aws

ユーザーガイド

Amazon Detective

Amazon Detective: ユーザーガイド

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 を使用すると、最長 1 年間の履歴イベントデータにアクセスできるようになりました。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によって表示されます。Detective GuardDuty はこれらの変化を調査結果に関連付けます。Detective のソースデータの詳細については、「the section called “動作グラフで使用されるソースデータ”」を参照してください。

Amazon Detective では、データを自動的に集約し、視覚的なツールを提供することで、セキュリティ調査をより迅速かつ効率的に実施できます。潜在的な問題をすばやく分析し、セキュリティ上の脅威の範囲を判断できます。

トピック

Amazon Detective の特徴

Amazon Detective AWS が環境内の疑わしいアクティビティを調査し、リソースを分析してセキュリティ問題の根本原因を特定するのに役立つ主な方法をいくつか紹介します。

Detective 検索グループ

Detective 検索グループを使用すると、潜在的なセキュリティイベントに関連する複数のアクティビティを調べることができます。検索グループを使用すると、 GuardDuty 重要度の高い結果の根

本原因を分析できます。 AWS 脅威アクターがお客様の環境を侵害しようとすると、通常、一連のアクションを実行して、複数のセキュリティ結果や異常な動作が発生します。

Detective の検索グループページには、検索グループページの行動グラフから抽出された関連するすべての検索グループが表示されます。さまざまなプリンシパルタイプ (IAM ユーザーや IAM ロールなど) の証拠を確認できます。一部の証拠タイプでは、[すべてのアカウント] について証拠を確認できます。

Detective では、各検出グループをインタラクティブに視覚化できるため、セキュリティの問題をより迅速かつ詳細に調査できます。このビジュアライゼーションは、セキュリティインシデントに関係するエンティティと調査結果を表示するように設計されているため、関連性や根本原因を理解しやすくなります。これにより、問題をより迅速に、より少ない労力で徹底的に調査できます。検出結果グループの [視覚化] パネルには、検出結果グループに含まれる検出結果とエンティティが表示されます。

Detective 調査による結果の優先順位付け

Detective Investigation では、セキュリティ侵害の指標を使用して IAM ユーザーと IAM ロールを調査できます。これは、リソースがセキュリティインシデントに関与しているかどうかを判断するのに役立ちます。侵害のインジケータ (IOC) とは、ネットワーク、システム、または環境内で観察され、悪意のあるアクティビティまたはセキュリティインシデントを (高い信頼性レベルで) 特定できるアーティファクトです。Detective 調査により、効率を最大化し、セキュリティ上の脅威に集中し、インシデント対応能力を強化することができます。

Detective Investigationは、機械学習モデルとスレッドインテリジェンスを使用して最も重大で疑わしい問題のみを特定し、高レベルの調査に集中できるようにします。 AWS 環境内のリソースを自動的に分析して、侵害や疑わしいアクティビティの兆候を特定します。これにより、パターンを特定し、どのリソースがセキュリティイベントの影響を受けるかを把握できるため、脅威の特定と軽減に対する積極的なアプローチが可能になります。

Detective コンソールから [Detective 調査の実行] を使用してDetective 調査を開始できます。調査をプログラムで実行するには、Detective API StartInvestigationの操作を使用します。 AWS Command Line Interface (AWS CLI) を使用している場合は、start-Investigation コマンドを実行してください。

Amazon セキュリティレイクとのDetective 統合

Detective は Amazon セキュリティレイクと統合されているため、セキュリティレイクに保存されている未加工のログデータをクエリして取得できます。このインテグレーションにより、Security Lake がネイティブにサポートしている以下のソースからログとイベントを収集できます。

- AWS CloudTrail 管理イベント
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs

Detective をセキュリティレイクと統合すると、Detective AWS CloudTrail は管理イベントと Amazon VPC フローログに関連する未加工のログをセキュリティレイクから取得し始めます。未加工のログをクエリして、Detective のログとイベントを表示できます。

VPC フロー量の調査

Detective を使用すると、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと Kubernetes ポッドの仮想プライベートクラウド (VPC) ネットワークフローのアクティビティの詳細をインタラクティブに調べることができます。Detective は、監視対象アカウントから VPC フローログを自動的に収集し、EC2 インスタンスごとに集計し、これらのネットワークフローに関する視覚的な概要と分析を表示します。

EC2 インスタンスについては、[Overall VPC flow volume] (全体的な VPC のフロー量) のアクティビティの詳細には、選択した時間範囲中の EC2 インスタンスと IP アドレス間のインタラクションが表示されます。

Kubernetes ポッドの場合、[全体的な VPC フロー量] には、すべての送信先 IP アドレスについて、Kubernetes ポッドによって割り当てられた IP アドレスに出入りするバイト総数が表示されます。

Amazon Detective へのアクセス

Amazon Detective AWS リージョンはほとんどの地域でご利用いただけます。Detective が現在利用できるリージョンのリストについては、の「Amazon Detective エンドポイントとクォータ」を参照してください。AWS 全般のリファレンス AWS リージョン の管理については AWS アカウント、『リファレンスガイド』の「AWS リージョン アカウントで使用できるアカウントの指定」を参照してください。AWS Account Management

各地域では、以下のいずれかの方法でDetective と協力することができます。

AWS Management Console

AWS Management Console は、リソースの作成と管理に使用できるブラウザベースのインターフェースです。 AWS そのコンソールの一部として、Amazon Detective コンソールは Detective アカウント、データ、およびリソースへのアクセスを提供します。Detective コンソールを使用す

ると、潜在的なセキュリティ脅威を確認し、セキュリティ結果の根本原因を分析、調査、特定するなど、あらゆる検出タスクを実行できます。

AWS コマンドラインツール

AWS コマンドラインツールを使用すると、システムのコマンドラインでコマンドを発行して、Detective AWS タスクやタスクを実行できます。コマンドラインを使用すると、コンソールを使用するよりも高速で便利になります。コマンドラインツールは、タスクを実行するスクリプトを作成する場合にも便利です。

AWS には、 AWS Command Line Interface (AWS CLI) と 2 種類のコマンドラインツールが用意されています。 AWS Tools for PowerShellのインストールと使用方法については AWS CLI、『AWS Command Line Interface ユーザガイド』を参照してください。Tools for のインストールと使用方法については PowerShell、『AWS Tools for PowerShell ユーザーガイド』を参照してください。

AWS SDK

AWS には、Java、Go、Python、C++、.NET などのさまざまなプログラミング言語とプラットフォーム用のライブラリとサンプルコードで構成される SDK が用意されています。SDK を使用すると、Detective などへの便利なプログラムによるアクセスが可能になります。 AWS のサービス SDK は、暗号署名によるリクエスト、エラーの管理、リクエストの自動再試行などのタスクも処理します。 AWS SDK のインストールと使用について詳しくは、「ツール・トゥ・ビルド・オン」を参照してください。 AWS

Amazon Detective REST API

Amazon Detective REST API を使用すると、Detective アカウント、データ、およびリソースに包括的かつプログラム的にアクセスできます。この API を使用すると、HTTPS リクエストを Detective に直接送信できます。ただし、 AWS コマンドラインツールや SDK とは異なり、この API を使用するには、リクエストに署名するためのハッシュの生成など、低レベルの詳細をアプリケーションで処理する必要があります。この API の詳細については、Detective API リファレンスをご覧ください。

Amazon Detective の価格

AWS 他の製品と同様に、Amazon Detective を使用するための契約や最低契約はありません。

Detective の料金は複数の基準に基づいており、ソースに関係なくすべてのデータについて GB あたりの段階的定額料金が課金されます。詳細については、Amazon Detective の料金表を参照してください。

Detective の使用コストの把握と予測に役立つように、Detective はアカウントの推定使用コストを表示します。これらの見積もりは Amazon Detective コンソールで確認でき、Amazon Detective API を使用してアクセスできます。サービスの使用方法によっては、Security Lake の統合や Detective Investigations などの特定の Detective AWS のサービス 機能と組み合わせて他の機能を使用すると、追加費用が発生する場合があります。

Detective を初めて有効にすると、Detective の 30 AWS アカウント 日間の無料トライアルに自動的に登録されます。これには、 AWS Organizationsで組織の一部として有効化されている個別のアカウントが含まれます。無料試用期間中は、 AWS リージョン該当する Detective の使用は無料です。

無料トライアル終了後の Detective の使用コストの把握と予測に役立つように、Detective ではトライアル期間中の Detective の使用状況に基づいて推定使用コストを表示します。使用状況データには、無料トライアルが終了するまでの残り時間も示されます。このデータは Amazon Detective コンソールで確認し、Amazon Detective API を使用してアクセスできます。

Detective の仕組み

Detective は、Amazon VPC AWS CloudTrail フローログからのログイン試行、API 呼び出し、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自動的に抽出します。また、によって検出された結果も取り込まれます。 GuardDuty

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、 AWS これらのアクションがアカウントや 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も確認できます。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 AWS つ以上のアカウントから抽出および分析されたデータをリンクしてまとめたものです。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 も統合されています。 AWS Organizations組織管理アカウントが組織の 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、組織動作グラフのメンバーアカウントとして組織アカウントを有効にします。

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、the section called “動作グラフで使用されるソースデータ” 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 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: 招待とメンバーシップの管理” を参照してください。

管理者アカウントは、行動グラフから生成された分析と視覚化を使用して、 AWS リソースと調査結果を調査します。 GuardDuty GuardDutyとの Detective インテグレーションを使用すると AWS Security Hub、 GuardDuty これらのサービスの検索結果を直接 Detective コンソールに切り替えることができます。

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。

関連サービス

のデータ、ワークロード、アプリケーションをさらに保護するには、 AWS のサービス 以下を Amazon Detective と組み合わせて使用することを検討してください。 AWS

AWS Security Hub

AWS Security Hub AWS リソースのセキュリティ状態を包括的に把握でき、 AWS セキュリティ業界の標準やベストプラクティスに照らして環境をチェックするのに役立ちます。その一環として、複数の (Detective を含む) AWS 製品およびサポート対象のパートナーネットワーク AWS のサービス (APN) 製品から得たセキュリティ結果を収集、集約、整理、優先順位付けします。Security Hub は、セキュリティの傾向を分析し、 AWS 環境全体で最も優先度の高いセキュリティ問題を特定するのに役立ちます。

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

Amazon GuardDuty

Amazon GuardDuty は、Amazon S3 AWS AWS CloudTrail CloudTrail のデータイベントログや管理イベントログなど、特定の種類のログを分析して処理するセキュリティ監視サービスです。悪意のある IP アドレスやドメインのリストなどの脅威インテリジェンスフィードと機械学習を使用して、環境内で予期しない、または許可されていない可能性があるアクティビティや悪意のあるアクティビティを特定します AWS 。

詳細については GuardDuty、Amazon GuardDuty ユーザーガイドを参照してください。

Amazon Security Lake

Amazon Security Lake は、完全マネージド型のセキュリティデータレイクサービスです。Security Lake を使用すると、 AWS 環境、SaaS プロバイダー、オンプレミスソース、クラウドソース、サードパーティソースからのセキュリティデータを、アカウントに保存されている専用のデータレイクに自動的に一元化できます。 AWS Security Lake はセキュリティデータの分析に役立つため、組織全体のセキュリティ体制をより完全に把握できます。Security Lake を使用すると、ワークロード、アプリケーション、データの保護を強化することもできます。

セキュリティレイクの詳細については、Amazon セキュリティレイクユーザーガイドを参照してください。Detective と Security Lake を併用する方法の詳細については、を参照してくださいAmazon Security Lake との統合。

AWS その他のセキュリティサービスについては、「セキュリティ、ID、コンプライアンス」を参照してください。 AWS

Amazon Detective の開始方法

このチュートリアルでは、Amazon Detective の概要を説明します。 AWS アカウントで Detective を有効にする方法について説明します。また、Detective が 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を開始したことを確認する方法についても説明します。

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。その後、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できます。アカウントの管理 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。the section called “動作グラフの無料トライアル期間について” 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。詳細については、「the section called “管理者アカウントの使用量とコスト”」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。詳細については、「the section called “メンバーアカウントの使用量の追跡”」を参照してください。

トピック

開始する前に

Amazon Detective を有効にするには、まず AWS アカウントが必要です。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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、電話キーパッドで検証コードを入力するように求められます。

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

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] を選んで、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

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

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセス IAM アイデンティティセンターディレクトリを設定するAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

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

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

前提条件

次の要件が満たされていることを確認します。

必要な Detective アクセス許可の付与

Detective を有効にする前に、必要な Detective アクセス許可を IAM プリンシパルに付与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。

Amazon Web Services (AWS) にサインアップすると、Amazon Detective を含むすべての AWS のサービスに、アカウントが自動的にサインアップされます。ただし、Detective を有効化して使用するには、まず Amazon Detective コンソールと API オペレーションへのアクセスを許可するアクセス許可を設定する必要があります。これを行うには、 AWS Identity and Access Management (IAM) を使用して `AmazonDetectiveFullAccess`マネージドポリシーを IAM プリンシパルにアタッチし、すべての Detective アクションへのアクセスを許可します。

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。

サポートされている AWS Command Line Interface バージョン

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

レコメンデーション

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

GuardDuty と に登録している場合は AWS Security Hub、 アカウントをこれらのサービスの管理者アカウントとして設定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 検出結果の詳細を表示するときに、検出結果の詳細から Detective 検出結果プロファイルにピボットできます。
- Detective では、 GuardDuty 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、使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 管理者アカウントを使用して Detective を有効にします。

  AWS Organizations を使用してアカウントを管理する場合は、 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 アカウントの IAM ユーザーへのアクセスを提供する」を参照してください。

通知頻度の GuardDuty CloudWatch推奨更新

では GuardDuty、ディテクターは、結果のその後の出現を報告するための Amazon CloudWatch 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 管理者アカウントはディテクターの 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、 の使用コストには影響しないことに注意してください GuardDuty。

通知頻度の設定については、「Amazon GuardDuty ユーザーガイド」の「Amazon CloudWatch イベントによる検出結果のモニタリング」を参照してください。 GuardDuty

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 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. [開始する] を選択します。
3. Amazon Detective を有効にする ページで、管理者アカウントを Detective と Amazon および の間で調整するための推奨事項について説明します (推奨) AWS Security Hub。 GuardDuty the section called “ GuardDuty および との推奨アラインメント AWS Security Hub” を参照してください。
4. IAM ポリシーのアタッチボタンを使用すると、IAM コンソールに直接移動し、推奨ポリシーが開きます。Detective に使用するプリンシパルに推奨ポリシーをアタッチすることもできます。IAM コンソールで操作を行うアクセス許可を持っていない場合は、[必要なアクセス許可] でポリシーの Amazon リソースネーム (ARN) をコピーして、IAM 管理者に提供することができます。お客様に代わって IAM 管理者により、ポリシーがアタッチされます。

