーザーまたはロールにすることができるほか、Detective で使用するために新しいユーザーまたはロールを作成することもできます。

理想的には、管理者アカウントが IAM 管理者に必要なポリシーをアタッチするよう依頼します。

メンバーアカウント IAM ポリシーは、Amazon Detective のメンバーアカウントのアクションに対するアクセス権を付与します。動作グラフにデータを提供するよう招待する E メールには、その IAM ポリシーのテキストが含まれています。

このポリシーを使用するには、*<behavior graph ARN>* をグラフ ARN に置き換えます。

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

```
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

組織行動グラフの組織アカウントは招待状を受け取らず、組織の行動グラフからアカウントの関連付けを解除することはできません。他のビヘイビアグラフに属さない場合は、`ListInvitations`のアクセス許可。`ListInvitations`により、動作グラフの管理者アカウントを確認できます。招待を管理し、メンバーシップの関連付けを解除する権限は、招待によるメンバーシップにのみ適用されます。

動作グラフの招待のリストの表示

Amazon Detective コンソール、Detective API、または AWS Command Line Interface から、メンバーアカウントは動作グラフの招待を表示できます。

動作グラフの招待の表示 (コンソール)

AWS Management Console から動作グラフの招待を表示できます。

動作グラフの招待を表示するには (コンソール)

1. AWS Management Console にサインインします。その後、https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。

[Account management] (アカウント管理) ページの [My administrator accounts] (自分の管理者アカウント) には、現在のリージョンで未対応または承諾済みの動作グラフの招待が表示されます。組織アカウントの場合、管理者アカウントまた、組織行動グラフも含まれています。

アカウントが現在無料トライアル期間中の場合、ページには残りの無料トライアル期間 (日数) も表示されます。

このリストには、辞退した招待、辞退したメンバーシップ、または管理者アカウントが削除したメンバーシップは表示されません。

各招待は、管理者アカウント番号、招待が承諾された日、および招待の現在のステータスを表示します。

- 返信していない招待のステータスは [Invited] (招待済み) となります。
- 承諾した招待の場合、ステータスは次のいずれかになります。[Enabled (有効)]または有効ではありません。

  ステータスがである[Enabled (有効)]のアカウントは、動作グラフにデータを提供します。

  ステータスがである有効ではありませんのアカウントは、動作グラフにデータを提供しません。

アカウントのステータスは、最初は有効ではありませんDetective は GuardDuty が有効になっているかどうかを確認し、有効になっている場合は、アカウントにより、動作グラフのデータ量が Detective のクォータを超えることになるかどうかを確認します。

アカウントにより、動作グラフがクォータを超えることにはならない場合、Detective はアカウントのステータスを[Enabled (有効)]。それ以外の場合、ステータスは残ります。有効ではありません。

動作グラフがアカウントのデータ量に対応できる場合、Detective は自動的にそれを[Enabled (有効)]。例えば、管理者アカウントが他のメンバーアカウントを削除して、アカウントを有効にできる場合があります。管理者アカウントは、アカウントを手動で有効にすることもできます。

動作グラフの招待の表示 (Detective API、AWS CLI)

Detective API または AWS Command Line Interface から動作グラフの招待を一覧表示できます。

未対応または承諾済みの動作グラフへの招待のリストを取得するには (Detective API、AWS CLI)

- Detective API: を使用する`ListInvitations`オペレーション.
- AWS CLI: コマンドラインで、`list-invitations` コマンドを実行します。