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

- Detective API: `CreateGraph` オペレーションを使用します。
- 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"}'
```

リージョン間で Detective を有効にする (の Python スクリプト GitHub)

Detective は、以下 GitHub を実行するオープンソーススクリプトを に提供します。

- 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 スクリプトを設定して使用する方法については、「」を参照してくださいthe section called “Amazon Detective の Python スクリプト”。

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. https://console.aws.amazon.com/detective/ で Amazon Detective コンソールを開きます。
2. ナビゲーションペインで、[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。

Amazon Detective の概念と用語

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

AWS アカウント は動作グラフを作成し、その動作グラフを調査に使用しています。

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。詳細については、「the section called “動作グラフへのメンバーアカウントの招待”」を参照してください。

組織動作グラフの管理者アカウントは、組織管理アカウントが指定する Detective 管理者アカウントです。詳細については、「the section called “Detective 管理者アカウントの指定”」を参照してください。Detective 管理者アカウントは、組織動作グラフのメンバーアカウントとして任意の組織アカウントを有効にすることができます。詳細については、「the section called “組織メンバーアカウントの管理”」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。

自律システム組織 (ASO)

自律システムが割り当てられている、名前付き組織。この自律システムは、異種ネットワーク、または類似のルーティングロジックとポリシーを使用するネットワークのセットです。

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、相互にリンクされた一連のデータ。

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。

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 管理者アカウントは、組織管理アカウントでない限り、委任された管理者アカウントでもあります。組織管理アカウントは、委任された管理者アカウントになることはできません。

Detective では、自己委任が可能です。組織管理アカウントは自身のアカウントを Detective の委任された管理者として委任できますが、これは組織の範囲内でなく Detective の範囲内でのみ登録または記憶されます。

Detective 管理者アカウント

リージョン内の組織動作グラフの管理者アカウントとして組織管理アカウントから指定されたアカウント。詳細については、「the section called “Detective 管理者アカウントの指定”」を参照してください。

組織管理アカウントが Detective 管理者アカウントとして自身のアカウントのみを選択することが、Detective では推奨されます。

Detective 管理者アカウントが組織管理アカウントでない場合、Detective 管理者アカウントには組織内の Detective の委任された管理者アカウントがなります。

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:

- ログや Amazon VPC AWS AWS CloudTrail フローログなど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

取り込んだ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 ユーザーなどがあります。

エンティティは、 AWS 管理するリソースでも、リソースとやり取りした外部 IP アドレスでもかまいません。

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 によって検出されたセキュリティ上の問題 GuardDuty。

検出結果グループ

同じイベントまたはセキュリティ問題に関連している可能性のある検出結果、エンティティ、および証拠の集まり。Detective は、組み込みの機械学習モデルに基づいて検出結果グループを生成します。

Detective の証拠

Detective は、過去 45 日以内に収集された動作グラフのデータに基づいて、検出結果グループに関連する追加の証拠を特定します。この証拠は、[情報] という重要度値を含む検出結果として提示されます。証拠は、検出結果グループ内で見たときに疑わしいと思われる異常なアクティビティや不明な動作を浮き彫りにする、裏付けとなる情報です。その例としては、新たに観察された位置情報や、検出結果の時間範囲内に観察された API コールなどが挙げられます。現時点では、これらの検出結果は Security Hub には送信されず、Detective でのみ表示できます。

検索の概要

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。

ハイボリュームエンティティ

時間間隔中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。

詳細については、「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

AWS アカウント 管理者アカウントが行動グラフにデータを提供するよう招待したもの。組織動作グラフのメンバーアカウントには、 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がなることができます。

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。詳細については、「the section called “メンバーアカウント: 招待とメンバーシップの管理”」を参照してください。

組織アカウントは、組織動作グラフ内のメンバーシップを変更できません。

また、すべてのメンバーアカウントは、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。

組織行動グラフ

Detective 管理者アカウントが所有する動作グラフ。Detective 管理者アカウントは、組織管理アカウントが指定します。詳細については、「the section called “Detective 管理者アカウントの指定”」を参照してください。

Detective 管理者アカウントは、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にするかどうかを制御できます。組織アカウントは、自身を組織動作グラフから削除することはできません。

Detective 管理者アカウントは、組織アカウント以外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。

プロファイル

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、キーバリューペア、テーブル、タイムライン、棒グラフ、または位置情報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。

動作グラフのデータ

Amazon Detective では、Detective の動作グラフのデータを使用して調査を実行します。

動作グラフは、1 つ以上のアマゾン ウェブ サービス (AWS) アカウントから取り込まれた Detective ソースデータから生成されたデータのリンクされたセットです。

動作グラフは、ソースデータを使用して次を実行します。

- システム、ユーザー、およびそれらの間の時間の経過に伴うインタラクションの全体像を生成する
- 特定のアクティビティのより詳細な分析を実行して、調査を実行するときに生じる疑問を解決するのをサポートする
- 同じイベントまたはセキュリティ問題に関連している可能性のある検出結果の集まり、エンティティの集まり、証拠の集まりを相互に関連付ける。

動作グラフデータのすべての抽出、モデリング、および分析は、個々の動作グラフのコンテキスト内で行われることに注意してください。

管理者アカウントが動作グラフでメンバーアカウントを管理する方法については、「アカウントの管理」を参照してください。

コンテンツ

Amazon Detective がソースデータを使用して動作グラフを作成する方法

調査の raw データを提供するために、Detective は、 AWS 環境全体のみならず、それを超えてデータを収集します。これには次のデータが含まれます。

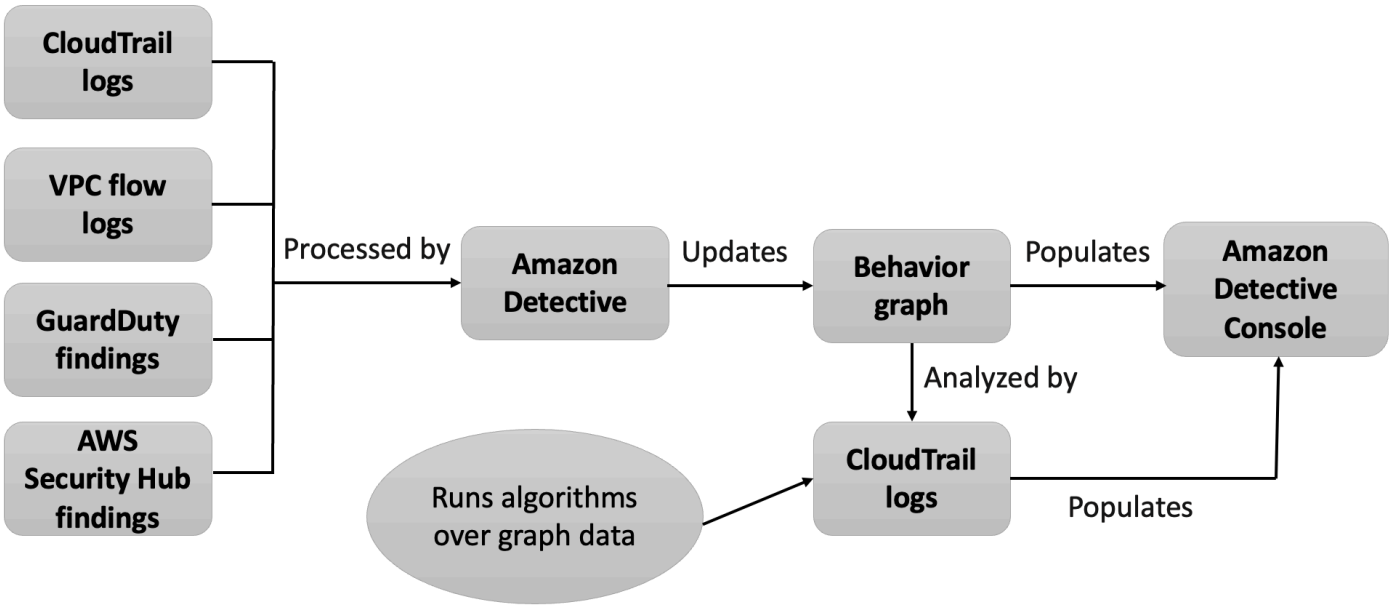
- アマゾン仮想プライベートクラウド (Amazon VPC) を含むログデータと AWS CloudTrail
- Amazon からの調査結果 GuardDuty

- からの調査結果 AWS Security Hub

ビヘイビアグラフで使用されるソースデータについて詳しくは、「ビヘイビアグラフで使用されるソースデータ」を参照してください。

Detective によるソースデータの処理方法

新しいデータが提供されると、Detective は抽出と分析の組み合わせを使用して動作グラフにデータを入力します。



Detective の抽出

抽出は、設定されたマッピングルールに基づきます。マッピングルールは、基本的に「ある特定のデータについては、常にある特定の方法でそのデータを使用して動作グラフデータを更新する」ためのものです。

例えば、受信した Detective ソースデータレコードに IP アドレスが含まれている場合があります。その場合、Detective はそのレコードに含まれている情報を使用して、新しい IP アドレスエンティティを作成するか、既存の IP アドレスエンティティを更新します。

Detective の分析

分析は、データを分析してエンティティに関連付けられているアクティビティのインサイトを提供する、より複雑なアルゴリズムです。

例えば、あるタイプの Detective 分析では、アルゴリズムを実行して、アクティビティが発生する頻度を分析します。API コールを実行するエンティティの場合、アルゴリズムを実行することで、エンティティが通常使用しない API コールが検索されます。アルゴリズムでは、API コールの数の大幅なスパイクも検索されます。

分析インサイトは、アナリストの主要な質問に対する回答を提供することで調査をサポートし、検出結果およびエンティティプロファイルのパネルにデータを入力するために頻繁に使用されます。

新しい動作グラフのトレーニング期間

検出結果の調査する 1 つの方法は、検出結果のスコープ時間中のアクティビティを、検出結果が検出される前に発生したアクティビティと比較することです。これまでに観察されていないアクティビティは、疑わしいアクティビティとして判断される可能性が高くなります。

Amazon Detective プロファイルの一部のパネルでは、検出前の期間に観察されなかったアクティビティが強調表示されます。いくつかのプロファイルパネルには、スコープ時間の 45 日前の平均アクティビティを示すベースライン値も表示されます。スコープタイムは、エンティティのアクティビティを時系列でまとめたものです。

より多くのデータが動作グラフに抽出されるにつれて、Detective では、組織内の正常なアクティビティと異常なアクティビティの状況をより正確に確認できます。

ただし、このより正確な状況を確認するには、Detective は少なくとも 2 週間分のデータにアクセスする必要があります。また、Detective 分析の成熟度は、動作グラフのアカウント数とともに高まります。

Detective をアクティブ化してから最初の 2 週間は、トレーニング期間とみなされます。この期間中、スコープ時間のアクティビティを以前のアクティビティと比較するプロファイルパネルには、Detective がトレーニング期間中であるというメッセージが表示されます。

試用期間中、Detective は行動グラフにできるだけ多くのメンバーアカウントを追加することを推奨しています。これにより、Detective は、より大きいサイズのデータプールを利用できるようになり、組織の通常のアクティビティをより正確に把握できます。

動作グラフのデータ構造の概要

動作グラフのデータ構造は、抽出および分析されたデータの構造を定義します。また、ソースデータを動作グラフにマッピングする方法も定義します。

動作グラフのデータ構造内の要素のタイプ

動作グラフのデータ構造は、次の情報の要素で構成されています。

エンティティ

エンティティは、Detective ソースデータから抽出された項目を表します。

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 ユーザーなどがあります。

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されることもあれば、複数のレコードにまたがって集計される場合もあります。

一部のプロパティは、単一のスカラー値または集計値で構成されます。例えば、EC2 インスタンスの場合、Detective はインスタンスのタイプと処理された合計バイト数を追跡します。

時系列プロパティは、時間の経過に合わせてアクティビティを追跡します。例えば、EC2 インスタンスの場合、Detective は使用した一意のポートを時間の経過に合わせて追跡します。

関係

関係は、個々のエンティティ間で発生するアクティビティを表します。また、関係は、Detective ソースデータから抽出されます。

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。関係タイプの例としては、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。

特定のインスタンスに接続する特定の IP アドレスなど、個々の関係ごとに、Detective は時間の経過に合わせてアクティビティの発生を追跡します。

動作グラフのデータ構造内のエンティティのタイプ

動作グラフのデータ構造は、次を実行するエンティティと関係タイプで構成されます。

- 使用されているサーバー、IP アドレス、ユーザーエージェントを追跡する
- AWS 使用中のユーザー、ロール、アカウントを追跡します。

- ご利用の AWS 環境で発生するネットワーク接続と承認を追跡する

動作グラフのデータ構造には、次のエンティティタイプが含まれます。

AWS アカウント

AWS Detective ソースデータに存在するアカウント。

各アカウントについて、Detective は次のいくつかの質問に対する回答を提供します。

- アカウントで使用されたことがある API コール
- アカウントで使用されたことがあるユーザーエージェント
- アカウントで使用されたことがある自律型システム組織 (ASO)
- アカウントがアクティブになったことがある地理的場所

AWS 役割

AWS Detective ソースデータに存在するロール。

ロールごとに、Detective はいくつかの質問に対する回答を提供します。

- ロールで使用されたことがある API コール
- ロールで使用されたことがあるユーザーエージェント
- ロールで使用されたことがある ASO
- ロールがアクティブになったことがある地理的場所
- このロールを引き受けたリソース
- このロールを引き受けたロール
- このロールが関係するロールセッション

AWS ユーザ

AWS Detective ソースデータに存在するユーザー。

ユーザーごとに、Detective はいくつかの質問に対する回答を提供します。

- ユーザーが使用したことのある API コール
- ユーザーが使用したことのあるユーザーエージェント
- ユーザーがアクティブになったことがある地理的場所
- このユーザーが引き受けたロール
- このユーザーが関係するロールセッション

フェデレーティッドユーザー

フェデレーティッドユーザーのインスタンス。フェデレーティッドユーザーの例には次が含まれます。

- Security Assertion Markup Language (SAML) を使用してログインするアイデンティティ
- ウェブ ID フェデレーションを使用してログインするアイデンティティ

フェデレーティッドユーザーごとに、Detective は以下の質問に対する回答を提供します。

- フェデレーティッドユーザーが認証の際に使用したアイデンティティプロバイダー
- フェデレーティッドユーザーのオーディエンス オーディエンスは、フェデレーティッドユーザーのウェブアイデンティティトークンをリクエストしたアプリケーションを識別します。
- フェデレーティッドユーザーがアクティブになったことがある地理的場所
- フェデレーティッドユーザーが使用したことのあるユーザーエージェント
- フェデレーティッドユーザーが使用したことのある ASO
- このフェデレーティッドユーザーが引き受けたロール
- このフェデレーティッドユーザーが関係するロールセッション

EC2 インスタンス

Detective ソースデータに存在する EC2 インスタンス。

EC2 インスタンスごとに、Detective はいくつかの質問に対する回答を提供します。

- インスタンスと通信した IP アドレス
- インスタンスとの通信に使用されたポート
- インスタンスとの間で送受信されたデータの量
- インスタンスを含む VPC
- EC2 インスタンスで使用されたことがある API コール
- EC2 インスタンスで使用されたことがあるユーザーエージェント
- EC2 インスタンスで使用されたことがある ASO
- EC2 インスタンスがアクティブになったことがある地理的場所
- EC2 インスタンスが引き受けたことがあるロール

ロールセッション

ロールを引き受けるリソースのインスタンス。各ロールセッションは、ロール識別子とセッション名で識別されます。

ロールごとに、Detective はいくつかの質問に対する回答を提供します。

- このロールセッションで関係したリソース。つまり、引き受けられたロールとそのロールを引き受けたリソース。

  クロスアカウントのロールの引き受けの場合、Detective はロールを引き受けたリソースを識別できないことに注意してください。
- ロールセッションが使用したことのある API コール
- ロールセッションが使用したことのあるユーザーエージェント
- ロールセッションが使用したことのある ASO
- ロールセッションがアクティブになったことがある地理的場所
- このロールセッションを開始したユーザーまたはロール
- このロールセッションから開始されたロールセッション

結果

GuardDuty Amazonが発見した調査結果は、Detectiveのソースデータに入力されます。

検出結果ごとに、Detective は、検出結果のアクティビティについて、検出結果のタイプ、オリジン、および時間枠を追跡します。

また、検出されたアクティビティに関係するロールや IP アドレスなど、検出結果に固有の情報も保存されます。

IP アドレス

Detective ソースデータに存在する IP アドレス。

IP アドレスごとに、Detective はいくつかの質問に対する回答を提供します。

- アドレスで使用されたことがある API コール
- アドレスで使用されたことがあるポート
- IP アドレスを使用したことがあるユーザーおよびユーザーエージェント
- IP アドレスがアクティブになったことがある地理的場所
- この IP アドレスが割り当てられ、通信している EC2 インスタンス

S3 バケット

Detective ソースデータにある S3 バケット。

S3 バケットごとに、Detective は以下の質問に対する回答を提供します。

- S3 バケットとインタラクションしたプリンシパル
- S3 バケットに対して実行された API コール
- プリンシパルが S3 バケットに対して API コールを実行した地理的場所
- S3 バケットとのインタラクションに使用されたユーザーエージェント
- S3 バケットとのインタラクションに使用された ASO

S3 バケットを削除してから、同じ名前の新しいバケットを作成できます。Detective は S3 バケット名を使用して S3 バケットを識別するため、これらを単一の S3 バケットエンティティとして扱います。エンティティプロファイルでは、[Creation time] (作成時刻) は最初の作成時刻です。[Deletion time] (削除時刻) は、最新の削除時刻です。

すべての作成イベントおよび削除イベントを表示するには、作成時刻で開始し、削除時刻で終了するようにスコープ時間を設定します。[Overall API call volume] (全体的な API コールの量) のプロファイルパネルで、スコープ時間のアクティビティの詳細を表示します。API メソッドをフィルタリングして、`Create` メソッドと `Delete` メソッドを表示します。the section called “[全体的な API コール量]” を参照してください。

User agent

Detective ソースデータに存在するユーザーエージェント。

ユーザーエージェントごとに、Detective は以下のような質問に対する回答を提供します。