```
aws detective list-invitations
```

動作グラフの招待への応答

招待を受け入れると、アカウントのステータスは、最初は有効ではありませんDetective は、アカウントにより、動作グラフのデータ量が Detective のクォータを超えることになるかどうかを確認します。Detective がこの確認を実行するには、アカウントで Amazon GuardDuty が有効になってから 48 時間以上が経過している必要があります。

アカウントにより、動作グラフがクォータを超えることにはならない場合、Detective はアカウントのステータスを[Enabled (有効)]。Detective は、その時点で、ログと検出結果から動作グラフへのデータの取り込みと抽出を開始します。アカウントには、データについての料金も請求されます。

アカウントを追加することで動作グラフのデータ量が Detective のクォータを超えることになる場合、または GuardDuty が有効になっていない場合、ステータスは残ります。有効ではありません。この場合、アカウントを削除しない限り、Detective は動作グラフがそれに対応でき次第、自動的にアカウントを有効にします。管理者アカウントは、アカウントを手動で有効にすることもできます。

招待を辞退すると、招待のリストから削除され、Detective は動作グラフのアカウントデータを使用しません。

動作グラフの招待への応答 (コンソール)

AWS Management Console を使用して招待メールに返信できます。このメールには Detective コンソールへのリンクが含まれています。ステータスが [Invited] (招待済み) の招待にのみ返信できます。

動作グラフの招待に応答するには (コンソール)

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. [My administrator accounts] (自分の管理者アカウント) で、招待を承諾して動作グラフへのデータの提供を開始するには、[Accept invitation] (招待を承諾) を選択します。

招待を辞退してリストから削除するには、[Decline] (辞退) を選択します。

動作グラフの招待への応答 (Detective API、AWS CLI)

Detective API または AWS Command Line Interface から動作グラフの招待に応答できます。

動作グラフの招待を承諾するには (Detective API、AWS CLI)

- Detective API: を使用するAcceptInvitationオペレーション. グラフ ARN を指定する必要があります。
- AWS CLI: コマンドラインで、accept-invitation コマンドを実行します。

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

例:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

動作グラフの招待を辞退するには (Detective API、AWS CLI)

- Detective API: を使用するRejectInvitationオペレーション. グラフ ARN を指定する必要があります。
- AWS CLI: コマンドラインで、reject-invitation コマンドを実行します。

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

例:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

動作グラフからのアカウントの削除

招待を承諾した後、いつでも動作グラフからアカウントを削除できます。動作グラフからアカウントを削除すると、Amazon Detective はアカウントから動作グラフへのデータの取り込みを停止します。既存のデータは動作グラフに残ります。

招待アカウントのみが動作グラフからアカウントを削除できます。組織アカウントは、組織の行動グラフから自分のアカウントを削除することはできません。

動作グラフからのアカウントの削除 (コンソール)

AWS Management Console を使用して、動作グラフからアカウントを削除できます。

動作グラフからアカウントを削除するには (コンソール)

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Account management] (アカウント管理) を選択します。
3. [My administrator accounts] (自分の管理者アカウント) で、辞退する動作グラフについて [Resign] (辞退) を選択します。

動作グラフからのアカウントの削除 (Detective API、AWS CLI)

Detective API または AWS Command Line Interface を使用して、動作グラフからアカウントを削除できます。

動作グラフからアカウントを削除するには (Detective API、AWS CLI)

- Detective API: を使用する`DisassociateMembership`オペレーション. グラフ ARN を指定する必要があります。
- AWS CLI: コマンドラインで、`disassociate-membership` コマンドを実行します。

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

例:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

行動グラフに対するアカウントアクションの影響

これらのアクションは、Amazon Detective のデータとアクセスに次の影響を与えます。

Detective が無効

管理者アカウントが Detective を無効にすると、次のようになります。

- ビヘイビアグラフが削除されます。
- Detective は、その動作グラフの管理者アカウントとメンバーアカウントからのデータの取り込みを停止します。

行動グラフから削除されたメンバーアカウント

動作グラフからメンバーアカウントが削除されると、Detective はそのアカウントからのデータの取り込みを停止します。

動作グラフ内の既存のデータは影響を受けません。

招待されたアカウントの場合、アカウントはマイメンバーアカウントリスト。

組織行動グラフの組織アカウントの場合、勘定科目のステータスはメンバーではない。

メンバーアカウントが組織を離れる

メンバーアカウントが組織を離脱すると、次のようになります。

- アカウントは、マイメンバーアカウント組織行動グラフのリストです。
- Detective は、そのアカウントからのデータの取り込みを停止します。

動作グラフ内の既存のデータは影響を受けません。

AWSアカウントの一時停止

で管理者アカウントが一時停止されている場合AWSの場合、アカウントは Detective で行動グラフを表示する権限を失います。Detective は動作グラフへのデータの取り込みを停止します。

でメンバーアカウントが一時停止された場合AWS、Detective はそのアカウントのデータの取り込みを停止します。

90 日後、アカウントは終了または再アクティブ化されます。管理者アカウントが再アクティブ化されると、Detective 権限が復元されます。Detective はアカウントからのデータの取り込みを再開します。メンバーアカウントが再アクティブ化されると、Detective はアカウントからのデータの取り込みを再開します。

AWSアカウント閉鎖

ある時点AWSアカウントが閉鎖され、Detective は閉鎖に次のように応答します。

- 管理者アカウントの場合、Detective は動作グラフを削除します。
- メンバーアカウントの場合、Detective は動作グラフからアカウントを削除します。

AWS は、管理者アカウントの閉鎖の発効日から 90 日間にわたり、そのアカウントのポリシーデータを保持します。90 日の期間の終了時、AWS は、アカウントのすべてのポリシーデータを完全に削除します。

- 結果を 90 日を超えて保持するには、ポリシーをアーカイブします。EventBridge ルールを用いてカスタムアクションを使用して、結果を S3 バケットに保存することもできます。
- AWS がポリシーデータを保持している限り、閉鎖されたアカウントを再度開くと、AWS は、アカウントをサービス管理者として再割り当てし、そのアカウントのサービスポリシーデータを回復します。
- 詳細については、アカウントの解約を参照してください。

> Important
>
> AWS GovCloud (US) リージョンの顧客の場合:
>
> - アカウントを閉鎖する前に、ポリシーデータおよびその他のアカウントリソースをバックアップしてから、削除します。アカウントを閉鎖した後は、もうそのアカウントへのアクセス権はなくなります。

Amazon Detective でのアクションおよび使用量の追跡

Detective のアクティビティの追跡に役立つよう、[Usage] (使用量) のページには、取り込まれたデータの量と予測コストが表示されます。

- 管理者アカウントの場合、[Usage] (使用量) のページには、動作グラフ全体のデータ量と予測コストが表示されます。
- メンバーアカウントの場合、[Usage] (使用量) のページには、メンバーがデータを提供している動作グラフ全体で、自己のアカウントのデータ量と予測コストが表示されます。

また、Detective は AWS CloudTrail ログ記録をサポートしています。

目次

動作グラフの使用量とコストのモニタリング (管理者アカウント)

Amazon Detective は、アカウントが属する各動作グラフで使用されるデータについて、各アカウントに請求します。Detective は、ソースにかかわらず、すべてのデータについて GB あたりの階層的な定額料金を請求します。

管理者アカウントの場合、使用Detective コンソールのページでは、取り込まれたデータの量を表示できますデータソース別またはアカウント別直近 30 日間にわたって。管理者アカウントには、アカウントと動作グラフ全体の通常の 30 日間の予測コストも表示されます。

Detective の使用量に関する情報を表示するには

1. AWS Management Console にサインインします。その後、https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Settings] (設定) の [Usage] (使用量) を選択します。
3. タブを選択して、使用状況を表示するかを選択しますデータソース別またはアカウント別。

各アカウントについて取り込まれるデータの量

[Ingested volume by member account] (メンバーアカウント別の取り込み量) には、動作グラフのアクティブなアカウントが表示されます。削除されたメンバーアカウントはリストに表示されません。

各アカウントについて、取り込み量のリストに次の情報が表示されます。

- AWS アカウント識別子と root ユーザーのメールアドレス。
- アカウントが動作グラフにデータを提供し始めた日。

  管理者アカウントの場合、これはアカウントが Detective を有効にした日です。

  メンバーアカウントの場合、これはアカウントが招待を受け入れた後にメンバーアカウントとして有効になった日です。
- 直近 30 日間にアカウントから取り込まれたデータの量。合計には、すべてのソースタイプが含まれます。
- アカウントが現在、無料トライアル期間中かどうか。現在、無料トライアル期間中のアカウントの場合、リストには残りの日数が表示されます。

  無料トライアル期間中のアカウントがない場合、無料トライアルステータスの列は表示されません。

動作グラフの予測コスト

[This account's projected cost] (このアカウントの予測コスト) には、管理者アカウントの 30 日間のデータの予測コストが示されます。予測コストは、管理者アカウントの 1 日の平均量に基づきます。

> Important
>
> この金額は予測コストのみです。これは、通常の 30 日間の管理者アカウントデータについての合計コストを予測します。直近 30 日間の使用量に基づきます。the section called “Detective による予測コストの計算方法” (p. 47) を参照してください。

動作グラフの予測コスト

[All accounts' projected cost] (すべてのアカウントの予測コスト) には、動作グラフ全体の 30 日間のデータの合計予測コストが示されます。予測コストは、各アカウントの 1 日の平均量に基づきます。

> Important
>
> この金額は予測コストのみです。これは、通常の 30 日間の動作グラフデータについての合計コストを予測します。直近 30 日間の使用量に基づきます。予測コストには、動作グラフから削除されたメンバーアカウントは含まれません。the section called “Detective による予測コストの計算方法” (p. 47) を参照してください。

ソースパッケージによって取り込まれるデータの量

Selectソースパッケージ別をクリックして、ビヘイビアグラフで有効になっているさまざまなソースパッケージによって一覧表示された、取り込まれたデータの量を表示します。

すべてのアカウントは、自分のアカウントのこのデータを表示できます。管理者アカウントは、各メンバーのソースパッケージごとの使用状況を一覧表示する追加のパネルを表示できます。削除されたメンバーアカウントはリストに表示されません。

Detective コア

> Detective コアパネルには、Detectiveのコアソースから取り込まれたデータの量が表示されます（ CloudTrail ログ、VPC フローログ、 GuardDuty の結果 ）の直前の 30 日になります。

EKS 監査ログ

> EKS 監査ログパネルには、過去 30 日間に EKS 監査ログソースから取り込まれたデータの量が表示されます。このソースパッケージのパネルは、行動グラフで EKS 監査ログが有効になっている場合にのみ使用できます。

動作グラフ全体の使用量とコストのモニタリング (メンバーアカウント)

Amazon Detective は、アカウントが属する各動作グラフで使用されるデータについて、各アカウントに請求します。Detective は、ソースにかかわらず、すべてのデータについて GB あたりの階層的な定額料金を請求します。

メンバーアカウントの場合、[Usage] (使用量) のページには、そのアカウントのみのデータ量と 30 日間の予測コストが表示されます。

Detective の使用量に関する情報を表示するには

1. AWS Management Console にサインインします。その後、https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Settings] (設定) の [Usage] (使用量) を選択します。

各動作グラフの取り込み量

[This account's ingested volume] (このアカウントの取り込まれた量) には、メンバーアカウントがデータを提供する動作グラフが示されます。削除したメンバーシップ、または管理者アカウントが削除したメンバーシップは含まれません。

動作グラフごとに、リストには次の情報が含まれています。

- 管理者アカウントのアカウント番号
- 直近 30 日間にメンバーアカウントから取り込まれたデータの量。合計には、すべてのソースタイプが含まれます。
- 動作グラフについてメンバーアカウントが有効になった日。

動作グラフ全体の予測コスト

[This account's projected cost] (このアカウントの予測コスト) は、メンバーアカウントがデータを提供するすべての動作グラフにおけるメンバーアカウントの 30 日間のデータの予測コストを示します。予測コストは、メンバーアカウントの 1 日の平均量に基づきます。

> **Important**
>
> この金額は予測コストのみです。これは、通常の 30 日間の管理者アカウントデータについての合計コストを予測します。直近 30 日間の使用量に基づきます。the section called “Detective による予測コストの計算方法” (p. 47) を参照してください。

Amazon Detective による予測コストの計算方法

[Usage] (使用量) のページに表示される予測コストの値を計算するために、Detective は次を実行します。

1. 動作グラフで個々のアカウントの予測コストを取得するために、Detective は次を実行します。
   a. 1 日あたりの平均量を計算します。すべてのアクティブな日のデータ量を加えて、アカウントがアクティブであった日数で除します。

      アカウントが有効になってから 30 日を超える期間が経過している場合、日数は 30 日です。アカウントが有効になってから 30 日よりも短い期間しか経過していない場合、受入日以降の日数です。

例えば、アカウントが 12 日前に有効にされた場合、Detective はそれらの 12 日間に取り込まれた量を追加し、それを 12 で除します。

b. アカウントの 1 日の平均に 30 を乗じます。これはアカウントの 30 日間の予測使用量です。

c. 料金モデルを使用して、30 日間の予測使用量についての 30 日間の予測コストを計算します。

2. 動作グラフの合計予測コストを取得するために、Detective は次を実行します。

a. 動作グラフのすべてのアカウントの 30 日間の予測使用量を組み合わせます。

b. 料金モデルを使用して、30 日間の合計予測使用量についての 30 日間の予測コストを計算します。

3. 動作グラフ全体でメンバーアカウントの合計予測コストを取得するために、Detective は次を実行します。

a. すべての動作グラフの 30 日間の予測使用量を組み合わせます。

b. 料金モデルを使用して、30 日間の合計予測使用量についての 30 日間の予測コストを計算します。

での Amazon Detective API コールのログ記録AWS CloudTrail

Detective は、AWS CloudTrail と統合されています。これは、Detective のユーザー、ロール、または AWS のサービスで実行されたアクションを記録するためのサービスです。CloudTrail は、Detective 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、Detective コンソールの呼び出しと、Detective 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、Detective 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 [Event history] (イベント履歴) で最新のイベントを表示できます。

CloudTrail によって収集されたデータを使用して、以下の情報を判断できます。

- Detective に対して実行されたリクエスト
- リクエストが行われた IP アドレス
- リクエストを行ったユーザー
- リクエストが行われた時刻
- リクエストに関するその他の詳細

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。

CloudTrail の Detective に関する情報

CloudTrailは、アカウントを作成すると AWS アカウントで有効になります。Detective 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 のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。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。

Detective 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、コンソールで追跡を作成するときに、追跡がすべてのAWSリージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントを ログに記録し、明記した Amazon S3 バケットにログファイルを配信します。その他の AWS のサービスを設定して、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づく対応を行うこともできます。

詳細については、以下を参照してください:

- [Overview for Creating a Trail] (追跡を作成するための概要)
- CloudTrailのサポート対象サービスと統合
- Amazon SNSのCloudTrailの通知の設定
- 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

CloudTrail は、Detective API リファレンスに記載されているすべての Detective 操作をログに記録します。

例えば `CreateMembers`、`AcceptInvitation`、`DeleteMembers` の各演算へのコールは、CloudTrail ログファイル内にエントリを生成します。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。この ID 情報は以下のことを確認するのに役立ちます。

- リクエストが、ルートと AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか
- リクエストが、別の AWS のサービスによって送信されたかどうか

詳細については、CloudTrail userIdentity エレメントを参照してください。

Detective のログファイルエントリの理解

追跡は、指定したAmazon S3バケットにイベントをログファイルとして配信するように設定できるものです。CloudTrail ログファイルには、1 つ以上のログエントリがあります。

イベント は、任意の送信元からの単一の要求を表します。イベントには、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、エントリは特定の順序では表示されません。

次の例は、`AcceptInvitation` アクションを証明するCloudTrail· ログエントリです。