- ユーザーエージェントが使用したことのある API コール
- ユーザーエージェントを使用したことがあるユーザーおよびロール
- ユーザーエージェントを使用したことがある IP アドレス

EKS クラスター

Detective ソースデータに存在する EKS クラスター。

> **Note**
>
> このエンティティタイプの詳細をすべて表示するには、オプションの EKS 監査ログデータソースを有効にする必要があります。詳細については、「Detective のオプションデータソースの種類」を参照してください。

EKS クラスターごとに、Detective は以下のような質問に対する回答を提供します。

- このクラスターではどのような Kubernetes API コールが実行されていますか?

- このクラスターではどの Kubernetes ユーザーとサービスアカウント (サブジェクト) がアクティブですか?
- このクラスターではどのコンテナが起動されていますか?
- このクラスターのコンテナの起動にはどのようなイメージが使用されていますか?

Kubernetes ポッド

Detective ソースデータに存在する Kubernetes ポッド。

> **Note**
>
> このエンティティタイプの詳細をすべて表示するには、オプションの EKS 監査ログデータソースを有効にする必要があります。詳細については、「Detective のオプションデータソースの種類」を参照してください。

ポッドごとに、Detective は以下のような質問に対する回答を提供します。

- このポッドのどのコンテナイメージが私のアカウントでよく使用されていますか?
- このポッドに対し、どのようなアクティビティが指示されていますか?
- このポッドではどのコンテナが実行されていますか?
- このポッド内のコンテナのレジストリは、私のアカウントではよく使用されていますか?
- ワークロードの他のポッドでは他にどのようなコンテナが実行されていますか?
- このポッドには、ワークロードの他のポッドにはない異常なコンテナがありますか?

コンテナイメージ

Detective ソースデータに存在するコンテナイメージ。

> **Note**
>
> このエンティティタイプの詳細をすべて表示するには、オプションの EKS 監査ログデータソースを有効にする必要があります。詳細については、「Detective のオプションデータソースの種類」を参照してください。

コンテナイメージごとに、Detective は以下のような質問に対する回答を提供します。

- 環境内の他のどのイメージがこのイメージと同じリポジトリまたはレジストリを共有していますか?

- 私の環境ではこのイメージのコピーがいくつ実行されていますか?

Kubernetes サブジェクト

Detective ソースデータに存在する Kubernetes サブジェクト。Kubernetes サブジェクトはユーザーまたはサービスアカウントです。

> **Note**
>
> このエンティティタイプの詳細をすべて表示するには、オプションの EKS 監査ログデータソースを有効にする必要があります。詳細については、「Detective のオプションデータソースの種類」を参照してください。

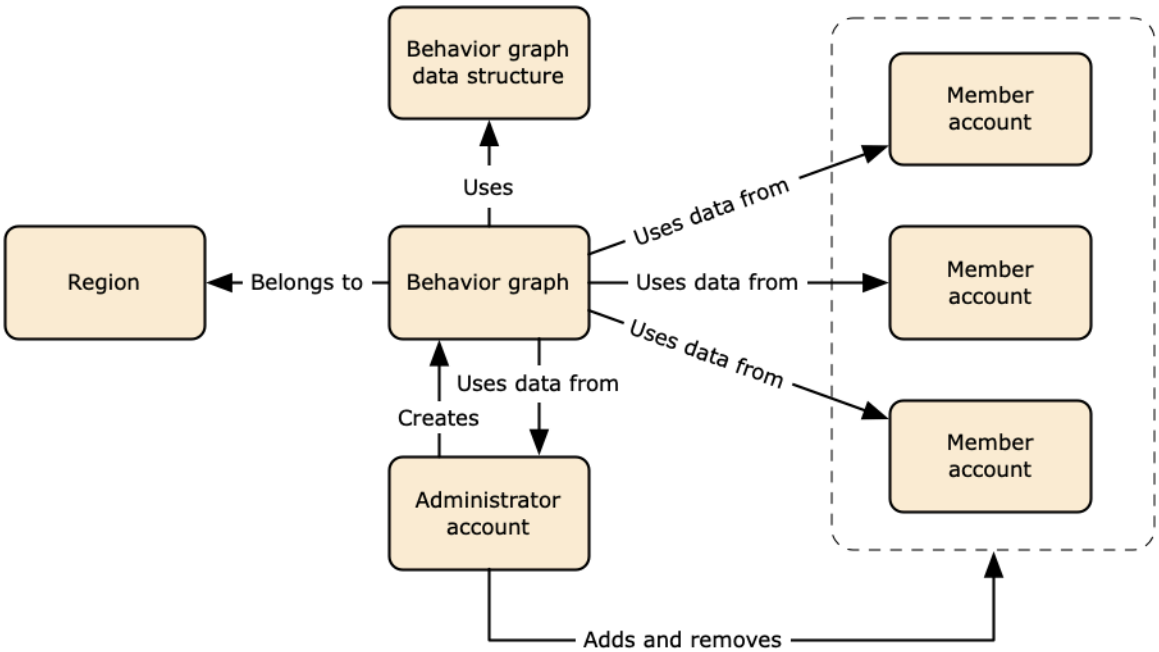
サブジェクトごとに、Detective は以下のような質問に対する回答を提供します。

- どの IAM プリンシパルがこのサブジェクトとして認証されていますか?
- このサブジェクトにはどのような検出結果が関連付けられていますか?
- サブジェクトはどの IP アドレスを使用していますか?

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。

Detective を使用すると、最長 1 年間の履歴イベントデータにアクセスできるようになりました。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によって表示されます。Detective GuardDuty はこれらの変化を調査結果と関連付けます。



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 AWS は次の種類のログからデータを取り込みます。

- AWS CloudTrail ログ
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs
  - IPv4 と IPv6 の両方のレコードを取り込むが、エラスティックファブリックアダプターが生成した MAC レコードは取り込まない。
  - `log-status`フィールドの値が in 状態になったときにログレコードを取り込みます。OK詳細については、Amazon VPC ユーザーガイドの「フローログレコード」を参照してください。
  - これらの VPC でのみ実行されている Amazon Elastic Compute Cloud インスタンスによって生成されたフローログを取り込みます。NAT ゲートウェイ、RDS インスタンス、Fargate クラスターなどの他のリソースは使用されません。
  - 受け入れられたトラフィックと拒否されたトラフィックの両方を取り込みます。
- 登録されているアカウントの場合 GuardDuty、Detective GuardDuty は結果も取り込みます。

Detective は VPC フローログの独立した重複ストリームを使用して VPC CloudTrail フローログイベントを消費し、VPC フローログを記録します。 CloudTrail これらのプロセスは、既存のフローロ

グ設定や VPC CloudTrail フローログ設定に影響を与えたり、使用したりすることはありません。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タイプ

Detective は、Detective コアパッケージで提供されている 3 つのデータソース (AWS CloudTrail コアパッケージにはログ、VPC フローログ、 GuardDutyおよび結果が含まれます) に加えて、オプションのソースパッケージを提供しています。オプションのデータソースパッケージは、動作グラフに対し、いつでも起動または停止できます。

Detective では、リージョンごとに、コアソースパッケージとオプションソースパッケージの両方で 30 日間の無料トライアルが提供されています。

> **Note**
>
> Detective は、各データソースパッケージから受信したすべてのデータを最大 1 年間保持します。

現在、以下のオプションソースパッケージをご利用いただけます。

- EKS 監査ログ

  このオプションデータソースパッケージにより、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、そのデータを動作グラフに追加できます。Detective は、ユーザーアクティビティを AWS CloudTrail マネジメントイベントに、ネットワークアクティビティを Amazon VPC フローログと関連付けます。これらのログを手動で有効化または保存する必要はありません。詳細については、「Detective 用の Amazon EKS 監査ログ」を参照してください。

- AWS セキュリティ調査結果

  このオプションのデータソースパッケージにより、Detective は Security Hub からデータを取り込み、そのデータを動作グラフに追加することができます。詳細については、「AWS セキュリティ調査結果」を参照してください。

オプションデータソースを起動したり停止したりするには、以下の手順を実行します。

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。

2. ナビゲーションパネルで [設定] の [全般] を選択します。
3. [オプションのソースパッケージ] で [更新] を選択します。次に、有効にするデータソースを選択します。または、既に有効になっているデータソースのチェックボックスをオフにして [更新] を選択し、有効にするデータソースパッケージを変更します。

> **Note**
>
> オプションのデータソースを停止して再起動すると、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発生します。このギャップはコンソール画面に表示され、データソースが停止していた期間を表します。データソースを再起動しても、Detective がデータを遡及的に取り込むことはありません。

Detective 用の Amazon EKS 監査ログ

Amazon EKS 監査ログは、Detective の動作グラフ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、アカウントにおけるそのステータスは、コンソールの [設定] ページまたは Detective API を使って確認できます。

このデータソースには 30 日間の無料トライアルが用意されています。詳細については、「オプションのデータソースの無料トライアル」を参照してください。

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動作グラフに追加できるようになります。このデータソースは、EKS クラスター、Kubernetes ポッド、コンテナイメージ、Kubernetes サブジェクトの 4 つのエンティティタイプに関して提供される情報を強化するものです。

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は、 GuardDuty から Kubernetes の結果の詳細を確認できます。 GuardDutyこのデータソースを有効にする方法の詳細については、「Amazon での Kubernetes 保護 GuardDuty 」を参照してください。 GuardDuty

> **Note**
>
> このデータソースは、2022 年 7 月 26 日より後に作成された新しい動作グラフではデフォルトで有効になります。2022 年 7 月 26 日より前に作成された動作グラフでは、データソースを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には、以下の手順を実行します。

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションパネルで [設定] の [全般] を選択します。
3. [ソースパッケージ] で [EKS 監査ログ] を選択することで、このデータソースを有効にします。既に有効になっている場合は、再選択すると、EKS 監査ログが動作グラフに取り込まれなくなります。

AWS セキュリティ調査結果

AWS セキュリティ調査結果は、Detective の動作グラフ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、アカウントにおけるそのステータスは、コンソールの [設定] ページまたは Detective API を使って確認できます。

このデータソースには 30 日間の無料トライアルが用意されています。詳細については、「オプションのデータソースの無料トライアル」を参照してください。

[AWS セキュリティ検出結果] を有効にすると、Detective は、Security Hub がアップストリームサービスから集約した Security Hub からの検出結果を、AWS Security Finding Format (ASFF) と呼ばれる標準の検出結果形式で使用できるようになります。このため、時間のかかるデータ変換作業の必要がなくなります。その後、複数の製品から取り込まれた結果を相互に関連付けて、最も重要なものを優先します。

AWS セキュリティ結果をオプションのデータソースとして追加または削除:

> **Note**
>
> 2023 年 5 月 16 日以降に作成された新しい行動グラフでは、 AWS セキュリティ結果データソースがデフォルトで有効になっています。2023 年 5 月 16 日より前に作成された動作グラフでは、データソースを手動で有効にする必要があります。

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションパネルで [設定] の [全般] を選択します。

3. [ソースパッケージ] で、 AWS セキュリティ結果を選択してこのデータソースを有効にします。データソースが既に有効になっている場合は、再選択すると、AWS Security Finding Format (ASFF) の検出結果が動作グラフに取り込まれなくなります。

現在サポートされている検出結果

Detective は、Amazon またはが所有するサービスからのすべての ASFF 結果をSecurity Hub に取り込みます。 AWS

- サポートされているサービス統合のリストを確認するには、 AWS Security Hub ユーザーガイドの「利用可能な AWS サービス統合」を参照してください。
- サポートされているリソースのリストについては、「 AWS Security Hub ユーザーガイド」の「リソース」を参照してください。
- AWS コンプライアンスステータスがに設定されておらず、FAILEDクロスリージョンの集計結果も取り込まれないサービス結果も取り込まれません。

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 10 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 10 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 10 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 15 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 15 TB のクォータは、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中断された場合は、 AWS Support ユーザーと協力して再度有効にする必要があります。可能であれば、連絡する前に AWS Support、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してください。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。

Amazon Detective を調査に使用する方法

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 を初めて使用する場合は、「Amazon Detective とは？」をご覧ください。 とAmazon Detective の概念と用語。

トピック

Detective 調査

Amazon Detective Investigations 機能を使用すると、セキュリティ侵害の兆候を使用して IAM ユーザーと IAM ロールを調査できます。これは、リソースがセキュリティインシデントに関与しているかどうかを判断するのに役立ちます。侵害のインジケータ (IOC) とは、ネットワーク、システム、または環境内で観察され、悪意のあるアクティビティまたはセキュリティインシデントを (高い信頼性レベルで) 特定できるアーティファクトです。Detective Investigationsを使用すると、効率を最大化し、セキュリティ上の脅威に集中し、インシデント対応能力を強化できます。

Detective Investigationsは、 AWS 機械学習モデルと脅威インテリジェンスを使用して環境内のリソースを自動的に分析し、潜在的なセキュリティインシデントを特定します。これにより、Detective の動作グラフの上に構築されたオートメーションを積極的、効果的、効率的に使用して、セキュリティ運用を改善できます。Detective Investigationsを使用すると、攻撃の手口や移動不能な攻撃、フラグが立てられたIPアドレス、グループの発見などを調査できます。セキュリティ調査の初期段階が実行されて、Detective によって特定されたリスクを強調したレポートが生成され、セキュリティイベントの把握と潜在的なインシデントへの対応に役立てることができます。

Detective 捜査の実施

[調査を実行] を使用して IAM ユーザーや IAM ロールなどのリソースを分析し、調査レポートを生成します。生成されたレポートには、侵害の可能性があることを示す異常な動作の詳細が記載されています。

Console

Amazon Detective コンソールを使用して [調査] ページからDetective 調査を実行するには、次の手順に従います。

1. マネジメントコンソールにサインインします。 AWS その後、https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで、[調査] を選択します。
3. [調査] ページで、右上隅の [調査を実行] を選択します。
4. 「リソースの選択」 セクションでは、調査を実行する方法が 3 つあります。Detective が推奨するリソースを対象に調査を実行することを選択できます。特定のリソースを対象に調査を実行できます。リソースは、Detective の [検索] ページからも調査できます。

   1. `Choose a recommended resource`— Detectiveは、調査結果と発見グループでのアクティビティに基づいてリソースを推奨しています。Detective が推奨するリソースの調査を実行するには、「推奨リソース」テーブルで、調査するリソースを選択します。

      推奨リソーステーブルには、以下の詳細が示されます。

      - リソース ARN — リソースの Amazon リソースネーム (ARN)。 AWS
      - 調査する理由 — リソースを調査する主な理由が表示されます。Detective がリソースの調査を推奨する理由は次のとおりです。
        - 過去 24 時間の重要度の高い検出結果にリソースが関与した場合。
        - 過去 7 日間に観察された検出結果グループにリソースが関与した場合。Detective の検出結果グループを使用すると、セキュリティイベントを引き起こす可能性がある複数のアクティビティを調査することができます。詳細については、「the section called “検出結果グループ”」を参照してください。
        - 過去 7 日間の検出結果にリソースが関与した場合。
      - 最新の検出結果 — 最新の検出結果が優先的にリストの上位に表示されます。
      - リソースタイプ — リソースのタイプを識別します。たとえば、 AWS AWS ユーザーやロールなどです。
   2. `Specify an AWS role or user with an ARN`— AWS AWS ロールまたはユーザーを選択して、特定のリソースについて調査を実行できます。

      以下の手順に従って、特定のリソースタイプを調査してください。

      a. 「リソースタイプを選択」 ドロップダウンリストから、 AWS AWS ロールまたはユーザーを選択します。

b. IAM リソースのリソース ARN を入力します。リソース ARN の詳細については、IAM ユーザーガイドの「Amazon リソースネーム (ARN)」を参照してください。

3. `Find a resource to investigate from the Search page`— Detective 検索ページからすべての IAM リソースを検索できます。

   次の手順に従って、検索ページからリソースを調査します。

   a. ナビゲーションペインで、[検索] を選択します。

   b. 検索ページで IAM リソースを検索します。

   c. リソースのプロファイルページに移動し、そこから調査を実行します。

5. 「調査対象期間」セクションで、選択したリソースのアクティビティを評価するための調査の対象期間を選択します。[開始日] と [開始時刻]、[終了日] と [終了時刻] を UTC 形式で選択します。選択した [時間範囲] ウィンドウは、最小 3 時間から最大 30 日の間で指定できます。

6. [調査を実行] を選択します。

API

調査をプログラムで実行するには、Detective API StartInvestigationの操作を使用します。 AWS Command Line Interface (AWS CLI) を使用している場合は、start-Investigation コマンドを実行してください。

リクエストで、以下のパラメーターを使用して Detective で調査を実行します。

- `GraphArn` — 動作グラフの Amazon リソースネーム (ARN) を指定します。
- `EntityArn` — IAM ユーザーと IAM ロールの一意の Amazon リソースネーム (ARN) を指定します。
- `ScopeStartTime` — オプションで、調査を開始するデータと時刻を指定します。値は UTC ISO8601 形式の文字列です。例えば、 `2021-08-18T16:35:56.284Z` です。
- `ScopeEndTime` — オプションで、調査を終了するデータと時刻を指定します。値は UTC ISO8601 形式の文字列です。例えば、 `2021-08-18T16:35:56.284Z` です。

この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
aws detective start-investigation \
```

```
--graph-arn arn:aws:detective:us-
east-1:123456789123:graph:fdac8011456e4e6182facb26dfceade0
 --entity-arn arn:aws:iam::123456789123:role/rolename --scope-start-
time 2023-09-27T20:00:00.00Z
--scope-end-time 2023-09-28T22:00:00.00Z
```