```
     {
           "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
           "Username": "JaneRoe",
           "EventTime": 1571956406.0,
           "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":{\"type
\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS:JaneRoe\",\"arn\":
\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",\"accountId\":
\"111122223333\",\"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",\"sessionContext\":{\"attributes
\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\"2019-10-24T21:54:56Z\"},
\"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS\",\"arn
\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",\"accountId\":\"111122223333\",
\"userName\":\"JaneRoe\"}}},\"eventTime\":\"2019-10-24T22:33:26Z\",\"eventSource\":
\"detective.amazonaws.com\",\"eventName\":\"AcceptInvitation\",\"awsRegion\":\"us-
east-2\",\"sourceIPAddress\":\"192.0.2.123\",\"userAgent\":\"aws /3 aws-sdk-java/1.11.648
 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.201-b09 java/1.8.0_201
 vendor/Oracle_Corporation exec-env/AWS_Lambda_java8\",\"errorCode\":\"ValidationException
\",\"requestParameters\":{\"masterAccount\":\"111111111111\"},\"responseElements\":
{\"message\":\"Invalid request body\"},\"requestID\":\"8437ff99-5ec4-4b1a-8353-173be984301f
\",\"eventID\":\"f2545ee3-170f-4340-8af4-a983c669ce37\",\"readOnly\":false,\"eventType\":
\"AwsApiCall\",\"recipientAccountId\":\"111122223333\"}",
```

```
            "EventName": "AcceptInvitation",
            "EventSource": "detective.amazonaws.com",
            "Resources": []
        },
```

動作グラフのタグの管理

動作グラフにタグを割り当てることができます。その後、IAM ポリシーのタグ値を使用して、Detective の動作グラフの機能へのアクセスを管理できます。「the section called “Detective の動作グラフのタグに基づく承認” (p. 62)」を参照してください。

また、タグをコストレポートのためのツールとして使用することもできます。例えば、セキュリティに関連するコストを追跡するために、同じタグを Detective の動作グラフ、AWS Security Hub ハブのリソース、および Amazon GuardDuty のディテクターに割り当てることができます。AWS Cost Explorer で、そのタグを検索して、これらのリソース全体のコストの統合ビューを表示できます。

動作グラフのタグの表示 (コンソール)

動作グラフのタグは、[General] (全般) ページから管理します。

動作グラフに割り当てられているタグを表示するには

1. Detective コンソールを開きます。
2. ナビゲーションペインで [Settings] の [General] を選択します。

動作グラフのタグの一覧表示 (Detective API、AWS CLI)

Detective API または AWS Command Line Interface を使用して、動作グラフのタグのリストを取得できます。

動作グラフのタグのリストを取得するには (Detective API、AWS CLI)

- Detective API: を使用する`ListTagsForResource`オペレーション. 動作グラフの ARN を入力する必要があります。
- AWS CLI: コマンドラインで、`list-tags-for-resource` コマンドを実行します。

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

例

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

動作グラフへのタグの追加 (コンソール)

[General] (全般) ページのタグリストから、動作グラフにタグ値を追加できます。

動作グラフにタグを追加するには

1. [新しいタグを追加] をクリックします。

2. [Key] (キー) で、タグの名前を入力します。
3. [Value] (値) で、タグの値を入力します。

動作グラフへのタグの追加 (Detective API、AWS CLI)

Detective API または AWS CLI を使用して、動作グラフにタグ値を追加できます。

動作グラフにタグを追加するには (Detective API、AWS CLI)

- Detective API: を使用する`TagResource`オペレーション. 動作グラフ ARN と追加するタグ値を入力します。
- AWS CLI: コマンドラインで、`tag-resource` コマンドを実行します。

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior graph
 ARN> --tags '{"TagName":"TagValue"}'
```

例

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

動作グラフからのタグの削除 (コンソール)

[General] (全般) ページのリストからタグを削除するには、そのタグの [Remove] (削除) オプションを選択します。

動作グラフからのタグの削除 (Detective API、AWS CLI)

Detective API または AWS CLI を使用して、動作グラフからタグ値を削除できます。

動作グラフからタグを削除するには (Detective API、AWS CLI)

- Detective API: を使用する`UntagResource`オペレーション. 動作グラフ ARN と削除するタグの名前を入力します。
- AWS CLI: コマンドラインで、`untag-resource` コマンドを実行します。

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys "TagName"
```

例

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Amazon Detective 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のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWSお客様の間の共有責任です。共有責任モデルでは、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して説明しています。

- クラウドのセキュリティ - AWS は、AWS クラウドで AWS 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、安全に使用できるサービスを供給します。

  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。

  Amazon Detective に適用されるコンプライアンスプログラムについては、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–お客様の責任は、使用するAWSのサービスに応じて判断されます。また、お客様は、データの機密性、お客様の会社の要件、および適用可能な法律および規制など、そ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、Detective 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ために Detective を設定する方法を示します。また、Detective リソースのモニタリングや保護に役立つ、他の AWS のサービスの使用方法についても説明します。

目次

Amazon Detective でのデータ保護

Amazon Detective でのデータ保護には、AWS の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、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を担います。ご利用者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、のセキュリティ設定と管理タスクが含まれます。AWS のサービスおれが使っていること。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 Identity and Access Management(IAM)を使用して個々のユーザーアカウント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アクセス許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします:

- 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 以降が推奨されています。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS暗号化ソリューションをAWSサービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- Amazon Macieなどのアドバンストマネージドセキュリティサービスを使用します。これは、Amazon S3に保存されている個人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 を使用して AWS にアクセスするときに FIPS 140-2の検証を受けた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、[Federal Information Processing Standard (FIPS) 140-2] (連邦情報処理規格 (FIPS) 140-2) を参照してください。

顧客のメールアドレスなどの機密または注意を要する情報は、タグや [Name] (名前) フィールドなど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。これは、コンソール、API、AWS CLI、または AWS SDK で Detective または他の AWS サービスを使用する場合も同様です。タグまたは名前に使用する自由記入欄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。q

Detective は、保管中および転送中、処理および保存するすべてのデータを暗号化します。

内容

Amazon Detective のキー管理

Detective は個人の特定が可能な顧客データを保存しないため、AWS マネージドキー を使用します。

このタイプの KMS キーは、複数のアカウントで使用できます。AWS Key Management Service デベロッパーガイドの AWS 所有キーの説明を参照してください。

このタイプの KMS キーは、3 年 (1095 日) ごとに自動的にローテーションします。AWS Key Management Service デベロッパーガイドのキーのローテーションの説明を参照してください。

Amazon Detective のための 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、誰を認証 (サインイン) し、誰に Detective リソースの使用を承認する (許可を付与する) 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。

目次

対象者

AWS Identity and Access Management (IAM) の用途は、Detective で行う作業によって異なります。

サービスユーザー – ジョブを実行するために Detective サービスを使用する場合は、管理者から必要な許可と認証情報が与えられます。作業を実行するためにさらに多くの Detective の特徴を使用するとき、追加の許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Detective の特徴にアクセスできない場合は、Amazon Detective アイデンティティとアクセスのトラブルシューティング (p. 67) を参照してください。

サービス管理者 - 社内の Detective リソースを担当している場合は、通常、Detective へのフルアクセスがあります。サービスユーザーがどの Detective の特徴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管理者のジョブです。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許可を変更する必要があります。このページの情報を確認して、IAM の基本概念を理解してください。貴社が Detective で IAM を利用する方法の詳細については、Amazon Detective で IAM が機能する仕組み (p. 59) を参照してください。

IAM 管理者 – IAM 管理者は、Detective へのアクセスを管理するポリシーの、作成方法の詳細を確認する場合があります。IAM で使用できる Detective アイデンティティベースのポリシーの例を表示するには、Amazon Detective のアイデンティティベースポリシーの例 (p. 63) を参照してください。

アイデンティティを使用した認証

認証とは、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。AWS Management Console を使用したサインインの詳細については、「IAM ユーザーガイド」の「IAM ユーザーまたはルートユーザーとして AWS Management Console にサインインする」を参照してください。

ユーザーは AWS のルートユーザーもしくは IAM 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、認証を受ける (AWS アカウント にサインインする) 必要があります。会社のシングルサインオン認証を使用したり、Google や Facebook を使用したりしてサインインすることもできます。このような場合、管理者が事前に IAM ロールを使用して ID フェデレーションを設定している必要があります。他の会社の認証情報を使用して AWS にアクセスした場合、ロールは間接的に割り当てられています。

AWS Management Console に直接サインインするには、パスワードとルートユーザーの E メールまたは IAM ユーザー名を使用します。ルートユーザーまたは IAM ユーザーのアクセスキーを使用して AWS にプログラムからアクセスできます。AWS では、ユーザーの認証情報を使用してリクエストに暗号的に署名するための SDK とコマンドラインツールが提供されます。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。これには、インバウンド API リクエストを認証するためのプロトコルである署名バージョン 4 を使用します。リクエストの認証の詳細については、「AWS 全般のリファレンス」の「署名バージョン 4 の署名プロセス」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を要求される場合もあります。例えば、AWS は、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用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「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 ルートユーザー

AWS アカウント を作成する場合は、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 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、AWS 全般のリファレンスの「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持つ 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 ユーザーと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、次を参照してください。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()IAM ユーザーガイド。

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許可を指定できます。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許可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って、AWS Management Console で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、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 ID にアクセス許可を割り当てるには、ロールを作成し、ロールのアクセス許可を定義します。フェデレーティッド ID が認証されると、ID はロールに関連付けられ、ロールで定義されているアクセス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、以下を参照してください。サードパーティー ID プロバイダーのロールの作成()IAM ユーザーガイド。

  IAM アイデンティティセンターを使用する場合、許可セットを設定します。認証後に ID が何にアクセスできるかを制御するために、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、アクセス権限セット()AWS IAM Identity Center (successor to AWS Single Sign-On)ユーザーガイド。
- 一時的な IAM ユーザー許可— 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許可を一時的に 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を許可する主な方法は、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添付できます。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、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、またはサービスにリンクされたロールを使用してこれを行う場合があります。

- プリンシパル許可 - 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みなされます。ポリシーによって、プリンシパルに許可が付与されます。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。この場合、両方のアクションを実行するための許可が必要です。アクションがポリシーで追加の依存アクションを必要とするかどうかを確認するには、サービス認証リファレンスの Amazon Detective 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 にアクセス許可を委任するロールの作成」を参照してください。
- サービスにリンクされたロール - サービスにリンクされたロールは、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 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、サービスにリンクされた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。

- 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「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。

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

ポリシーを使用したアクセスの管理

AWS でアクセスをコントロールするには、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。ポリシーでの許可により、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 AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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。

すべての IAM エンティティ (ユーザーまたはロール) は、許可のない状態からスタートします。デフォルトでは、ユーザーは何もできず、自分のパスワードを変更することすらできません。何かを実行する許可をユーザーに付与するには、管理者がユーザーに許可ポリシーを添付する必要があります。また、管理者は、必要な許可があるグループにユーザーを追加できます。管理者がグループに許可を付与すると、そのグループ内のすべてのユーザーにこれらの許可が付与されます。

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。このポリシーがあるユーザーは、AWS Management Console、AWS CLI、または AWS API からロールの情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティに添付できる 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。マネージドポリシーは、AWS アカウント 内の複数のユーザー、グループ、およびロールに添付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マネージド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。ポリシーが添付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、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 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コントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Simple Storage Service (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、その他の一般的ではないポリシータイプも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た最大の許可を設定できます。

- 許可の境界 - 許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる許可の上限を設定する高度な機能です。エンティティに許可の境界を設定できます。結果として許可される範囲は、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、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、許可は無効になります。許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの許可の境界」を参照してください。
- サービスコントロールポリシー (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、お客様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 ではメンバーアカウントのエンティティ (各 AWS アカウント ルートユーザーなど) に対する許可が制限されます。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許可される範囲は、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許可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、許可は無効になります。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許可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。

Amazon Detective で IAM が機能する仕組み

Detective は IAM アイデンティティベースのポリシーを使用して、次のタイプのユーザーおよびアクションについての許可を付与します。

- 管理者アカウント — 管理者アカウントは、アカウントのデータを使用する動作グラフの所有者です。管理者アカウントは、動作グラフにデータを提供するよう、メンバーアカウントを招待することもできます。また、動作グラフは、これらのアカウントに関連する検出結果とリソースのトリアージおよび調査にも使用します。

  管理者アカウントの異なるユーザーが異なるタイプのタスクを実行できるよう、異なるポリシーを設定できます。例えば、管理者アカウントのユーザーは、メンバーアカウントを管理するための許可しか付与されていない場合があります。別のユーザーは、調査のために動作グラフを使用するための許可しか付与されていない場合があります。
- メンバーアカウント — メンバーアカウントは、動作グラフにデータを提供するように招待されるアカウントです。メンバーアカウントは招待に応答します。招待を承諾した後、メンバーアカウントは動作グラフから自分のアカウントを削除できます。

Detective およびその他の AWS のサービスが IAM と連携する方法の概要を把握するには、IAM ユーザーガイドの IAM と連携する AWS のサービスを参照してください。

Detective 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。Detective は、特定のアクション、リソース、および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 ポリシーの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許可を付与するポリシーで使用されます。

ポリシーステートメントには、`Action` 要素または `NotAction` 要素を含める必要があります。`Action` 要素は、ポリシーによって許可されるアクションをリストします。`NotAction` 要素は、許可されていないアクションをリストします。

Detective のために定義されたアクションには、Detective を使用して実行できるタスクが反映されます。Detective のポリシーアクションには、プレフィックス `detective:` が付いています。

例えば、`CreateMembers` API 操作を使用してメンバーアカウントを動作グラフに招待するための許可を付与するには、`detective:CreateMembers` アクションをポリシーに含めます。

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。例えば、メンバーアカウントの場合、ポリシーには、招待の管理に関連する一連のアクションが含まれます。

```
"Action": [
      "detective:ListInvitations",
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

複数のアクションを指定するために、ワイルドカード (*) を使用することもできます。例えば、動作グラフで使用されるデータを管理するには、Detective の管理者アカウントが次のタスクを実行できる必要があります。

- メンバーアカウントのリストを表示する (`ListMembers`)。
- 選択したメンバーアカウントに関する情報を取得する (`GetMembers`)。
- メンバーアカウントを動作グラフに招待する (`CreateMembers`)。
- 動作グラフからメンバーを削除する (`DeleteMembers`)。

これらのアクションを個別にリストする代わりに、`Members` という単語で終わるすべてのアクションへのアクセス権を付与できます。それについてのポリシーには、次のアクションが含まれます。

```
"Action": "detective:*Members"
```

Detective アクションのリストを確認するには、サービス認証リファレンスの Amazon Detective で定義されるアクションを参照してください。

リソース

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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、オブジェクトあるいはアクションが適用されるオブジェクトを指定します。ステートメントには、`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの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、リソースレベルの許可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": "*"
```

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

Detective の場合、リソースタイプは動作グラフのみです。Detective の動作グラフのリソースの ARN は次のとおりです。

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

例えば、動作グラフには以下の値があります。

- 動作グラフのリージョンは `us-east-1` です。
- 管理者アカウント ID のアカウント ID は `111122223333` です。
- 動作グラフのグラフ ID は `027c7c4610ea4aacaf0b883093cab899` です。

`Resource` ステートメントでこの動作グラフを識別するには、次の ARN を使用します。

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

`Resource` ステートメントで複数のリソースを指定するには、コンマを使用してそれらを区切ります。

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

例えば、同じ AWS アカウントを、複数の動作グラフのメンバーアカウントになるよう招待することができます。そのメンバーアカウントのポリシーでは、`Resource` ステートメントは、招待された動作グラフをリストします。

```
"Resource": [
      "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

動作グラフの作成、動作グラフの一覧表示、動作グラフの招待の一覧表示など、Detective のいくつかのアクションは、特定の動作グラフでは実行されません。これらのアクションについては、`Resource` ステートメントはワイルドカード (*) を使用する必要があります。

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

管理者アカウントのアクションについては、Detective は、リクエストを実行するユーザーが、影響を受ける動作グラフの管理者アカウントに属していることを毎回確認します。メンバーアカウントのアクションについては、Detective は、リクエストを実行するユーザーが、メンバーアカウントに属していることを毎回確認します。IAM ポリシーが動作グラフへのアクセス権を付与しても、ユーザーが正しいアカウントに属していない場合、ユーザーはアクションを実行できません。

特定の動作グラフで実行されるすべてのアクションについて、IAM ポリシーにはグラフ ARN が含まれている必要があります。グラフ ARN は後で追加できます。例えば、アカウントが最初に Detective を有効にする際に、初期 IAM ポリシーは、グラフ ARN のワイルドカードを使用して、すべての Detective アクションに対するアクセスを提供します。これにより、ユーザーはすぐにメンバーアカウントの管理を開始し、動作グラフで調査を実施できます。動作グラフを作成したら、ポリシーを更新してグラフ ARN を追加できます。

条件キー

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがど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することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の `Condition` 要素を指定する場合、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。単一の条件キーに複数の値を指定する場合、AWS では `OR` 論理演算子を使用して条件を評価します。ステートメントの許可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許可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。

Detective は独自の一連の条件キーを定義しません。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。

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、Amazon Detective で定義されるアクションを参照してください。

例

Detective アイデンティティベースのポリシーの例を表示するには、Amazon Detective のアイデンティティベースポリシーの例 (p. 63) を参照してください。

Detective リソースベースのポリシー (サポートされていません)

Detective では、 リソースベースのポリシーはサポートされていません。

Detective の動作グラフのタグに基づく承認

各動作グラフには、タグ値を割り当てることができます。条件ステートメントでこれらのタグ値を使用して、動作グラフへのアクセスを管理できます。

タグ値についての条件ステートメントは、次の形式を使用します。

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

例えば、次のコードを使用して、`Department` タグの値が `Finance` の場合にアクションを許可または拒否します。

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

リソースタグ値を使用するポリシーの例については、the section called “管理者アカウント: タグ値に基づくアクセスの制限” (p. 66) を参照してください。