Detective の以下のページからも調査を実行できます。

- Detective の IAM ユーザーまたは IAM ロールのプロフィールページ。
- 検出結果グループのグラフ可視化ペイン。
- 関係するリソースのアクション列。
- 検出結果ページの IAM ユーザーまたは IAM ロール。

Detective がリソースの調査を実行すると、調査レポートが生成されます。レポートにアクセスするには、ナビゲーションペインから [調査] に移動します。

調査レポートの確認

調査レポートでは、Detective で以前に実行した調査について生成されたレポートを確認できます。

調査レポートを確認するには

1. AWS 管理コンソール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. ナビゲーションペインで、[調査] を選択します。

調査レポートの次の属性を記録します。

- ID — 生成された調査レポートの識別子。この ID を選択すると、調査の詳細が記載された調査レポートの概要を読むことができます。
- ステータス — 各調査は、調査の完了ステータスに基づいてステータスに関連付けられます。ステータス値は、[進行中]、[成功]、または [失敗] のいずれかになります。
- 重要度 — 各調査には重要度が割り当てられます。Detective では、自動的に重要度が検出結果に割り当てられます。

重要度は、特定のスコープ時間における単一のリソースの調査で分析された際のディスポジションを表します。調査によって報告される重要度は、影響を受けたリソースが組織に対する緊急性または重要性を意味する、または示すものではありません。

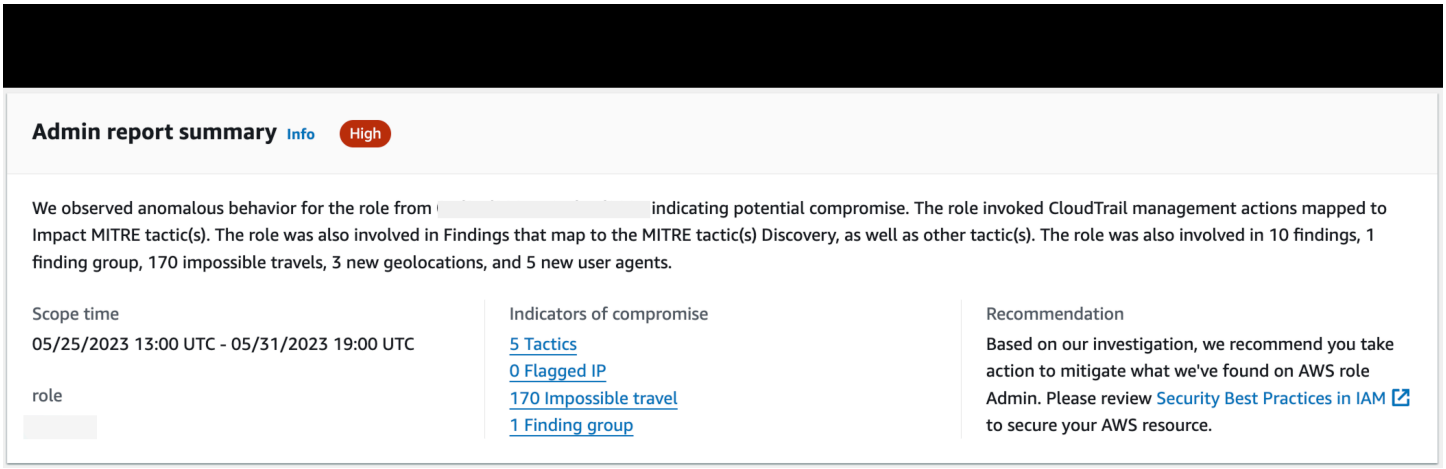
調査の重要度値は、重要度が高いものから低いものへと順に、[重要]、[高]、[中]」、[低]、または [情報] となります。

調査の重要度値が [重要] または [高] の場合は、Detective によって特定された影響度の高いセキュリティ問題があることを示している可能性が高いため、今後の検査でその調査を優先的に検討する必要があります。

- エンティティ — [エンティティ] 列には、調査で検出された特定のエンティティの詳細が表示されます。ユーザーやロールなど、 AWS 一部のエンティティはアカウントです。
- ステータス — [作成日] 列には、調査レポートが最初に作成された日時に関する詳細が表示されます。

Detective 調査レポートを理解する

Detective 調査レポートには、侵害を示唆する珍しい行動や悪意のあるアクティビティの概要が記載されています。また、セキュリティリスクを軽減するために Detective が提案する推奨事項も記載されています。



特定の調査 ID の調査レポートを表示するには、次の手順に従います。

1. 管理コンソールにサインインします。 AWS その後、https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで、[調査] を選択します。

3. [レポート] テーブルで、調査 ID を選択します。

Detective では、選択したスコープ時間とユーザーのレポートを生成します。レポートには、以下に示す 1 つ以上の侵害のインジケータに関する詳細を含む [侵害のインジケータ] セクションが含まれています。各侵害のインジケータを確認しながら、必要に応じて項目を選択して掘り下げ、詳細を確認します。

- [戦術]、[テクニック]、および[手順] — 潜在的なセキュリティイベントで使用される戦術、テクニック、手順 (TTP) を特定します。MITRE ATT&CK フレームワークを使用して、TTP を把握します。戦術は、「MITRE ATT&CK matrix for Enterprise」に基づいています。
- 脅威インテリジェンスフラグ付き IP アドレス — 疑わしい IP アドレスには、Detective 脅威インテリジェンスに基づいてフラグが付けられ、重大または重要な脅威として識別されます。
- 不可能な移動 — アカウントの通常とは異なるか、または不可能なユーザーアクティビティを検出して識別します。例えば、このインジケータには、短期間にユーザーの移動元と移動先の間で急激な変化があったことが示されます。
- 関連する検出結果グループ — 潜在的なセキュリティイベントに関連する複数のアクティビティを表示します。Detective では、検出結果とエンティティの関係を推測して、検出結果とエンティティを検出結果グループとしてグループ化するグラフ分析手法を使用しています。
- 関連検出結果 — 潜在的なセキュリティイベントに関連付けられた関連アクティビティ。リソースまたは検出結果グループに関連付けられた証拠を明確に分類して、それらのすべてを一覧表示します。
- 新しい位置情報 — リソースレベルまたはアカウントレベルで使用される新しい位置情報を識別します。例えば、このインジケータには、観測された位置情報のうち、以前のユーザーアクティビティに基づいて使用頻度が低いか、未使用の位置情報が一覧表示されます。
- 新規ユーザーエージェント — リソースレベルまたはアカウントレベルで使用される新しいユーザーエージェントを識別します。
- 新しい ASO — リソースレベルまたはアカウントレベルで使用される新しい自律システム組織 (ASO) を識別します。例えば、この指標には ASO として割り当てられた新しい組織が表示されます。

調査レポートの概要

調査の概要では、選択したスコープ時間で注意が必要な異常インジケータが強調表示されます。この概要を使用すると、潜在的なセキュリティ問題の根本原因をより迅速に特定し、パターンを特定して、セキュリティイベントの影響を受けるリソースを把握できます。

詳細調査レポートの概要では、次の詳細が表示されます。

調査の概要

[概要] パネルでは、重要度の高いアクティビティがある IP が視覚化され、攻撃者の経路に関するより多くのコンテキストを入手できます。

Detective では、IAM ユーザーによる移動元から遠くの移動先への不可能な移動など、異常なアクティビティが調査内で強調表示されます。

Detective は、潜在的なセキュリティイベントで使用される戦術、テクニック、手順 (TTP) に調査を関連付けます。MITRE ATT&CK フレームワークを使用して、TTP を把握します。戦術は、「MITRE ATT&CK matrix for Enterprise」に基づいています。

調査インジケータ

[インジケータ] ペインの情報を使用して、悪意のある動作とその影響を示すような異常なアクティビティに AWS リソースが関与しているかどうかを判断できます。侵害のインジケータ (IOC) とは、ネットワーク、システム、または環境内で観察され、悪意のあるアクティビティまたはセキュリティインシデントを (高い信頼性レベルで) 特定できるアーティファクトです。

調査レポート書のダウンロード

Detective 調査レポートは JSON 形式でダウンロードしてさらに分析したり、Amazon S3 バケットなどのお好みのストレージソリューションに保存したりできます。

[レポート] テーブルから調査レポートをダウンロードするには、次の手順に従います。

1. AWS マネジメントコンソール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. ナビゲーションペインで、[調査] を選択します。
3. [レポート] テーブルから調査を選択し、[ダウンロード] を選択します。

[概要] ページから調査レポートをダウンロードするには、次の手順に従います。

1. AWS 管理コンソール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. ナビゲーションペインで、[調査] を選択します。
3. [レポート] テーブルから調査を選択します。
4. [調査の概要] ページで、[ダウンロード] を選択します。

調査レポートのアーカイブ

Amazon Detective で調査を完了すると、調査レポートをアーカイブできます。調査がアーカイブされると、調査のレビューが完了したことを示します。

調査をアーカイブまたはアーカイブ解除できるのは、Detective 管理者のみです。Detective では、アーカイブされた調査を 90 日間保存します。

[レポート] テーブルから調査レポートをアーカイブするには、次の手順に従います。

1. AWS 管理コンソール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. ナビゲーションペインで、[調査] を選択します。
3. [レポート] テーブルから調査を選択し、[アーカイブ] を選択します。

[概要] ページから調査レポートをアーカイブするには、次の手順に従います。

1. AWS 管理コンソール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. ナビゲーションペインで、[調査] を選択します。
3. [レポート] テーブルから調査を選択します。
4. [調査の概要] ページで、[アーカイブ] を選択します。

調査の各フェーズと開始点

Amazon Detective は、調査プロセス全体をサポートするツールを提供しています。Detective での調査は、検出結果、検出結果グループ、またはエンティティから開始できます。

調査の各フェーズ

調査プロセスには、以下のフェーズが含まれます。

トリアージ

調査プロセスは、悪意があるか、高リスクであることが疑われるアクティビティについて通知された時点で開始されます。たとえば、Amazon や Amazon GuardDuty Inspector などのサービスによって明らかになった調査結果やアラートを調査するよう依頼されたとします。

トリアージのフェーズでは、ユーザーが、対象のアクティビティが真陽性 (本物の悪意のあるアクティビティであること) であるか、偽陽性 (悪意のあるアクティビティや高リスクのアクティビティではないこと) であるかを判断します。Detective プロファイルは、関係するエンティティのアクティビティに関するインサイトを提供することにより、トリアージプロセスをサポートします。

真陽性の場合は、次のステップに進みます。

スコープの特定

スコープの特定のフェーズでは、アナリストが、悪意のあるアクティビティまたは高リスクのアクティビティの程度と根本的な原因を特定します。

スコープの特定では、次の種類の質問に対する回答が提供されます。

- 侵害されたシステムとユーザー
- 攻撃元
- 攻撃の継続時間
- 他の関連アクティビティ。攻撃者がシステムからデータを抽出している場合は、その取得方法など。

Detective のビジュアライゼーションは、関係する、または影響を受けた他のエンティティを特定するのに役立ちます。

対処

最後のステップでは、攻撃を停止し、損害を最小限に抑え、類似の攻撃が再び起こらないようにするために、攻撃に対処します。

Detective 捜査の出発点

Detective のすべての調査には、重要な開始点があります。たとえば、あなたに Amazon GuardDuty AWS Security Hub または調査結果を割り当てられる場合があります。または、特定の IP アドレスの異常なアクティビティについて懸念があるかもしれません。

調査の一般的な出発点には、Detective GuardDuty ソースデータによって検出された結果と抽出されたエンティティが含まれます。

によって検出された結果は次のとおりです。 GuardDuty

GuardDuty ログデータを使用して、悪意のある、またはリスクの高いアクティビティの疑いのある事例を発見します。Detective では、これらの検出結果を調査するのに役立つリソースを用意しています。

各検出結果について、Detective は、関連する検出結果の詳細を提供します。Detective には、検索結果に関連するエンティティ (IP AWS アドレスやアカウントなど) も表示されます。

その後、関係するエンティティのアクティビティを詳しく調べて、検出結果から検出されたアクティビティが懸念の真の原因であるかどうかを判断できます。

詳細については、「the section called “検出結果の概要”」を参照してください。

AWS セキュリティハブによって集約されたセキュリティ調査結果

AWS Security Hub さまざまな調査結果プロバイダーのセキュリティ結果を 1 か所に集約し、でのセキュリティ状態を包括的に把握できます。 AWS Security Hub を使用すると、複数のプロバイダーからの大量の検出結果を処理する手間が不要になります。これにより、 AWS すべてのアカウント、リソース、およびワークロードのセキュリティを管理および改善するために必要な労力が軽減されます。Detective では、これらの検出結果を調査するのに役立つリソースを用意しています。

各検出結果について、Detective は、関連する検出結果の詳細を提供します。Detective には、検索結果に関連するエンティティ (IP AWS アドレスやアカウントなど) も表示されます。

詳細については、「the section called “検出結果の概要”」を参照してください。

Detective ソースデータから抽出されたエンティティ

取り込んだ Detective のソースデータから、Detective は、IP アドレスや AWS ユーザーなどのエンティティを抽出します。これらのいずれかを調査の開始点として使用できます。

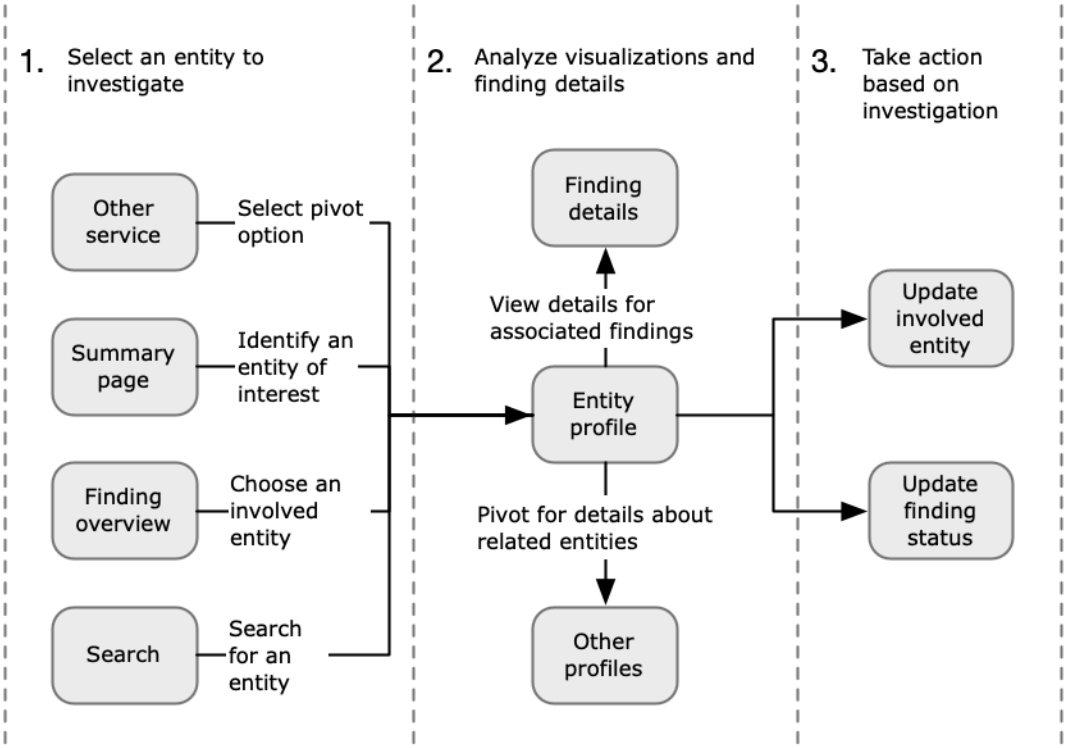
Detective は、IP アドレスやユーザー名など、エンティティに関する一般的な詳細を提供します。また、アクティビティ履歴の詳細も提供します。例えば、Detective は、これまでにエンティティが接続した、接続された、または使用した他の IP アドレスを報告できます。

詳細については、「エンティティの分析」を参照してください。

Amazon Detective 捜査フロー

Amazon Detective を使用して、EC2 AWS インスタンスやユーザーなどのエンティティを調査できます。セキュリティに関する検出結果も調査できます。

次の画像は、Detective 捜査のプロセスを大まかに示しています。



ステップ 1: 調査するエンティティを選択する

アナリストは Detective で結果を確認する際に GuardDuty、関連するエンティティを Detective で調査することを選択できます。the section called “別のコンソールからのピボット” を参照してください。

エンティティを選択すると、Detective のエンティティプロファイルに移動します。

ステップ 2: プロファイルのビジュアライゼーションを分析する

各エンティティプロファイルには、動作グラフから生成される一連のビジュアライゼーションが含まれています。動作グラフは、Detective に入力されるログファイルや他のデータから作成されます。

ビジュアライゼーションには、エンティティに関連するアクティビティが表示されます。これらのビジュアライゼーションを使用して、エンティティのアクティビティが異常かどうかを判断するための質問に回答できます。エンティティの分析 を参照してください。

調査のガイドとして、視覚的な各情報向けに提供される Detective ガイダンスを使用できます。ガイダンスは、表示された情報の概要を示し、尋ねるべき質問を提案し、その回答に基づいて次のステップを提案します。the section called “プロファイルパネルのガイダンスの使用” を参照してください。