Detective 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。

Detective 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、AWS STSなどの API オペレーションAssumeRoleまたはGetFederationToken。

Detective では、一時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

サービスにリンクされたロールは、AWS サービスが他のサービスのリソースにアクセスして自動的にアクションを完了することを許可します。サービスにリンクされたロールは 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、サービスにリンクされた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。

Detective サービスにリンクされたロールの作成または管理の詳細については、the section called “サービスリンクロールの使用” (p. 69)。

サービスロール (サポートされていません)

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、サービスがユーザーに代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービスロールは、IAM アカウントに表示され、アカウントによって所有されます。つまり、IAM 管理者が、このロールの許可を変更することができます。ただし、これを行うことにより、サービスの機能が損なわれる場合があります。

Detective は、サービスロールをサポートしていません。

Amazon Detective のアイデンティティベースポリシーの例

デフォルトでは、IAM ユーザーおよびロールには、Detective リソースを作成または変更する許可はありません。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もできません。

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。その後、管理者はそれらの許可が必要な IAM ユーザーまたはグループにそのポリシーをアタッチします。

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

ポリシーのベストプラクティス

ID ベースのポリシーにより、アカウント内で、Detective リソースを作成、アクセス、または削除できるか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 に追加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 マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの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のために許可を付与する 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 カスタマーマネージド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することができます。また、AWS のサービス などの特定の 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、次を参照してください。IAM JSON ポリシー要素: Condition()IAM ユーザーガイド。
- IAM Access Analyzer 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 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 Access Analyzer 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を作成できるようサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – 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。

Detective コンソールの使用

Amazon Detective コンソールを使用するには、ユーザーまたはロールが、関連するアクションであって、API の対応するアクションに一致するアクションにアクセスできる必要があります。

Detective を有効にして動作グラフの管理者アカウントになるには、ユーザーまたはロールに `CreateGraph` アクションについての許可を付与する必要があります。

Detective コンソールを使用して管理者アカウントのアクションを実行するには、ユーザーまたはロールに `ListGraphs` アクションについての許可を付与する必要があります。これにより、アカウントが管理者アカウントである動作グラフを取得するための許可が付与されます。また、特定の管理者アカウントのアクションを実行するための許可を付与する必要があります。

管理者アカウントの最も基本的なアクションは、動作グラフでメンバーアカウントのリストを表示したり、調査のために動作グラフを使用したりすることです。

- 動作グラフでメンバーアカウントのリストを表示するには、プリンシパルに `ListMembers` アクションについての許可が付与されている必要があります。
- 動作グラフで調査を実施するには、プリンシパルに `SearchGraph` アクションについての許可が付与されている必要があります。

Detective コンソールを使用してメンバーアカウントのアクションを実行するには、ユーザーまたはロールに `ListInvitations` アクションについての許可を付与する必要があります。これにより、動作グラフの招待を表示するための許可が付与されます。その後、特定のメンバーアカウントのアクションについての許可を付与できます。

ユーザー自身のアクセス許可を表示することをユーザーに許可する

この例では、ユーザーアイデンティティに添付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を作成する方法を示します。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アクセス許可が含まれています。

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

管理者アカウント: 動作グラフでのメンバーアカウントの管理

このサンプルポリシーは、動作グラフで使用されるメンバーアカウントの管理のみを担当する管理者アカウントのユーザー向けのものです。また、このポリシーは、ユーザーが使用量に関する情報を表示したり、Detective を無効化したりすることを許可します。このポリシーは、動作グラフを調査に使用するための許可を付与しません。

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteGraph","d
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
```

```
 ]
}
```

管理者アカウント: 調査のための動作グラフの使用

このサンプルポリシーは、調査のみに動作グラフを使用する管理者アカウントのユーザー向けのものです。動作グラフでメンバーアカウントのリストを表示したり、編集したりすることはできません。

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
   },
   {
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

メンバーアカウント: 動作グラフの招待とメンバーシップの管理

このサンプルポリシーは、メンバーアカウントに属するユーザー向けのものです。この例では、メンバーアカウントは 2 つの動作グラフに属しています。ポリシーは、招待に応答したり、動作グラフからメンバーアカウントを削除したりするための許可を付与します。

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
       "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
       "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

管理者アカウント: タグ値に基づくアクセスの制限

次のポリシーは、動作グラフの `SecurityDomain` タグがユーザーの `SecurityDomain` タグと一致する場合に、ユーザーが調査のために動作グラフを使用することを許可します。

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Allow",
        "Action":["detective:SearchGraph"],
```

```
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals"{
                "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":["detective:ListGraphs"],
        "Resource":"*"
    } ]
}
```

次のポリシーは、動作グラフの `SecurityDomain` タグの値が `Finance` である場合に、ユーザーが調査のために動作グラフを使用できないようにします。

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

Amazon Detective アイデンティティとアクセスのトラブルシューティング

次の情報は、Detective 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。

Detective でアクションを実行する権限がない

AWS Management Console から、アクションを実行することが認可されていないと通知された場合、管理者に問い合わせ、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。

次のエラー例は、`mateojackson` IAM ユーザーがコンソールを使用して、動作グラフのメンバーアカウントになるための招待を受け入れようとしたが、`detective:AcceptInvitation` 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: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

この場合、Mateo は、`detective:AcceptInvitation` アクションを使用して `arn:aws:detective:us-east-1:444455556666:graph:567856785678` リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

iam を実行する認可がないPassRole

を実行する権限がないというエラーが表示された場合`iam:PassRole`アクション、Detective にロールを渡すことができるようにポリシーを更新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せずに、既存のロールをサービスに渡すことが許可されています。そのためには、サービスにロールを渡す許可が必要です。

以下の例のエラーは、`marymajor` という IAM ユーザーがコンソールを使用して Detective 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アクセス許可が必要です。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、メアリー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 管理者に問い合わせてください。サインイン資格情報を提供した担当者が管理者です。

アクセスキーを表示したい

IAM ユーザーアクセスキーを作成した後は、いつでもアクセスキー ID を表示できます。ただし、シークレットアクセスキーを再表示することはできません。シークレットアクセスキーを紛失した場合は、新しいキーペアを作成する必要があります。

アクセスキーは、アクセスキー ID (例: `AKIAIOSFODNN7EXAMPLE`) とシークレットアクセスキー (例: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`) の 2 つの部分から構成されています。ユーザー名とパスワードと同様に、リクエストを認証するために、アクセスキー ID とシークレットアクセスキーの両方を使用する必要があります。ユーザー名とパスワードと同様に、アクセスキーを安全に管理してください。

> Important
>
> 正規のユーザー ID を確認するためであっても、アクセスキーをサードパーティーに提供しないでください。提供すると、第三者がアカウントへの永続的なアクセスを取得する場合があります。

アクセスキーペアを作成する場合、アクセスキー ID とシークレットアクセスキーを安全な場所に保存するように求めるプロンプトが表示されます。このシークレットアクセスキーは、作成時にのみ使用できます。シークレットアクセスキーを紛失した場合、IAM ユーザーに新しいアクセスキーを追加する必要があります。アクセスキーは最大 2 つまで持つことができます。既に 2 つある場合は、新しいキーペアを作成する前に、いずれかを削除する必要があります。手順を表示するには、「IAM ユーザーガイド」の「アクセスキーの管理」を参照してください。

管理者として Detective へのアクセスを他のユーザーに許可したい

Detective へのアクセスを他のユーザーに許可するには、アクセスを必要とする人またはアプリケーションの IAM エンティティ (ユーザーまたはロール) を作成する必要があります。ユーザーまたはアプリケーションは、このエンティティの認証情報を使用して AWS にアクセスします。その後、Detective の適切な許可を付与するポリシーを、そのエンティティにアタッチする必要があります

すぐにスタートするには、「IAM ユーザーガイド」の「IAM が委任した初期のユーザーおよびグループの作成」を参照してください。

自分の AWS アカウント以外のユーザーに Detective 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ユーザーが、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することができます。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。

- Detective がこれらの機能をサポートしているかどうかを確認するには、Amazon Detective で IAM が機能する仕組み (p. 59) 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「第三者が所有する AWS アカウント へのアクセス権を付与する」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。

Detective のサービスにリンクされたロールの使用

Amazon DetectiveAWS Identity and Access Management(IAM)サービスリンクロール。サービスにリンクされたロールは、Detective に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは Detective によって事前定義されており、サービスから Other を呼び出すために必要なすべてのアクセス許可を備えています。AWSお客様に代わってのサービス。

サービスにリンクされたロールを使用すると、Detective の設定が簡単になります。これは必要なアクセス許可を手動で追加する必要がなくなるためです。Detective は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、Detective のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティに添付することはできません。

サービスリンクロールは、まずその関連リソースを削除しなければ削除できません。これにより、リソースへの意図しないアクセスによるアクセス許可の削除が防止され、Detective リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携する AWS のサービス」で「サービスにリンクされたロール」列が「はい」になっているサービスを検索してください。そのサービス用のサービスリンクロールを表示するためのリンクで、[Yes] (はい) を選択します。

Detective のサービスにリンクされたロールのアクセス許可

Detective は、という名前のサービスにリンクされたロールを使用します。AWSサービスロールフォーディテクティブ— Detective がアクセスを許可するAWS Organizationsお客様に代わっての情報。

AWSServiceRoleForDetective サービスリンクロールは、ロールを引き受ける上で次のサービスを信頼します。

- `detective.amazonaws.com`

AWSserviceRoleForDetective サービスリンクロールは、管理ポリシーを使用します。`AmazonDetectiveServiceLinkedRolePolicy` (p. 72)。

サービスリンクロールの作成、編集、削除をIAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。詳細については、IAM ユーザーガイドのサービスにリンクされたロールのアクセス許可を参照してください。

Detective のサービスにリンクされたロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。組織のDetective 管理者アカウントを指定するとAWS Management Consoleとすると、AWS CLI、またはAWSAPI、Detective はサービスにリンクされたロールを自動的に作成します。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。組織のDetective 管理者アカウントを指定すると、Detective によってサービスにリンクされたロールが再び作成されます。

Detective のサービスにリンクされたロールの編集

Detective では、AWSServiceRoleForDetective サービスリンクロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAMを使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイドのサービスにリンクされたロールの編集を参照してください。

Detective のサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> Note
>
> リソースを削除する際に Detective サービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから再度オペレーションを実行してください。

AWSServiceRoleForDetective で使用されている探偵リソースを削除するには

1. Detective 管理者アカウントを削除します。「the section called “Detective 管理者アカウントの指定” (p. 21)」を参照してください。
2. Detective 管理者アカウントを指定した各リージョンでこのプロセスを繰り返します。

IAM を使用して、サービスにリンクされたロールを手動で削除するには

IAM コンソールを使用して、AWS CLI、またはAWSAWSServiceRoleForDetective サービスリンクロールを削除するには API。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの削除」を参照してください。

Detective サービスリンクロールがサポートされるリージョン

Detective は、このサービスが利用可能なすべてのリージョンで、サービスにリンクされたロールの使用をサポートしています。詳細については、「AWS リージョンとエンドポイント」を参照してください。

Amazon Detective の AWS マネージドポリシー

ユーザー、グループ、ロールにアクセス権限を追加するには、自分でポリシーを作成するよりも、AWS マネージドポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマー管理ポリシーを作成するには、時間と専門知識が必要です。すぐに使用を開始するために、AWS管理ポリシーを使

用することができます。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 マネージドポリシーの詳細については、IAM ユーザーガイドのAWS マネージドポリシーを参照してください。

AWS のサービスは、AWS マネージドポリシーを維持し、更新します。AWS 管理ポリシーのアクセス許可を変更することはできません。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管理ポリシーにアクセス許可が追加されることがあります。この種類の更新は、ポリシーが添付されている、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 管理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 管理ポリシーからの許可を削除しないため、ポリシーの更新によって既存の許可が破棄されることはありません。

加えてAWSでは、複数のサービスにまたがるジョブ機能のための管理ポリシーもサポートしています。たとえば、`ViewOnlyAccess` AWS管理ポリシーは、多数のユーザーに読み取り専用アクセスを提供します。AWS のサービスとリソース。あるサービスで新しい機能を立ち上げる場合は、AWS 追加された演算とリソースに対し、読み取り専用のアクセス許可を設定します。職務ポリシーのリストと説明については、IAM ユーザーガイドの「職務のための AWS マネージドポリシー」を参照してください。

AWS 管理ポリシー: AmazonDetectiveFullAccess[]

`AmazonDetectiveFullAccess` ポリシーはあなたの IAM アイデンティティに添付できます。

このポリシーは、プリンシパルにすべての Detective アクションへのフルアクセスを許可する管理者許可を付与します。このポリシーは、アカウントのために Detective を有効にする前にプリンシパルにアタッチできます。Detective Python スクリプトを実行して動作グラフを作成および管理するために使用されるロールにアタッチする必要もあります。

これらの許可が付与されているプリンシパルは、メンバーアカウントを管理し、動作グラフにタグを追加し、調査に Detective を使用できます。アーカイブできますGuardDuty検出結果。ポリシーは、AWS Organizations にあるアカウントのアカウント名を表示するために Detective コンソールが必要とする許可も提供します。

同意の詳細

このポリシーには、以下の同意が含まれています。

- `detective` – プリンシパルに Detective のすべてのアクションへのフルアクセスを許可します。
- `organizations` – プリンシパルが組織内のアカウントに関する AWS Organizations の情報から取得することを許可します。アカウントが組織に属している場合、これらの許可は、Detective コンソールがアカウント番号に加えてアカウント名を表示することを許可します。
- `guardduty`— プリンシパルのアーカイブを許可するGuardDutyDetective の中からの調査結果。

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

```
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ArchiveFindings"
            ],
            "Resource": "arn:aws:guardduty:*:*:detector/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListDetectors"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 管理ポリシー: AmazonDetectiveServiceLinkedRolePolicy[]

IAM エンティティに `AmazonDetectiveServiceLinkedRolePolicy` をアタッチすることはできません。このポリシーは、ユーザーに代わって Detective がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、「the section called “サービスリンクロールの使用” (p. 69)」を参照してください。

このポリシーは、サービスにリンクされたロールが組織のアカウント情報を取得することを許可する、管理アクセス許可を付与します。

同意の詳細

このポリシーには、以下の同意が含まれています。

- `organizations`— 組織のアカウント情報を取得します。

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

AWS マネージドポリシーの Detective の更新

Detective の AWS 管理ポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更に関する自動通知については、の RSS フィードを購読してください。ドキュメント履歴 (p. 84)。

変更	説明	日付
AmazonDetectiveServiceLinkedRolePolicy (p. 42) – 新しいポリシー	Detective は、サービスにリンクされたロールに新しいポリシーを追加しました。 このポリシーは、サービスにリンクされたロールが組織内のアカウントに関する情報を取得することを許可します。	2021 年 12 月 16 日
Detective は変化を追跡し始めました	Detective が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 5 月 10 日

Amazon Detective でのログ記録とモニタリング

Amazon Detective は、統合された AWS CloudTrail です。CloudTrail は、Detective 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。

Detective で CloudTrail のログ記録を使用する方法の詳細については、the section called “CloudTrail を用いて Detective API コールをログに記録する” (p. 48) を参照してください。

Amazon Detective のコンプライアンス検証

Detective は AWS コンプライアンスプログラムの対象範囲外です。

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

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

AWS では、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティ & コンプライアンスクイックリファレンスガイド – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、AWS でセキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイするためのステップが記載されています。
- 『AWS Config デベロッパーガイド』の「Evaluating resources with rules」- AWS Config サービスは、リソース設定が社内の慣行、業界のガイドライン、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– AWS のこのサービスは、AWS 内でのユーザーのセキュリティ状態に関する包括的な見解を提供し、業界のセキュリティ標準、およびベストプラクティスに対するコンプライアンスを確認するために役立ちます。

Amazon Detective の回復力

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に構築されます。AWS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・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 Global Infrastructure] (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 グローバルインフラストラクチャに加えて、Detective は、Amazon DynamoDB と Amazon Simple Storage Service (Amazon S3) に組み込まれている回復力を利用します。

Detective のアーキテクチャは、単一のアベイラビリティーゾーンの障害に対する回復力も備えています。この回復力は Detective に組み込まれており、いかなる設定も必要ありません。

Amazon Detective 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 Amazon Detective はAWSで説明されているグローバルネットワークセキュリティ手順Amazon Web Services: セキュリティプロセスの概要ホワイトペーパー。

AWS が発行している API コールを使用して、ネットワーク経由で Detective にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降を推奨します。また、Ephemeral Diffie-Hellman (DHE)や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)などの Perfect Forward Secrecy (PFS)を使用した暗号スイートもクライアントでサポートされている必要があります。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。アクセスキーの詳細については、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。

必要に応じて、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。

Amazon Detective のセキュリティベストプラクティス

Detective には、独自のセキュリティポリシーを開発および実装する際に考慮する必要のあるいくつかのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションに相当するものではありません。これらのベストプラクティスはお客様の環境に適切ではないか、十分ではない場合があるため、これらは処方箋ではなく、有用な考慮事項と見なしてください。

Detective については、セキュリティのベストプラクティスは、動作グラフにおけるアカウントの管理に関連しています。

管理者アカウントのベストプラクティス

動作グラフにメンバーアカウントを招待するときは、自分が監督するアカウントのみを招待します。

動作グラフへのアクセスを制限します。ユーザーが動作グラフにアクセスできる場合、これらのユーザーはメンバーアカウントのすべての検出結果を表示できます。このような検出結果には、機密性の高いセキュリティ情報が含まれている場合があります。

メンバーアカウントのベストプラクティス

動作グラフへの招待を受け取ったら、招待元を検証してください。

招待を送信した管理者アカウントの AWS アカウント識別子を確認してください。アカウントの所属先が判明していること、および招待元のアカウントがセキュリティデータをモニタリングする正当な理由を有していることを検証します。

Amazon Detective の無効化

動作グラフの管理者アカウントは、Detective コンソール、Detective API、または AWS Command Line Interface から Amazon Detective を無効にすることができます。Detective を無効にすると、動作グラフとそれに関連する Detective データが削除されます。

動作グラフは、一度削除されると復元できません。

目次

Detective の無効化 (コンソール)

AWS Management Console から Amazon Detective を無効にできます。

Detective を無効にするには (コンソール)

1. Detective コンソールを開きます。
2. Detective のナビゲーションペインで、[Settings] (設定) の [General] (一般) を選択します。
3. [General] (全般) ページの [Disable Detective] (Detective を無効化) で、[Disable Detective] (Detective を無効化) を選択します。
4. 確認を求められたら、**`disable`** と入力します。
5. [Disable Detective] (Detective を無効化) を選択します。

Detective の無効化 (Detective API、AWS CLI)

Detective API または AWS Command Line Interface から Amazon Detective を無効にできます。リクエストで使用する動作グラフの ARN を取得するには、`ListGraphs` 操作を使用します。

Detective を無効化するには (Detective API、AWS CLI)

- Detective API: を使用する`DeleteGraph`オペレーション. グラフ ARN を入力する必要があります。
- AWS CLI: コマンドラインで、`delete-graph` コマンドを実行します。