各プロファイルには、関連する検出結果のリストが含まれます。検出結果の詳細を表示したり、検出結果の概要を表示したりできます。the section called “エンティティの検出結果の表示” を参照してください。

エンティティプロファイルから、他のエンティティと検出結果プロファイルにピボットし、関連するアセットのアクティビティをさらに調査できます。

ステップ 3: アクションを実行する

調査の結果に基づいて、適切な措置を講じます。

偽陽性の検出結果については、その検出結果をアーカイブできます。Detective では、GuardDuty 調査結果をアーカイブできます。the section called “調査結果をアーカイブする GuardDuty ” を参照してください。

それ以外の場合は、脆弱性に対処し、損害を軽減するための適切な措置を講じます。例えば、リソースの設定を更新する必要がある場合があります。

Amazon Detective での調査結果の分析

検出結果とは、悪意のある可能性があるものとして検出されたアクティビティなどのリスクのインスタンスです。Amazon GuardDuty AWS とセキュリティの調査結果は Amazon Detective に読み込まれるため、Detective を使用して関係するエンティティに関連するアクティビティを調査できます。 GuardDuty 結果はDetectiveコアパッケージの一部であり、デフォルトで取り込まれます。AWS Security Hub によって集計された他のすべてのセキュリティ結果は、オプションのデータソースとして取り込まれます。詳細については、「Source data used in a behavior graph」を参照してください。

Detective の検出結果の概要では、検出結果に関する詳細情報を確認できます。また、関係するエンティティの概要と、関連付けられたエンティティプロファイルへのリンクも表示されます。

検出結果が大きなアクティビティに関連している場合、[検出結果グループに移動] を選択するように Detective から通知されます。検出結果グループを使用すると、潜在的なセキュリティイベントに関連する複数のアクティビティを調査できるため、調査を進めるには検出結果グループを使用することをおすすめします。the section called “検出結果グループ” を参照してください。

コンテンツ

調査結果の概要の分析

Detective の検出結果の概要では、検出結果に関する詳細情報を確認できます。また、関係するエンティティの概要と、関連付けられたエンティティプロファイルへのリンクも表示されます。

検出結果の概要に使用されるスコープ時間

検出結果の概要の時間範囲は、検出結果の時間枠に設定されます。検出結果の時間枠には、検出結果のアクティビティが観察された最初と最後の時刻が反映されます。

検出結果の詳細

右側のパネルには、検出結果の詳細が含まれます。これらの詳細は、検出結果プロバイダーによって提供されたものです。

検出結果の詳細から、検出結果をアーカイブすることもできます。the section called “調査結果をアーカイブする GuardDuty ” を参照してください。

関連エンティティ

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。各エンティティについて、リストにはエンティティに関する概要情報が表示されます。この情報には、対応するエンティティプロファイルのエンティティ詳細プロファイルパネルの情報が反映されます。

エンティティタイプに基づいてリストをフィルタリングできます。エンティティ識別子のテキストに基づいてリストをフィルタリングすることもできます。

エンティティのプロファイルにピボットするには、[See profile] (プロファイルを表示) を選択します。エンティティのプロファイルにピボットすると、以下の処理が実行されます。

- スコープ時間は、検出結果の時間枠に設定されます。
- エンティティの [Associated findings] (関連する検出結果) パネルで、検出結果が選択されます。検出結果の詳細は、エンティティプロファイルの右側に表示されたままとなります。

「ページが見つかりません」のトラブルシューティング

Detective 内でエンティティまたは検出結果に移動すると、「ページが見つかりません」というエラーメッセージが表示されることがあります。

これを解決するには、次のいずれかを実行します。

- そのエンティティまたは検出結果がメンバーアカウントのいずれかに属していることを確認してください。メンバーアカウントを確認する方法については、「アカウントのリストを表示する」を参照してください。
- 管理者アカウントが、これらのサービスから Detective にピボットするようにSecurity Hub GuardDuty と連携していることを確認してください。推奨事項については、「Security Hub GuardDuty との推奨連携」を参照してください。
- メンバーアカウントが招待を受け入れた後に検出結果の発生したことを確認します。
- Detective 動作グラフがオプションのデータソースパッケージからデータを取り込んでいることを確認します。Detective 行動グラフで使用されるソースデータの詳細については、「行動グラフで使用されるソースデータ」を参照してください。

- Detective が Security Hub からデータを取り込み、そのデータを動作グラフに追加できるようにするには、 AWS セキュリティ結果の Detective をデータソースパッケージとして有効にする必要があります。詳細については、「セキュリティ調査結果」を参照してくださいAWS 。

- Detective でエンティティプロファイルまたは検出結果の概要に移動する場合は、URL が正しい形式であることを確認してください。プロファイル URL の形成について詳しくは、「URL を使用したエンティティプロファイルまたは検出結果の概要への移動」を参照してください。

検出結果グループを分析する

Amazon Detective の検出結果グループを使用すると、セキュリティイベントを引き起こす可能性がある複数のアクティビティを調査することができます。検出 GuardDuty 結果グループを使用して、重要度の高い検出結果の根本原因を分析できます。脅威アクターが AWS 環境を侵害しようとすると、通常、複数のセキュリティ検出結果や異常な動作につながる一連のアクションを実行します。これらのアクションは、多くの場合、長い時間や複数のエンティティにわたって行われます。セキュリティ上の検出結果を単独で調査すると、その重要度が誤解され、根本原因の特定が困難になる可能性があります。Amazon Detective ではこの問題に対処するため、検出結果とエンティティの関係を推測して、検出結果とエンティティをグループ化するグラフ分析手法を適用しています。関連するエンティティと検出結果を調査する出発点として、検出結果グループを検討することをお勧めします。

Detective は検出結果のデータを分析し、共有するリソースに基づいて関連する可能性が高い他の検出結果とグループ化します。例えば、同じ IAM ロールセッションで実行したアクションに関連する検出結果や、同じ IP アドレスで実行したアクションによる検出結果は、基となるアクティビティが同じである可能性が非常に高くなります。検出結果と証拠を 1 つのグループとして調査することは、Detective が行った関連付けが関連していない場合でも有益です。

各グループには、検出結果に加えて、検出結果に関係するエンティティも含まれます。エンティティには、IP アドレスやユーザーエージェント AWS など、 外のリソースを含めることができます。

> **Note**
>
> 別の GuardDuty 検出結果に関連する最初の検出結果が発生すると、関連するすべての検出結果と関連するすべてのエンティティを含む検出結果グループが 48 時間以内に作成されます。

[検出結果グループ] ページを理解する

[検出結果グループ] ページには、Amazon Detective が動作グラフから収集したすべての検出結果グループがリスト表示されます。検出結果グループの次の属性に注目してください。

グループの重要度

各検出結果グループには、関連する検出結果 AWS のセキュリティ検出結果形式 (ASFF) の重要度に基づいて重要度が割り当てられます。検出結果の ASFF 重要度値は、重要度が高いものから低いものへと順に、[重要]、[高]、[中]」、[低]、または [情報] となります。グループの重要度は、そのグループ内の検出結果の中で最も重要度の高い検出結果の重要度と等しくなります。

多数のエンティティに影響する、重要度が [重要] または [高] の検出結果で構成されるグループは、影響の大きいセキュリティ問題を表す可能性が高いため、優先的に調査する必要があります。

グループタイトル

[タイトル] 列では、各グループに一意の ID と、各グループに一意ではないタイトルが表示されます。これらは、グループの ASFF タイプの名前空間と、クラスターのその名前空間に含まれる検出結果の数に基づいて決定されます。例えば、TTP (2)、Effect (1)、Unusual behavior (2) というタイトルが付いているグループには、TTP 名前空間の 2 つの検出結果、Effect 名前空間の 1 つの検出結果、および Unusual behavior 名前空間の 2 つの検出結果から成る、合計 5 つの検出結果が含まれます。名前空間の完全なリストについては、「タイプ」を参照してください。

グループの戦術

グループの [戦術] 列には、アクティビティが分類される戦術カテゴリが表示されます。続いて表示されるリストの [戦術]・[テクニック]・[手順](tactics, techniques, and procedures: TTP) カテゴリは、MITRE ATT&CK の Enterprise Matrix に対応しています。

チェーン上の戦術を選択すると、その戦術の説明を表示できます。チェーンの下には、グループ内で検出された戦術のリストが表示されます。これらのカテゴリとその代表的なアクティビティは次のとおりです。

- 初期アクセス — 攻撃者が他者のネットワークに侵入しようとしています。
- 実行 — 攻撃者が他者のネットワークに侵入しようとしています。
- 永続化 — 攻撃者が足場を固めようとします。
- 権限昇格 — 攻撃者がより高いレベルのアクセス許可を取得しようとしています。
- 防衛回避 — 攻撃者が検出されないようにしようとしています。
- 認証情報アクセス — 攻撃者がアカウント名とパスワードを盗もうとしています。

- 探索 — 攻撃者が環境を理解し、知ろうとしています。
- 横展開 — 攻撃者が環境内を進もうとしています。
- 収集 — 攻撃者が目標達成に必要なデータを収集しようとしています。
- C&C (Command and Control) — 攻撃者が他者のネットワークに侵入しようとしています。
- 持ち出し — 攻撃者がデータを盗もうとしています。
- 影響 — 攻撃者がユーザーのシステムおよびデータを操作、中断、または破壊しようとしています。
- その他 — 検出結果によるアクティビティが、「matrix」に記載されている「tactics」(戦術) と一致しないことを示します。

グループ内のエンティティ

[エンティティ] 列には、検出されたこのグループ内の特定エンティティの詳細が表示されます。この値を選択すると、エンティティの内訳が [アイデンティティ]、[ネットワーク]、[ストレージ]、[コンピューティング] のカテゴリに分けて表示されます。カテゴリごとにエンティティの例を示します。

- ID - ユーザーやロールなどの AWS アカウント IAM プリンシパルと 。
- ネットワーク - IP アドレスまたはその他のネットワークおよび VPC エンティティ
- ストレージ - Amazon S3 バケットや DDB
- コンピューティング - Amazon EC2 インスタンスや Kubernetes コンテナ

グループ内のアカウント

アカウント列には、グループ内の検出結果に関係するエンティティを所有する AWS アカウントが示されます。 AWS アカウントは名前と AWS ID でリストされるため、重要なアカウントに関連するアクティビティの調査に優先順位を付けることができます。

グループ内の検出結果

[検出結果] 列には、グループ内のエンティティが重要度順に一覧表示されます。検出結果には、Amazon GuardDuty の検出結果、Amazon Inspector の検出結果、 AWS セキュリティの検出結果、Detective からの証拠が含まれます。グラフを選択すると、重要度ごとの正確な検出結果数を確認できます。

GuardDuty 検出結果は Detective コアパッケージの一部であり、デフォルトで取り込まれます。Security Hub によって集計された他のすべての AWS セキュリティ検出結果は、オプションのデータソースとして取り込まれます。詳細については、「Source data used in a behavior graph」を参照してください。

検出結果グループ内の重要度 [情報] の検出結果

Amazon Detective は、過去 45 日以内に収集された動作グラフのデータに基づいて、検出結果グループに関連する追加の情報を特定します。Detective はこの情報を、重要度が [情報] である検出結果として表示します。証拠は、検出結果グループ内で見たときに疑わしいと思われる異常なアクティビティや不明な動作を浮き彫りにする、裏付けとなる情報です。証拠としては、新たに観察された位置情報や、検出結果の時間範囲内に観察された API コールなどが挙げられます。証拠の検出結果は Detective でのみ表示でき、 には送信されません AWS Security Hub。

Detective は MaxMind GeoIP データベースを使用してリクエストの場所を決定します。 MaxMind は、国レベルでデータの精度が非常に高くなりますが、精度は国や IP の種類などの要因によって異なります。の詳細については MaxMind、MaxMind 「IP Geolocation」を参照してください。GeoIP データのいずれかが正しくないと思われる場合は、MaxMind 正しい GeoIP2 データ で Maxmind に修正リクエストを送信できます。

さまざまなプリンシパルタイプ (IAM ユーザーや IAM ロールなど) の証拠を確認できます。一部の証拠タイプでは、[すべてのアカウント] について証拠を確認できます。つまり、証拠は動作グラフ全体に影響するということです。すべてのアカウントについて証拠の検出結果が見つかった場合は、個々の IAM ロールについて、同じタイプの、情報を提供する証拠の検出結果も少なくとも 1 つ、新たに表示されます。例えば、[すべてのアカウントで見つかった新しい位置情報] の検出結果が表示された場合、[特定のプリンシパルで見つかった新しい位置情報] の検出結果も表示されます。

検出結果グループ内の証拠のタイプ

- 見つかった新しい位置情報
- 見つかった新しい ASO (Autonomous System Organization: 自律システム組織)
- 見つかった新しいユーザーエージェント
- 発行された新しい API コール
- すべてのアカウントで見つかった新しい位置情報
- すべてのアカウントで見つかった新しい IAM プリンシパル

検出結果グループプロファイル

グループタイトルを選択すると、検出結果グループプロファイルが開き、そのグループに関する詳細が表示されます。[検出結果グループプロファイル] ページの [詳細] パネルには、検出結果グループの親と子に対し、1,000 件までのエンティティと検出結果を表示できます。

グループプロフィールページには、グループに設定された時間範囲が表示されます。この時間範囲とは、グループに含まれる最も古い検出結果または証拠の日付と時刻から、グループ内の最も新しい検出結果または証拠の日付と時刻までの範囲を指します。また、[検出結果グループの重要度] も確認できます。これは、グループ内の検出結果の中で重要度が最も高いカテゴリを指します。このプロファイルパネルの他の詳細としては、以下のものがあります。

- [関係する戦術] チェーンには、グループ内の検出結果から作成された戦術が表示されます。戦術は、「MITRE ATT&CK Matrix for Enterprise」に基づいています。戦術は、攻撃の代表的な進行状況 (初期ステージから最新ステージまでのどのステージか) を表す、色付きの点線で表示されます。つまり、チェーンの一番左の円は通常、攻撃者がお客様環境へのアクセスを取得または維持しようとしている、それほど深刻ではないアクティビティを表しています。逆に、右側のアクティビティは最も深刻で、データの改ざんや破壊が含まれる場合があります。
- このグループと他のグループとの関係。場合によっては、既存のグループのエンティティが関係する検出結果など、新たに検出された関係に基づいて、これまで接続されていなかった 1 つ以上の検出結果グループが新しいグループにマージされることがあります。この場合、Amazon Detective は親グループを非アクティブ化し、子グループを作成します。どのグループの系統も親グループまでトレースできます。グループには、次の関係を含めることができます。
  - 子検出結果グループ - 他の 2 つの検出結果グループに含まれる検索結果が新しい検出結果に含まれる場合に作成される検出結果グループ。任意の子グループについて、検出結果の親グループがリスト表示されます。
  - 親検出結果グループ - 検出結果グループから子グループが作成されると、その検出結果グループは親になります。検出結果グループが親の場合、関連する子も一緒にリスト表示されます。親グループがアクティブな子グループにマージされると、その親グループのステータスは [非アクティブ] になります。

プロファイルパネルが開く情報タブは 2 つあります。[関係するエンティティ] タブと [関係する検出結果] タブです。これらを使用すると、グループに関する詳細を表示できます。

[調査を実行] を使用して、調査レポートを生成します。生成されたレポートには、侵害を示す異常な動作が詳しく記載されています。

グループ内のプロファイルパネル

関係するエンティティ

グループ内の検出結果にリンクされているエンティティなど、検出結果グループ内のエンティティを示します。各エンティティに付けられたタグも表示されるので、タグに基づいて重要な工

ンティティをすばやく識別できます。エンティティを選択すると、そのエンティティのプロファイルが表示されます。

関係する検出結果

検出結果の重要度、関係するすべてのエンティティ、その検出結果が最初と最後に確認された日時など、各検出結果に関する詳細を示します。リストで検出結果タイプを選択すると、[検出結果の詳細] パネルが開き、その検出結果の詳細が表示されます。[関係する検出結果] パネルの一部として、Detective が動作グラフから収集した証拠に基づく [情報] の検出結果が表示される場合があります。

検出結果グループの視覚化

Amazon Detective では、検出結果グループのインタラクティブな視覚化を行うことができます。この視覚化は、少ない労力で問題をより迅速かつ詳細に調査できるようにするために設計されました。検出結果グループの [視覚化] パネルには、検出結果グループに含まれる検出結果とエンティティが表示されます。このインタラクティブな視覚化を使用して、検出結果グループの影響を分析、理解、トリアージできます。このパネルでは、[関係するエンティティ] と [関係する検出結果] のテーブルに表示される情報が視覚化されます。視覚的な表示から、検出結果またはエンティティを選択してさらに分析できます。