```
aws detective delete-graph --graph-arn <graph ARN>
```

例:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

リージョン全体での Detective の無効化 (GitHub の Python スクリプト)

Detective は、GitHub でオープンソーススクリプトを提供します。これにより、指定されたリージョンのリスト全体で管理者アカウントのために Detective を無効にできます。

GitHub スクリプトの設定方法と使用方法については、Amazon Detective Python スクリプトの使用 (p. 78) を参照してください。

Amazon Detective Python スクリプトの使用

Amazon Detective は、で一連のオープンソース Python スクリプトを提供します GitHub 倉庫Amazon探偵-マルチアカウントスクリプト。スクリプトには Python 3 が必要です。

これらを使用して、次のタスクを実行できます。

- リージョン全体で管理者アカウントのために Detective を有効にします。

  Detective を有効にすると、動作グラフにタグ値を割り当てることができます。
- リージョン全体で管理者アカウントの動作グラフにメンバーアカウントを追加します。
- オプションで、メンバーアカウントに招待メールを送信します。招待メールを送信しないようにリクエストを設定することもできます。
- リージョン全体で管理者アカウントの動作グラフからメンバーアカウントを削除します。
- リージョン全体で管理者アカウントのために Detective を無効にします。管理者アカウントが Detective を無効にすると、各リージョンでの管理者アカウントの動作グラフが無効になります。

enableDetective.py スクリプトの概要

enableDetective.py スクリプトは次のことを実行します。

1. 指定された各リージョンで管理者アカウントが Detective をまだ有効にしていない場合は、そのリージョンで管理者アカウントのために Detective を有効にします。

   スクリプトを使用して Detective を有効にすると、動作グラフにタグ値を割り当てることができます。
2. オプションで、各動作グラフについて、管理者アカウントから指定されたメンバーアカウントに招待を送信します。

   招待メールのメッセージはデフォルトのメッセージコンテンツを使用するため、カスタマイズすることはできません。

   招待メールを送信しないようにリクエストを設定することもできます。
3. メンバーアカウントになるための招待を自動的に承諾します。

   スクリプトは自動的に招待を承諾するため、メンバーアカウントはこれらのメッセージを無視できます。

   メンバーアカウントに直接連絡して、招待が自動的に承諾されることを通知することをお勧めします。

disableDetective.py スクリプトの概要

disableDetective.py スクリプトは、指定されたリージョン全体で、管理者アカウントの動作グラフから、指定されたメンバーアカウントを削除します。

また、指定されたリージョン全体で、管理者アカウントのために Detective を無効にするオプションも提供します。

スクリプトに必要な許可

スクリプトを実行するには、管理者アカウントと、追加または削除するすべてのメンバーアカウントに既存の AWS ロールが存在している必要があります。

Note

ロール名は、すべてのアカウントで同じである必要があります。

IAM ポリシー推奨ベストプラクティス最小スコープの役割を使用することです。スクリプトのワークフローを実行するにはグラフの作成,メンバーの作成, およびグラフへのメンバーの追加必要なアクセス許可は次のとおりです。

- Detective: グラフの作成
- Detective: メンバーの作成
- 探偵:DeleteGraph
- Detective: メンバーの削除
- 探偵:リストグラフ
- Detective: メンバーのリスト
- 探偵:招待を受け入れる

ロールの信頼関係

ロールの信頼関係は、インスタンスまたはローカルの認証情報がロールを引き受けることを許可する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

必要な許可が付与されている共通のロールがない場合、少なくともそれらの許可が付与されているロールを各メンバーアカウントに作成する必要があります。管理者アカウントでもロールを作成する必要があります。

ロールを作成する場合は、必ず次を実行してください。

- すべてのアカウントで同じロール名を使用します。
- 上記の必要な権限を追加するか (推奨)、AmazonDetectiveFullAccess管理ポリシー。
- 上で説明したように、ロールの信頼関係ブロックを追加します。

このプロセスを自動化するために、`EnableDetective.yaml` AWS CloudFormation テンプレートを使用できます。テンプレートはグローバルリソースのみを作成するため、どのリージョンでも実行できます。

Python スクリプトの実行環境の設定

スクリプトは EC2 インスタンスまたはローカルマシンのいずれかから実行できます。

EC2 インスタンスの起動と設定

スクリプトを実行するための 1 つのオプションは、EC2 インスタンスからスクリプトを実行することです。

EC2 インスタンスを起動して設定するには

1. 管理者アカウントで EC2 インスタンスを起動します。EC2 インスタンスを起動する方法の詳細については、Linux インスタンス向け Amazon EC2 ユーザーガイドの Amazon EC2 Linux インスタンスの開始方法を参照してください。
2. インスタンスが管理者アカウント内で `AssumeRole` を呼び出せるようにするための許可が付与されている IAM ロールをインスタンスにアタッチします。

   `EnableDetective.yaml` AWS CloudFormation テンプレートを使用した場合は、`EnableDetective` という名前のプロファイルを持つインスタンスロールが作成されています。

   それ以外の場合、インスタンスロールの作成については、ブログ投稿の Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console を参照してください。
3. 必要なソフトウェアをインストールします。

   - APT: `sudo apt-get -y install python3-pip python3 git`
   - RPM: `sudo yum -y install python3-pip python3 git`
   - Boto (最小バージョン 1.15): `sudo pip install boto3`
4. リポジトリのクローンを EC2 インスタンスに作成します。

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

スクリプトを実行するためのローカルマシンの設定

スクリプトはローカルマシンからも実行できます。

スクリプトを実行するようにローカルマシンを設定するには

1. `AssumeRole` を呼び出す許可を持つ管理者アカウントについて、ローカルマシンの認証情報を設定していることを確認してください。
2. 必要なソフトウェアをインストールします。

   - Python 3
   - Boto (最小バージョン 1.15)
   - GitHub スクリプト

プラットフォーム	セットアップ手順
Windows	1. Python 3 をインストールします (https://www.python.org/downloads/windows/)。 2. コマンドプロントを開きます。 3. Boto をインストールするには、`pip install boto3` を実行します。 4. スクリプトのソースコードを GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).

プラットフォーム	セットアップ手順
Mac	1. Python 3 をインストールします (https://www.python.org/downloads/mac-osx/)。 2. コマンドプロントを開きます。 3. Boto をインストールするには、`pip install boto3` を実行します。 4. スクリプトのソースコードを GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Linux	1. Python 3 をインストールするには、次のいずれかを実行します。 • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. Boto をインストールするには、`sudo pip install boto3` を実行します。 3. https://github.com/aws-samples/amazon-detective-multiaccount-scripts からスクリプトのソースコードのクローンを作成します。

追加または削除するメンバーアカウントの .csv リストの作成

動作グラフに追加したり、動作グラフから削除したりするメンバーアカウントを特定するには、アカウントのリストを含む .csv ファイルを提供します。

各アカウントを別々の行に一覧表示します。各メンバーアカウントのエントリには、AWS アカウント ID とアカウントのルートユーザーのメールアドレスが含まれています。

次の例を参照してください。

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

enableDetective.py の実行

enableDetective.py スクリプトは、EC2 インスタンスまたはローカルマシンから実行できます。

Mac で **enableDetective.py**

1. .csv ファイルを EC2 インスタンスまたはローカルマシンの amazon-detective-multiaccount-scripts ディレクトリにコピーします。
2. amazon-detective-multiaccount-scripts ディレクトリを変更します。
3. enableDetective.py スクリプトを実行します。

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
disable_email
```

スクリプトを実行すると、次の値を置き換えます。

administratorAccountID

管理者アカウントの AWS アカウント ID。

roleName

管理者アカウントと各メンバーアカウントで引き受ける AWS ロールの名前。

inputFileName

管理者アカウントの動作グラフに追加するメンバーアカウントのリストを含む .csv ファイルの名前。

tagValueList

(オプション) 新しい動作グラフに割り当てるタグ値のコンマ区切りのリスト。

各タグ値の形式は *key*=*value* です。例:

```
--tags Department=Finance,Geo=Americas
```

regionList

(オプション) メンバーアカウントを管理者アカウントの動作グラフに追加するリージョンのコンマ区切りのリスト。例:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

管理者アカウントは、リージョンで Detective をまだ有効にしていない可能性があります。その場合、スクリプトは Detective を有効にして、管理者アカウント用に新しい動作グラフを作成します。