検出結果が集約された Detective 検出結果グループは、同じタイプのリソースに関係している検出結果のクラスターです。集約された検出結果を参照することで、検出グループの構成をすばやく判断し、セキュリティ上の問題をより迅速に解釈できます。検出結果グループの詳細パネルでは、比較的類似した検出結果をまとめて表示する、検出結果表示の拡張を行うことができます。例えば、同じ種類の、[情報] の検出結果と [中] の検出結果が証拠ノードとして集約されます。現時点では、検出結果グループのタイトル、ソース、タイプ、および重要度と、集約した検出結果を表示できます。

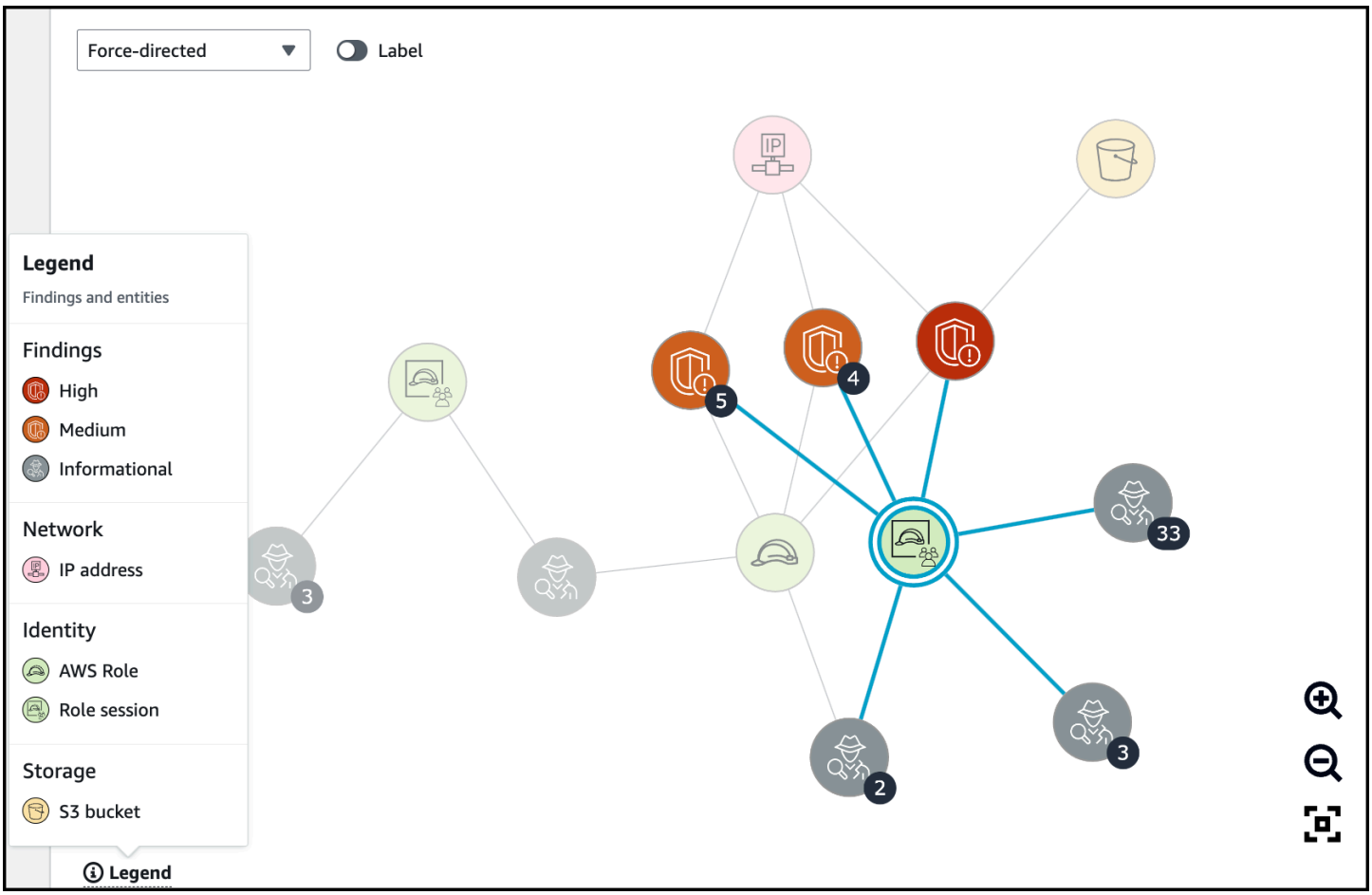
このインタラクティブパネルでは、次のことができます。

- [調査を実行] を使用して、調査レポートを生成します。生成されたレポートには、侵害を示す異常な動作が詳しく記載されています。
- 検出結果グループの詳細および集約された検出結果を表示することで、関係する証拠、エンティティ、および検出結果を分析する。
- エンティティと検出結果のラベルを表示して、セキュリティ上の問題がある可能性のある、影響を受けたエンティティを特定します。[ラベル] はオフに切り替えることができます。

- エンティティと検出結果を並べ替えて、それらの相互関係をよりよく理解できるようにします。検出結果グループ内の選択した項目を移動して、エンティティと検出結果をグループから分離します。
- 証拠、エンティティ、および検出結果を選択して、それらに関する詳細を表示します。複数の項目を選択するには、**command/control** を選択した上で項目を選択するか、ポインタを使って項目をドラッグアンドドロップします。
- すべてのエンティティと検出結果が検出結果グループウィンドウに収まるようにレイアウトを調整する。検出結果グループでどのエンティティタイプが一般的かを確認できます。

> **Note**
>
> 検出結果グループの [視覚化] パネルでは、最大 100 個のエンティティと検出結果を含めた検出結果グループを表示できます。

[レイアウトを選択してください] を選択すると、検出結果とエンティティをサークル、力指向、またはグリッドレイアウトで表示できます。[力指向] レイアウトでは、項目間のリンクの長さが一定になり、リンクが均等に分散されるように、エンティティと検出結果が配置されます。これにより、重複を減らすことができます。選択したレイアウトによって、[視覚化] パネル内での検出結果の配置が決まります。



上図の凡例は、現在のグラフ内のエンティティと検出結果に応じて変化する動的なものです。各視覚要素が何を表しているのかを識別するのに役立ちます。

生成 AI を活用した検出結果グループの概要

デフォルトでは、Amazon Detective は個々の検出結果グループの概要を自動的に提供します。概要は、Amazon Bedrock でホストされている生成人工知能 (生成 AI) モデルを活用して生成されています。

検出結果グループを使用することで、潜在的なセキュリティイベントに関連する複数のセキュリティ検出結果を調べ、潜在的な脅威アクターを特定できます。検出結果グループの検出結果グループ概要は、これらの機能に基づいて構築されています。検出結果グループの概要では、検出結果グループのデータが使用され、検出結果と影響を受けるリソースとの関係が迅速に分析され、潜在的な脅威が自然言語で要約されています。これらの概要を活用することで、より大規模なセキュリティ脅威を特定し、調査の効率を高め、対応期間を短縮することができます。

> **Note**
>
> 生成 AI を活用した検出結果グループの概要により、完全に正確な情報が得られる場合もありますが、常に得られるとは限りません。詳細については、「AWS Responsible AI Policy」を参照してください。

検出結果グループの概要の確認

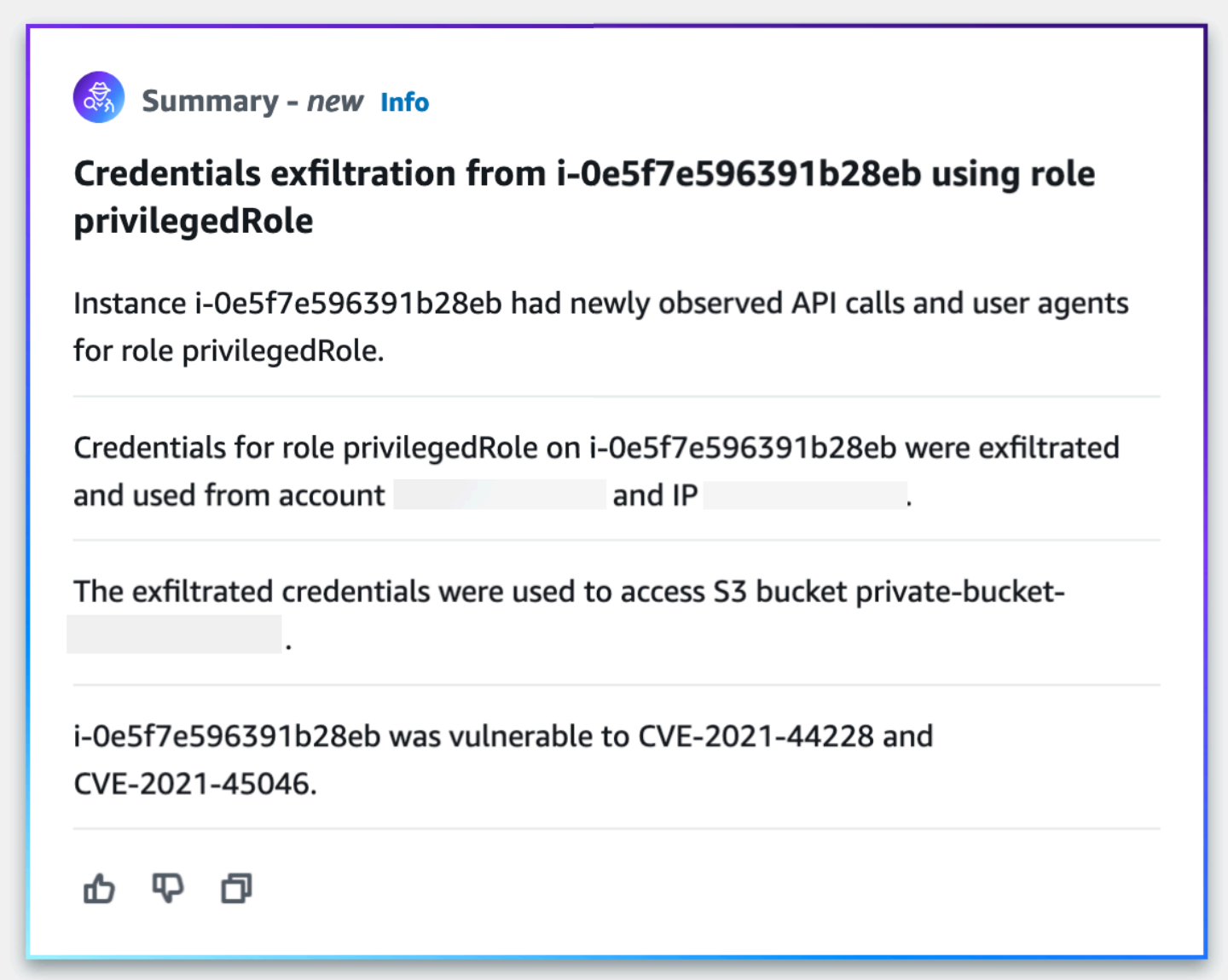
検出結果グループの検出結果グループ概要は、セキュリティイベントを明確で詳細な説明を提供します。説明は、自然言語で作成され、簡潔なタイトル、関連するリソースの要約、およびそれらのリソースに関する精選された情報が含まれます。

検出結果グループの概要を確認するには

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで [検出結果グループ] を選択します。
3. [検出結果グループ] テーブルで、概要を表示する検出結果グループを選択します。詳細ページが表示されます。

詳細ページでは、[概要] ペインを使用して、検出結果グループ内の上位の検出結果について生成された説明的な概要を確認できます。また、検出結果グループ内の上位の脅威イベントの分析を確認して、さらに調査することもできます。生成された概要をメモやチケットシステムに追加するには、ペインのコピーアイコンを選択します。概要がクリップボードにコピーされます。また、概要で検出結果グループの概要の出力に関するフィードバックを共有することもできます。これにより、将来のエクスペリエンスが向上します。フィードバックを共有するには、フィードバックの内容に応じて、サムズアップまたはサムズダウンアイコンを選択します。

> **Note**
>
> 提供される検出結果グループの概要に関するフィードバックは、モデルの調整には使用されません。Detective のプロンプトを効果的に作成しやすくする目的でのみ使用されます。



検出結果グループの概要を無効にする

デフォルトでは、検出結果グループでは検出結果グループの概要が有効になっています。検出結果グループの概要は、いつでも無効にできます。無効にする場合は、後で有効にすることができます。

検出結果グループの概要を無効にするには

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [検出結果グループの概要] で [編集] を選択します。
4. [有効] を無効にします。

5. [保存] を選択します。

検出結果グループの概要を有効にする

検出結果グループの検出結果グループ概要を無効にしていた場合、いつでも有効にできます。

検出結果グループの概要を有効にするには

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [検出結果グループの概要] で [編集] を選択します。
4. [有効] を有効にします。
5. [保存] を選択します。

サポートされるリージョン

検索グループの概要は、 AWS 以下のリージョンで利用できます。

- 米国東部 (バージニア北部)
- 米国西部 (オレゴン)
- アジアパシフィック (東京)
- 欧州 (フランクフルト)

Amazon Detective でのエンティティの分析

エンティティは、ソースデータから抽出される単一のオブジェクトです。例には、特定の IP アドレス、Amazon EC2 インスタンス、 AWS またはアカウントが含まれます。エンティティタイプのリストについては、the section called “動作グラフのデータ構造内のエンティティのタイプ” を参照してください。

Amazon Detective エンティティプロファイルは、エンティティとそのアクティビティに関する詳細情報を提供する単一のページです。エンティティプロファイルは、検出結果の調査に関する補足情報を得るために使用できるほか、疑わしいアクティビティを一般的に捕捉する取り組みの一部として使用することもできます。

コンテンツ

[Summary] (概要) ページを使用した対象エンティティの特定

Amazon Detective の [概要] ページを使用して、過去 24 時間のアクティビティの発生源を調査するためのエンティティを特定します。Amazon Detective の [Summary] (概要) ページは、特定のタイプの異常なアクティビティに関連するエンティティを特定するのに役立ちます。これは、調査のための出発点の 1 つとなり得ます。

[Summary] (概要) ページを表示するには、Detective のナビゲーションペインで [Summary] (概要) を選択します。Detective コンソールを最初に開いたときに、デフォルトで [Summary] (概要) ページも表示されます。

[Summary] (概要) ページから、次の基準を満たすエンティティを特定できます。

- Detective によって特定された潜在的なセキュリティイベントを示す調査
- 新たに観察されたジオロケーションで発生したアクティビティに関係するエンティティ
- API コール数が最多のエンティティ
- トラフィック量が最大だった EC2 インスタンス
- コンテナ数が最多のコンテナクラスター

各 [Summary] (概要) ページのパネルから、選択したエンティティのプロファイルにピボットできます。

[概要] ページを確認しながら、過去 365 日間の任意の 24 時間枠のアクティビティを表示する [時間範囲] の値を調整できます。[開始日時] を変更すると、[終了日時] が、選択した開始時刻から 24 時間後の日時に自動的に更新されます。

Detective を使用すると、最長 1 年間の履歴イベントデータにアクセスできるようになりました。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によって表示されます。Detective GuardDuty はこれらの変更を調査結果に関連付けます。

Detective のソースデータについて詳しくは、「動作グラフで使用されるソースデータ」を参照してください。

調査

調査は、Detective によって特定された潜在的なセキュリティイベントを示します。調査パネルでは、重要な調査と、これに対応し、一定期間にセキュリティイベントの影響を受けた AWS ロールとユーザーを確認できます。調査では侵害の指標をグループ化して、 AWS 悪意のある行動やその影響を示すような異常なアクティビティにリソースが関与しているかどうかを判断するのに役立ちます。

[すべての調査を表示] を選択して検出結果を確認し、検出結果のグループとリソースの詳細をトリアージしてセキュリティ調査を加速させます。調査は、選択したスコープ時間に応じて表示されます。スコープ時間は、過去 365 日間の調査を 24 時間枠で表示するように調整できます。[重要な調査] に直接移動すると、詳細な調査レポートを確認できます。

AWS 疑わしいアクティビティがあると思われるロールまたはユーザーを特定した場合は、調査パネルからそのロールまたはユーザーに直接移動して調査を続行できます。ロールまたはユーザーにピボットして [調査を実行] をクリックすると、調査レポートが生成されます。ロールまたはユーザーに対して調査を実行すると、そのロールまたはユーザーは [調査済み] タブに移動します。

新たに観察された位置情報

[新たに観察された位置情報] には、直近 24 時間のアクティビティの起点であったが、その前のベースライン期間には見られなかった地理的場所が示されます。

パネルには、最大 100 個のジオロケーションが含まれます。場所は地図上でマークされ、地図の下の表にリストされます。

表には、各ジオロケーションについて、直近 24 時間にそのジオロケーションから実行された API コールの失敗数と成功数が表示されます。

各ジオロケーションを展開して、そのジオロケーションから API コールを実行したユーザーとロールのリストを表示できます。各プリンシパルについて、表にはタイプと関連する AWS アカウントがリスト表示されます。

疑わしいと思われるユーザーまたはロールを特定した場合は、パネルからユーザーまたはロールのプロファイルに直接ピボットして、調査を続行できます。プロファイルにピボットするには、ユーザーまたはロールの識別子を選択します。