リージョンのリストを提供しない場合、スクリプトは Detective がサポートするすべてのリージョンで機能します。

--disable_email

(オプション) 含まれている場合、Detective はメンバーアカウントに招待メールを送信しません。

disableDetective.py の実行

disableDetective.py スクリプトは、EC2 インスタンスまたはローカルマシンから実行できます。

Mac で **disableDetective.py**

1. .csv ファイルを amazon-detective-multiaccount-scripts ディレクトリへコピーします。
2. この .csv ファイルを使用して、指定されたリージョンのリスト全体で、管理者アカウントの動作グラフからリストされたメンバーアカウントを削除するには、次のように disableDetective.py スクリプトを実行します。

```
disabledetective.py --master_account administratorAccountID --assume_role roleName --
input_file inputFileName --disabled_regions regionList
```

3. すべてのリージョンで管理者アカウントのために Detective を無効にするには、--delete-master フラグを併用して disableDetective.py スクリプトを実行します。

```
disabledetective.py --master_account administratorAccountID --assume_role roleName --
input_file inputFileName --disabled_regions regionList --delete_master
```

スクリプトを実行すると、次の値を置き換えます。

administratorAccountID

管理者アカウントの AWS アカウント ID。

roleName

管理者アカウントと各メンバーアカウントで引き受ける AWS ロールの名前。

inputFileName

管理者アカウントの動作グラフから削除するメンバーアカウントのリストを含む .csv ファイルの名前。

Detective を無効にしている場合でも、.csv ファイルを提供する必要があります。

regionList

(オプション) 次のいずれかを実行するリージョンのコンマ区切りリスト:

- 管理者アカウントの動作グラフからメンバーアカウントを削除します。
- --delete-master フラグが含まれている場合は、Detective を無効にします。

例:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

リージョンのリストを提供しない場合、スクリプトは Detective がサポートするすべてのリージョンで機能します。

Detective 管理ガイドのドキュメント履歴

次の表は、このガイドの更新履歴を示しています。

変更	説明	日付
新しいオプションのデータソースを追加しました	Detective は、オプションのデータソースパッケージとして EKS 監査ログをサポートするようになりました。管理者アカウントは、既存の動作グラフに対してこの新しいデータソースを有効にできます。この日付以降に作成されたグラフでは、このデータソースがデフォルトで有効になります。データソースはいつでも手動で無効にできます。	2022 年 7 月 26 日
AWS Organizations との統合を追加	Detective がOrganizations に統合されました。 組織管理アカウントは、組織の Detective 管理者アカウントを指定します。 Detective 管理者アカウントは、組織内のすべてのアカウントを表示し、組織の行動グラフでそれらのアカウントをメンバーアカウントとして有効にすることができます。	2021 年 12 月 16 日
Detective の新しいサービスリンクロールと管理ポリシー	Detective がサービスにリンクされたロールを持っている`AWSServiceRoleForDetective`。サービスにリンクされたロールは、ユーザーの代わりに Organizations データにアクセスするために使用されます。ロールは新しい`AmazonDetectiveServiceLinkedRolePolicy`マネージドポリシー。	2021 年 12 月 16 日
動作グラフのデータ量のクォータの値を更新しました	動作グラフのデータ量のクォータを引き上げました。 1 日あたり 3.24 TB で、Detective は警告を発します。 1 日あたり 3.6 TB で、新しいアカウントを動作グラフに追加することができなくなります。	2021 年 6 月 10 日

変更	説明	日付
	1 日あたり 4.5 TB で、Detective は動作グラフへのデータの取り込みを停止します。	
Python スクリプトのオプションにタグ値を追加しました	Detective Python スクリプト `enableDetective.py` を使用して Detective を有効にする際に、動作グラフにタグ値を割り当てることができるようになりました。	2021 年 5 月 19 日
データ量のチェックに合格したメンバーアカウントの自動的な有効化を追加しました	メンバーアカウントが招待を承諾すると、そのデータによって動作グラフのデータ量がクォータを超えるものではないことを Detective が検証するまで、そのステータスは [Accepted (Not enabled)] (承諾済み (有効ではありません)) となります。 データ量に問題がない場合、Detective は、自動的にステータスを [Accepted (Enabled)] (承諾済み (有効)) に変更します。 現在 [Accepted (Not enabled)] (承諾済み (有効ではありません)) の既存のメンバーアカウントは、自動的に有効にできないことに注意してください。	2021 年 5 月 12 日
セキュリティの章にマネージドポリシーに関する情報を追加しました	セキュリティの章の新しいセクションでは、Detective のマネージドポリシーについて詳しく説明しています。 Detective では現在、単一のマネージドポリシー `AmazonDetectiveFullAccess` を使用できます。	2021 年 5 月 10 日
メンバーアカウントリストのデータ量の値を変更しました	アカウント管理ページで、メンバーアカウントリストに各メンバーアカウントの日次データ量が表示されるようになりました。 これまで、リストには、許可されたデータの総量の割合としてデータ量が表示されていました。	2021 年 4 月 29 日

変更	説明	日付
メンバーアカウントの管理オプションを改定しました	[Manage accounts] (アカウントを管理) メニューを [Actions] (アクション) メニューに置き換えました。 個々のアカウントを追加したり、.csv ファイルからアカウントを追加したりするためのオプションを組み合わせました。 [Enable accounts] (アカウントを有効化) を [Manage accounts] (アカウントの管理) から [Actions] (アクション) の横の個別のオプションに移動しました。	2021 年 4 月 5 日
動作グラフのタグおよびタグに基づく承認を追加しました	Detective を有効にすると、動作グラフにタグを追加できます。 動作グラフのタグは、[General] (全般) ページから管理できます。 Detective は、タグ値に基づく認証もサポートしています。	2021 年 3 月 31 日
AWS GovCloud (US) リージョンの違いを追加しました	Detective は、AWS GovCloud (US) リージョンで利用できるようになりました。 In (イン)AWS GovCloud (米国東部) およびAWS GovCloud (米国西部)、Detective がメンバーアカウントに招待メールを送信することはありません。 Detective は、AWS で終了するメンバーアカウントも自動的に削除しません。	2021 年 3 月 24 日
メンバーアカウントのステータスに基づいてメンバーアカウントのリストをフィルタリングするためのタブが追加されました	メンバーアカウントのリストに、メンバーアカウントのステータスに基づいてリストをフィルタリングするために使用できるタブが表示されるようになりました。 すべてのメンバーアカウント、ステータスが [Accepted (Enabled)] (承諾済み (有効)) のメンバーアカウント、またはステータスが [Accepted (Enabled)] (承諾済み (有効)) 以外のメンバーアカウントを表示できます。	2021 年 3 月 16 日

変更	説明	日付
招待メールを抑制するオプションを Python スクリプトに追加しました	Detective `enableDetective.py` スクリプトで `--disable_email` オプションが利用できるようになりました。 このオプションを含めると、Detective は、メンバーアカウントに招待メールを送信しません。	2021 年 2 月 26 日
メンバーアカウントに招待メールを送信しない API オプションを追加しました	Detective API を使用してメンバーアカウントを追加する場合、管理者アカウントは、メンバーアカウントに招待メールを送信しないことを選択できます。	2021 年 2 月 25 日
「マスターアカウント」という用語を「管理者アカウント」に変更しました。	「マスターアカウント」という用語が「管理者アカウント」に変更されました。この用語は、Detective コンソールと API でも変更されます。	2021 年 2 月 25 日
動作グラフのデータ量のクォータの値を追加しました	動作グラフのデータ量のクォータに特定のクォータ値を追加しました。	2020 年 12 月 11 日
メンバーアカウントのクォータが 1,200 に引き上げられました	マスターアカウントは、最大 1,200 のメンバーアカウントを動作グラフに招待できるようになりました。これまで、クォータは 1,000 でした。	2020 年 12 月 11 日
メンバーアカウントが使用量と予測コストを表示できるようになりました	メンバーアカウントは、各自の使用量に関する情報を表示できるようになりました。メンバーアカウントについては、[Usage] (使用量) ページには、メンバーアカウントがデータを提供する各動作グラフに取り込まれたデータの量が表示されます。メンバーアカウントは、30 日間の予測コストも表示できます。	2020 年 5 月 26 日
無料トライアルは、動作グラフごとではなくアカウントごとになりました	各アカウントの Amazon Detective は、各リージョン内で個別の無料トライアルを受け取るようになりました。無料トライアルは、アカウントが Detective を有効にしたとき、またはアカウントがメンバーアカウントとして初めて有効になったときに開始されます。	2020 年 5 月 26 日

変更	説明	日付
Amazon Detective の一般公開リリース	Detective は一般的にご利用いただけるようになりました。	2020 年 3 月 31 日
新しいオープンソース Python スクリプト GitHub (p. 78)	新しいamazon-detective-multiaccount-scriptsrepository GitHub は、リージョン全体の動作グラフを管理するために使用できるオープンソースの Python スクリプトを提供します。 マスターアカウントのために Detective を有効にしたり、動作グラフにメンバーアカウントを追加したり、動作グラフからメンバーアカウントを削除したり、マスターアカウントのために Detective を無効にしたりできます。	2020 年 1 月 21 日
Amazon Detective のご紹介 (プレビュー)	Detective は、機械学習と専用のビジュアライゼーションを使用して、アマゾン ウェブ サービス (AWS) のワークロード全体のセキュリティ問題を分析および調査するのに役立ちます。 Detective は現在プレビューで提供中です。	2019 年 12 月 3 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。