Detective は MaxMind GeoIP データベースを使用してリクエストの場所を特定します。 MaxMind 国や IP の種類などの要因によって精度は異なりますが、国レベルでは非常に高い精度でデータを報告します。詳細については MaxMind、「MaxMind IP ジオロケーション」を参照してください。GeoIP データのいずれかが正しくないと思われる場合は、「GeoIP2データの修正」MaxMind でMaxmindに修正リクエストを送信できます。

過去 7 日間にアクティブだった検出結果グループ

[過去 7 日間にアクティブだった検出結果グループ] には、環境で一定期間内に発生した、Detective からの検出結果、エンティティ、証拠の相関性があるグループが表示されます。これらのグループにより、悪意のある動作を示す異常なアクティビティが明らかになります。概要ページには、過去 1 週間にアクティブだった検出結果の重要度の順に、最大 5 つのグループが表示されます。

詳細を確認するには、[戦術]、[アカウント]、[リソース]、[検出結果] の値を選択します。

検出結果グループは毎日生成されます。関心のある検出結果グループが見つかったら、タイトルを選択してグループプロファイルの詳細ビューに移動し、調査を進めることができます。

API コール量が最も多いロールとユーザー

[API コール量が最も多いロールとユーザー] には、直近 24 時間で行った API コール (呼び出し) 回数が最も多いユーザーとロールが表示されます。

パネルには、最大 100 個のユーザとロールを含めることができます。各ユーザーまたはロールについて、タイプ (ユーザーまたはロール) および関連するアカウントを表示できます。また、直近 24 時間にそのユーザーまたはロールによって発行された API コールの数を表示することもできます。

デフォルトでは、サービスリンクロールが表示されます。 AWS CloudTrail サービスにリンクされたロールでは大量のアクティビティが発生する可能性があり、これによってさらに調査したいプリンシパルが変わってしまいます。[サービスリンクロールを表示] をオフにすることで、サービスリンクロールを概要ページビューから除外できます。

このパネルのデータを含むカンマ区切り値 (.csv) ファイルをエクスポートできます。

直近 7 日間の API コール量のタイムラインもあります。タイムラインは、API コール量がそのプリンシパルにとって異常であるかどうかを判断するのに役立ちます。

API コール量が疑わしいと思われるユーザーまたはロールを特定した場合は、パネルからユーザーまたはロールプロファイルに直接ピボットして、調査を続行できます。ユーザーまたはロールに関連付けられているアカウントのプロファイルを表示することもできます。プロファイルを表示するには、ユーザー、ロール、またはアカウント識別子を選択します。

トラフィック量が最も多い EC2 インスタンス

[トラフィック量が最多の EC2 インスタンス] には、直近 24 時間で合計トラフィック量が最多だった EC2 インスタンスが表示されます。

パネルには、最大 100 個の EC2 インスタンスを含めることができます。各 EC2 インスタンスについて、関連付けられたアカウントと、直近 24 時間のインバウンドバイト数、アウトバウンドバイト数、および合計バイト数を表示できます。

このパネルのデータを含んだカンマ区切り値 (CSV) ファイルをエクスポートできます。

直近 7 日間のインバウンドトラフィックとアウトバウンドトラフィックを示すタイムラインも表示できます。タイムラインは、トラフィックの量がその EC2 インスタンスにとって異常であるかどうかを判断するのに役立ちます。

トラフィック量が疑わしいと思われる EC2 インスタンスを特定した場合は、パネルから EC2 インスタンスプロファイルに直接移動して、調査を続行できます。EC2 インスタンスを所有するアカウントのプロファイルを表示することもできます。プロファイルを表示するには、EC2 インスタンスまたはアカウント識別子を選択します。

最も多くの Kubernetes ポッドが作成されたコンテナクラスター

[最も多くの Kubernetes ポッドが作成されたコンテナクラスター] には、過去 24 時間に最も多くのコンテナが実行されたクラスターが表示されます。

このパネルには、最大 100 個のクラスターが、関連する検出結果の多い順に表示されます。クラスターごとに、関連するアカウント、そのクラスター内の現在のコンテナ数、過去 24 時間にそのクラスターに関連付けられた検出結果の数を確認できます。このパネルのデータを含んだカンマ区切り値 (CSV) ファイルをエクスポートできます。

最近の検出結果を含むクラスターを特定した場合は、パネルからクラスタープロファイルに直接ピボットすることで、調査を続行できます。クラスターを所有するアカウントのプロファイルにピボットすることもできます。プロファイルにピボットするには、クラスター名またはアカウント識別子を選択します。

近似値の通知

[API コール量が最も多いロールとユーザー] および [トラフィック量が最多の EC2 インスタンス] で値の後にアスタリスク (*) が続く場合は、その値が近似値であることを意味します。実際の値は、表示された値以上です。

これは、Detective が各時間間隔の量を計算するために使用する方法が原因で発生します。[Summary] (概要) ページでは、時間間隔は 1 時間です。

各時間について、Detective は、最大の量を持つ 1,000 のユーザー、ロール、または EC2 インスタンスの合計量を計算します。残りのユーザー、ロール、または EC2 インスタンスのデータは除外されます。

リソースが上位 1,000 に含まれることもあれば含まれないこともある場合、そのリソースの計算量にはすべてのデータが含まれていない可能性があります。上位 1,000 に含まれていなかった時間間隔のデータは除外されます。

これは [Summary] (概要) ページにのみ適用されることに注意してください。ユーザー、ロール、または EC2 インスタンスのプロファイルは、正確な詳細を提供します。

エンティティプロファイルの使用

エンティティプロファイルは、次のいずれかのアクションを実行する際に表示されます。

- Amazon GuardDuty コンソールから、選択した結果に関連するエンティティを調査するオプションを選択します。

the section called “別のコンソールからのピボット” を参照してください。

- エンティティプロファイルの Detective URL に移動する。

  the section called “URL を使用した移動” を参照してください。
- Detective コンソールで Detective 検索を使用してエンティティを検索する。
- 別のエンティティプロファイルまたは検出結果の概要から、エンティティプロファイルへのリンクを選択する。

エンティティプロファイルのスコープ時間

スコープ時間を指定せずにエンティティプロファイルに直接移動すると、スコープ時間は直近 24 時間に設定されます。

あるエンティティプロファイルから別のエンティティプロファイルに移動しても、現在選択されているスコープ時間は変わりません。

検出結果の概要からエンティティプロファイルに移動すると、スコープ時間は検出結果の時間枠に設定されます。

スコープ時間をカスタマイズしてエンティティプロファイルに表示されるデータを制限する方法については、「スコープ時間の管理」を参照してください。

エンティティの識別子とタイプ

プロファイルの上部には、エンティティ識別子とエンティティタイプがあります。各エンティティタイプには対応するアイコンがあり、プロファイルのタイプの視覚的なインジケータを提供します。

関係する検出結果

各プロファイルには、スコープ期間中にエンティティが関係した検出結果のリストが含まれます。

各検出結果の詳細を表示したり、検出結果の時間枠を反映するように範囲時間を変更したり、検出結果の概要に移動して他の関係するリソースを検索したりできます。

the section called “エンティティの検出結果の表示” を参照してください。

このエンティティに関係する検出結果グループ

各プロファイルには、エンティティが含まれる検出結果グループのリストが含まれています。

検出結果グループは、検出結果、エンティティ、および証拠で構成されます。これらは、Detective が、発生する可能性のあるセキュリティ問題についてより多くのコンテキストを提供するために収集したものです。

検出結果グループの詳細については、「the section called “検出結果グループ”」を参照してください。

エンティティの詳細と分析結果を含むプロファイルパネル

各エンティティプロファイルには、1 つ以上のタブセットが含まれています。各タブには、1 つまたは複数のプロファイルパネルが含まれています。各プロファイルパネルには、動作グラフのデータから生成されたテキストとビジュアライゼーションが含まれています。特定のタブとプロファイルパネルは、エンティティタイプに合わせて調整されます。

ほとんどのエンティティについては、最初のタブの上部にあるパネルに、エンティティに関する概要レベルの情報が表示されます。

他のプロファイルパネルは、さまざまなタイプのアクティビティを強調表示します。検出結果と関係するエンティティについては、エンティティのプロファイルパネルの情報を確認することで、調査の完了に役立つ追加的な証拠を得ることができます。各プロファイルパネルでは、情報の使用方法に関するガイダンスにアクセスできます。詳細については、「the section called “プロファイルパネルのガイダンスの使用”」を参照してください。

プロファイルパネル、プロファイルパネルに含まれるデータのタイプ、およびそれらを操作するために使用可能なオプションの詳細については、the section called “プロファイルパネルの表示と操作” を参照してください。

プロファイルパネルの表示と操作

Amazon Detective コンソールの各エンティティプロファイルは、一連のプロファイルパネルで構成されています。プロファイルパネルは、エンティティに関連する一般的な詳細を表示したり、特定のアクティビティを重点的に表示したりするビジュアライゼーションを提供する機能です。プロファイルパネルは、さまざまな種類のビジュアライゼーションを使用して、さまざまな種類の情報を表示します。また、追加の詳細やその他のプロファイルへのリンクを提供することもできます。

各プロファイルパネルは、アナリストがエンティティとその関連アクティビティに関する特定の質問に対する回答を得るのをサポートすることを目的としています。それらの質問に対する回答は、そのアクティビティが真の脅威であるかどうかについての結論を得るのに役立ちます。

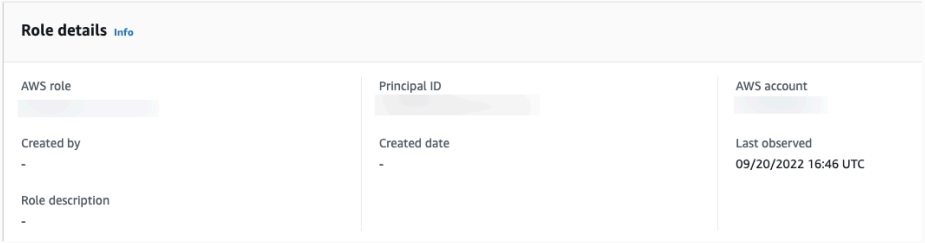
コンテンツ

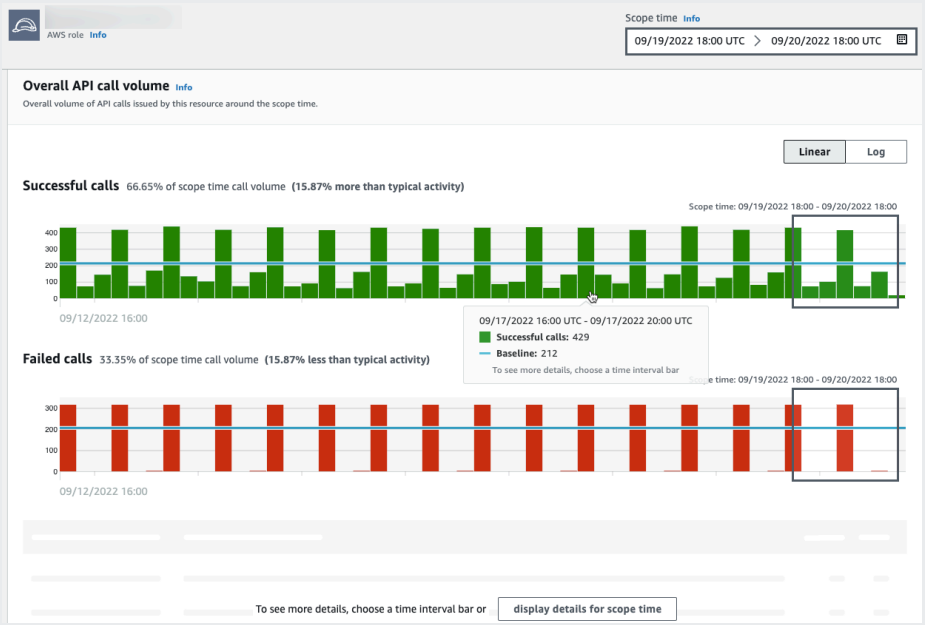
プロファイルパネルのコンテンツ

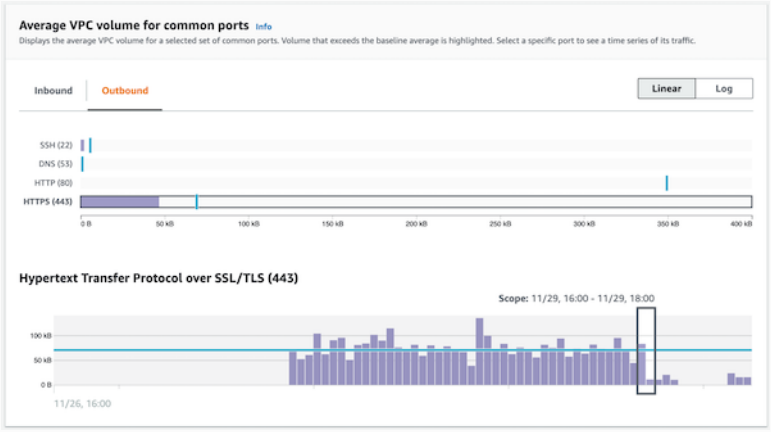
プロファイルパネルは、さまざまな種類のビジュアライゼーションを使用して、さまざまな種類の情報を表示します。

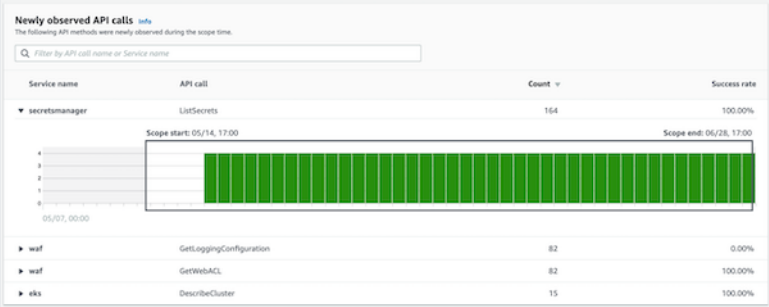
プロファイルパネルの情報の種類

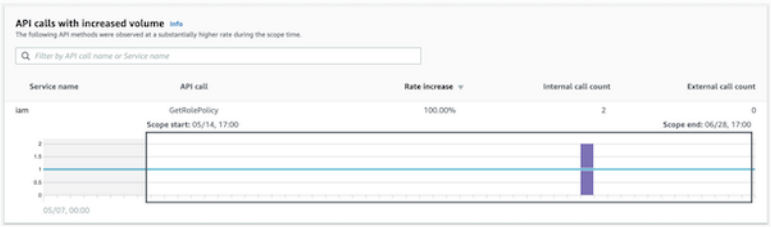
プロファイルパネルは、通常、次の種類のデータを提供します。

パネルデータのタイプ	説明
検出結果またはエンティティに関する概要レベルの情報	最もシンプルなタイプのパネルでは、エンティティに関する基本的な情報が提供されます。 情報パネルに含まれる情報の例として、識別子、名前、タイプ、作成日を挙げることができます。  ほとんどのエンティティプロファイルには、そのエンティティに関する情報パネルが含まれています。
時間の経過に合わせたアクティビティの一般的な概要	エンティティのアクティビティの概要を時間の経過に合わせて表示します。 このタイプのパネルは、スコープ時間中にエンティティがどのように動作しているかについての全体的なビューを提供します。

パネルデータのタイプ	説明
	 Detective プロファイルパネルで提供される概要データの例をいくつか以下に示します。 • 失敗した API コールと成功した API コール • インバウンド VPC ボリュームとアウトバウンド VPC ボリューム

パネルデータのタイプ	説明
値でグループ化されたアクティビティの概要	エンティティのアクティビティの概要を、特定の値別にグループ化して表示します。 このタイプのプロファイルパネルは、EC2 インスタンスについてのプロファイルに表示されます。プロファイルパネルには、特定のタイプのサービスに関連付けられている共通ポートについて、EC2 インスタンスとの間で送受信される VPC フローログデータ量の平均値が表示されます。 

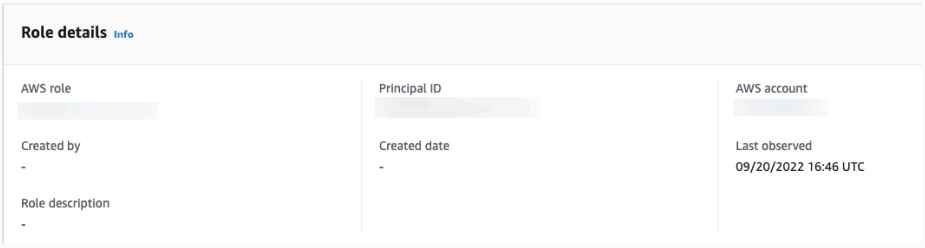
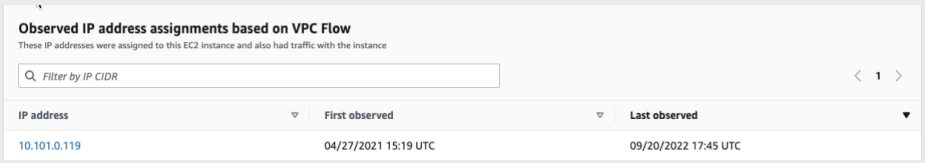
パネルデータのタイプ	説明
スコープ時間中にのみ開始されたアクティビティ	調査中、特定の時間枠に発生し始めたアクティビティのみを確認することは有益です。 例えば、該当の時間枠よりも前には見られなかった API コール、地理的場所、またはユーザーエージェントがあるかどうかを確認できます。  動作グラフがまだトレーニングモードの場合は、プロファイルパネルに通知メッセージが表示されます。メッセージは、動作グラフに少なくとも 2 週間分のデータが蓄積された場合に削除されます。トレーニングモードの詳細については、the section called “新しい動作グラフのトレーニング期間” を参照してください。

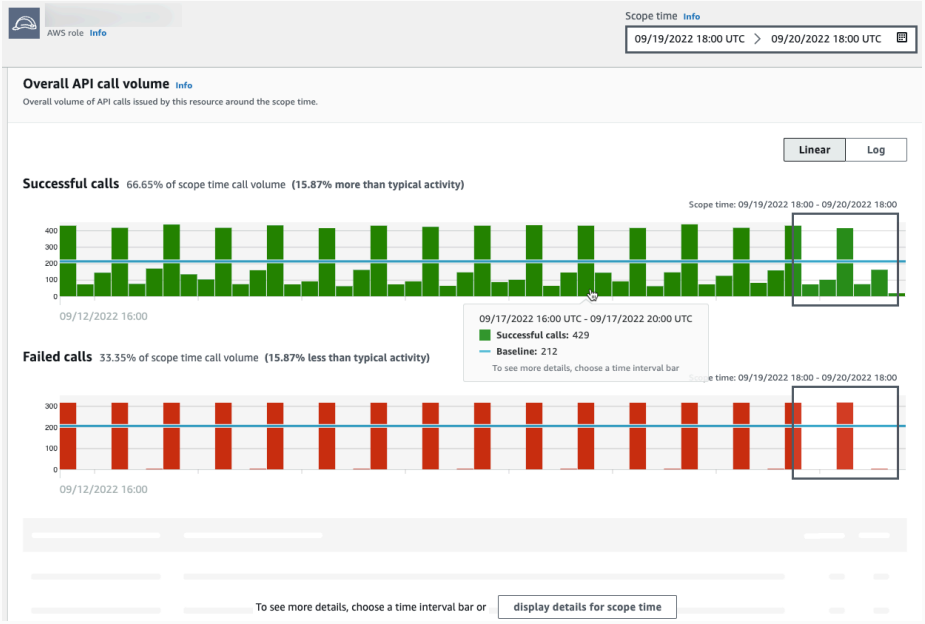
パネルデータのタイプ	説明
スコープ期間中に大幅に変化したアクティビティ	新しいアクティビティパネルと同様に、プロファイルパネルは、スコープ期間中に大幅に変化したアクティビティを表示することもできます。 例えば、あるユーザーが定期的に特定の API コールを週に数回発行することがあります。同じユーザーが突然、1 日に同じコールを複数回発行した場合、これは悪意のあるアクティビティを示唆している可能性があります。  動作グラフがまだトレーニングモードの場合は、プロファイルパネルに通知メッセージが表示されます。メッセージは、動作グラフに少なくとも 2 週間分のデータが蓄積された場合に削除されます。トレーニングモードの詳細については、the section called “新しい動作グラフのトレーニング期間” を参照してください。

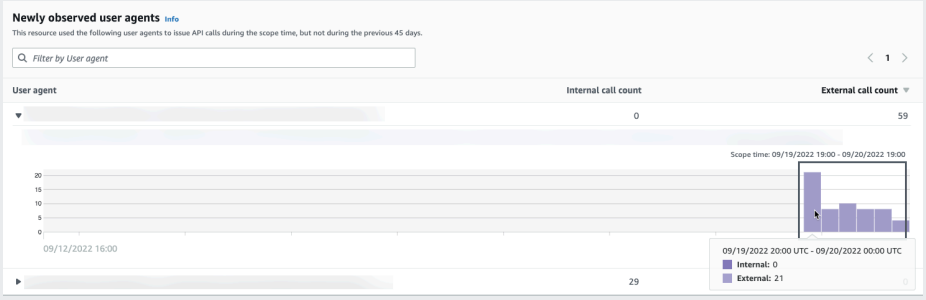
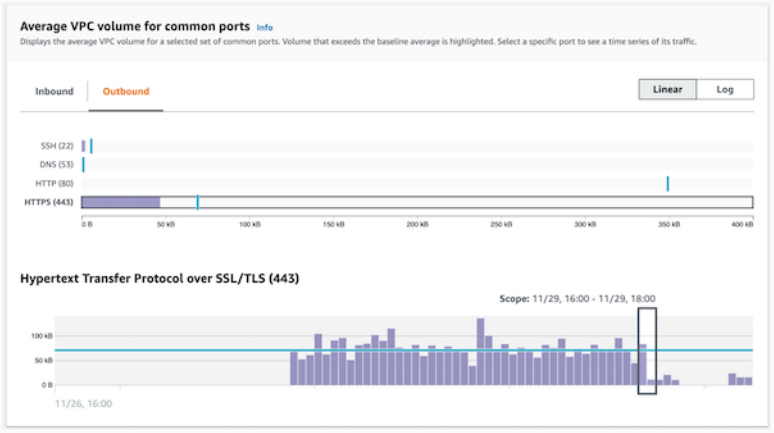
プロファイルパネルのビジュアライゼーションのタイプ

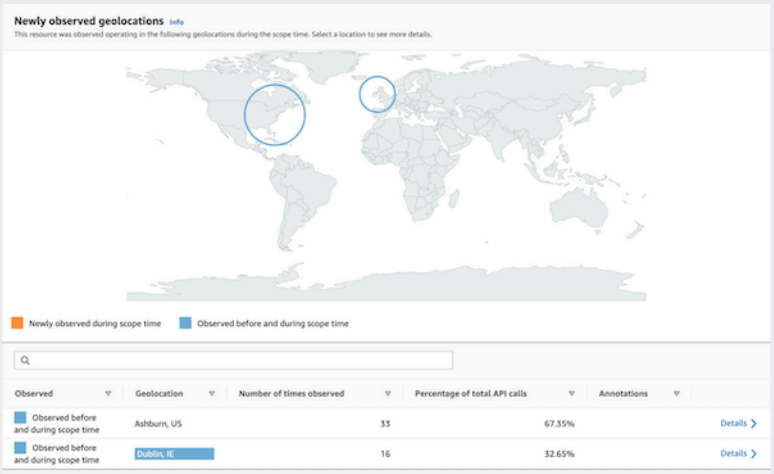
プロファイルパネルのコンテンツは、以下のいずれかの形式で定義できます。

ビジュアライゼーションのタイプ	説明
キーバリューペア	ビジュアライゼーションの最もシンプルなタイプは、キーバリューペアのセットです。 検出結果またはエンティティ情報パネルは、キーバリューペアのパネルの最も一般的な例です。

ビジュアライゼーションのタイプ	説明
	 キーバリューペアは、他のタイプのパネルにさらに情報を追加するためにも使用できます。 キーバリューペアのパネルから、値がエンティティの識別子である場合は、そのプロファイルにピボットできます。
テーブル	テーブルは、シンプルな複数列の項目リストです。  テーブルのソート、フィルタリング、およびページ分割を行うことができます。 ページごとに表示するエントリ数を変更できます。the section called “プロファイルパネルの詳細設定” を参照してください。 テーブル内の値がエンティティの識別子である場合は、そのプロファイルにピボットできます。

ビジュアライゼーションのタイプ	説明
タイムライン	タイムラインの視覚化では、定義された間隔について、一定期間にわたって集計された値が表示されます。  タイムラインは現在のスコープタイムを強調表示し、スコープ時間の前後の時間が追加的に含まれます。周辺時間により、スコープ時間内のアクティビティのコンテキストを確認できます。 時間間隔にカーソルを合わせると、その時間間隔のデータの概要を表示できます。

ビジュアライゼーションのタイプ	説明
拡張可能なテーブル	拡張可能なテーブルは、テーブルとタイムラインを組み合わせたものです。  ビジュアライゼーションはテーブルとして開始します。 テーブルのソート、フィルタリング、およびページ分割を行うことができます。 ページごとに表示するエントリ数を変更できます。the section called “プロファイルパネルの詳細設定” を参照してください。 その後、各行を展開して、その行に固有のタイムラインのビジュアライゼーションを表示できます。
棒グラフ	棒グラフは、グループに基づいて値を表示します。 グラフによっては、関連するアクティビティのタイムラインを表示する棒を選択できる場合があります。 

ビジュアライゼーションのタイプ	説明
ジオロケーションチャート	ジオロケーションチャートは、地理的場所に基づいてデータを強調表示するためにマークされたマップを表示します。これに続いて、個々のジオロケーションに関する詳細を含むテーブルが表示される場合があります。  受信する位置情報データを処理する場合、Detective は、緯度と経度の値を小数点第一位になるように四捨五入します。

プロファイルパネルのコンテンツに関するその他の注意事項

プロファイルパネルのコンテンツを表示するときは、以下の点に注意してください。

データが概数である旨の警告

この警告は、該当するデータの量により、数が極端に少ない項目が表示されていないことを示唆するものです。

完全に正確な数を確認するには、データの量を減らします。これを実行するための最も簡単な方法は、スコープ時間の長さを短くすることです。the section called “スコープ時間の管理” を参照してください。

地理的場所の丸め

Detective は、すべての緯度と経度の値を小数点第一位に丸めます。

Detective が API コールを表す方法の変更

2021 年 7 月 14 日以降、Detective は、各 API コールを実行したサービスを追跡します。Detective は、API メソッドを表示するたびに、関連するサービスも表示します。API コールに関する情報を表示するプロファイルパネルでは、コールは常にサービスごとにグループ化されます。その日付より前に Detective が取り込んだデータについては、サービス名は [Unknown service] (不明なサービス) としてリストされます。

また、2021 年 7 月 14 日以降、アカウントとロールについては、[全体的な API コール量] プロファイルパネルのアクティビティの詳細には、コールを発行したリソースの AKID が表示されなくなります。アカウントについては、Detective はコールを発行したプリンシパル (ユーザーまたはロール) の識別子を表示します。ロールについては、Detective はロールセッションの識別子を表示します。2021 年 7 月 14 日より前に Detective が取り込んだデータについては、識別子は [不明なリソース] としてリストされます。

API コールのリストを表示するプロファイルパネルについては、関連付けられたタイムラインは、この移行が生じた期間を強調表示します。強調表示は 2021 年 7 月 14 日に開始され、更新が Detective で完全に伝達されたときに終了します。

プロファイルパネルの詳細設定を設定する

Detective コンソールでは、[詳細設定] ページで [テーブルの長さ] と [タイムスタンプ] の表示を設定できます。

テーブルの長さを設定する

テーブルまたは展開可能なテーブルを含むプロファイルパネルについては、ページあたりで表示する行数を設定できます。

ページあたりのエントリ数の詳細設定を設定します。

1. https://console.aws.amazon.com/detective/ で Amazon 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 [Preferences] (詳細設定) を選択します。
3. [詳細設定] ページの [テーブルの長さ] で [編集] をクリックします。
4. 各ページに表示するテーブルの行数を選択します。
5. [保存] を選択します。

タイムスタンプ形式を設定する

プロファイルパネルでは、Detective 内の個々の IAM ユーザーや IAM ロールのすべてのタイムスタンプに適用されるタイムスタンプ形式の設定を行うことができます。

> **Note**
>
> タイムスタンプ形式の設定は、 AWS アカウント全体には適用されません。

タイムスタンプの設定を行います。

1. https://console.aws.amazon.com/detective/ で Amazon 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 [Preferences] (詳細設定) を選択します。
3. [詳細設定] ページの [タイムスタンプの設定] で、すべてのタイムスタンプの優先表示を表示および変更します。
4. デフォルトでは、タイムスタンプ形式は UTC に設定されています。ローカルタイムゾーンを選択するには [編集] をクリックします。

   例：

   Example

   UTC - 22 年 9 月 20 日 16:39 UTC

   ローカル - 2022 年 9 月 20 日 9:39 (UTC-07:00)
5. [保存] を選択します。

プロファイルパネルから別のコンソールへのピボット

EC2 インスタンス、 IAM ユーザー、および IAM ロールについては、詳細プロファイルパネルから、対応するコンソールに直接移動できます。コンソールから入手できる情報を確認することで、調査のための追加情報を得ることができます。

[EC2 instance details] (EC2 インスタンスの詳細) プロファイルパネルでは、EC2 インスタンス識別子が Amazon EC2 コンソールにリンクされています。

[User details] (ユーザーの詳細) プロファイルパネルでは、ユーザー名は IAM コンソールにリンクされています。

[Role details] (ロールの詳細) プロファイルパネルでは、ロール名は IAM コンソールにリンクされています。

プロファイルパネルから別のエンティティプロファイルへのピボット

プロファイルパネルに別のエンティティの識別子が含まれている場合、それは通常、そのエンティティプロファイルへのリンクです。例外は、EC2 インスタンス、IAM ユーザー、および IAM ロールのプロファイル上の Amazon EC2 および IAM コンソールへのリンクです。the section called “別のコンソールへのピボット” を参照してください。

例えば、IP アドレスのリストから、特定の IP アドレスのプロファイルを表示できる場合があります。これにより、調査の完了に役立つ他の情報が入手できるかどうかを確認できます。

プロファイルパネルにおけるアクティビティの詳細の確認

調査中に、エンティティのアクティビティのパターンをさらに調査したい場合があります。

次のプロファイルパネルでは、アクティビティの詳細の概要を表示できます。

- [全体的な API コール量](ユーザーエージェントプロファイルのプロファイルパネルを除く)
- 新たに観察された位置情報
- [Overall VPC flow volume] (全体的な VPC のフロー量)
- [VPC flow volume to and from the finding IP address] (検出結果 IP アドレスの間で送受信される VPC フロー量) (単一の IP アドレスに関連付けられている検出結果に関するもの)
- コンテナの詳細
- クラスターの [VPC フロー量]
- Kubernetes API アクティビティ全体

アクティビティの詳細を確認することで、次の種類の質問に対する回答を得ることができます。

- 使用された IP アドレス
- これらの IP アドレスがある場所
- 各 IP アドレスが実行した API コール、およびそれらのコールを実行した際の実行元のサービス

- コールの実行に使用されたプリンシパルまたはアクセスキー識別子 (AKID)
- それらのコールに使用されたリソース
- コールが実行された回数 成功数と失敗数
- 各 IP アドレスとの間で送受信された VPC フローログデータの量
- 特定のクラスター、イメージ、またはポッドでアクティブだったコンテナ

トピック

[全体的な API コール量] のアクティビティの詳細

[全体的な API コール量] のアクティビティの詳細は、選択した時間範囲中に発行された API コールを示します。

単一の時間間隔のアクティビティの詳細を表示するには、チャートで時間間隔を選択します。

現在のスコープ時間のアクティビティの詳細を表示するには、[Display details for scope time] (スコープ時間の詳細を表示) を選択します。

なお、Detective は、2021 年 7 月 14 日から API コールのサービス名の保存および表示を開始しました。その日付は、プロファイルパネルのタイムラインで強調表示されます。その日付より前に発生するアクティビティについては、サービス名は [Unknown service] (不明なサービス) となります。

アクティビティの詳細 (ユーザー、ロール、アカウント、ロールセッション、EC2 インスタンス、S3 バケット) の内容

IAM ユーザー、IAM ロール、アカウント、ロールセッション、EC2 インスタンス、および S3 バケットについては、アクティビティの詳細には次の情報が含まれます。

- 各タブは、選択した時間範囲中に発行された一連の API コールに関する情報を表示します。

  S3 バケットについては、情報は S3 バケットに対して実行された API コールを反映したものとなります。

API コールは、それらを呼び出したサービス別にグループ化されます。S3 バケットについては、サービスは常に Amazon S3 です。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。

- 各エントリについて、アクティビティの詳細では、成功したコールと失敗したコールの数が表示されます。[Observed IP addresses] (観察された IP アドレス) のタブには、各 IP アドレスの場所も表示されます。
- 各エントリは、コールを実行したユーザーに関する情報を表示します。アカウントについては、アクティビティの詳細でユーザーまたはロールが識別されます。ロールについては、アクティビティの詳細でロールセッションが識別されます。ユーザーおよびロールセッションについては、アクティビティの詳細でアクセスキー識別子 (AKID) が識別されます。

  2021 年 7 月 14 日現在、アカウントプロファイルについては、アクティビティの詳細では、AKID ではなく、ユーザーまたはロールが表示されることに注意してください。ロールプロファイルについては、アクティビティの詳細には、AKID ではなくロールセッションが表示されます。2021 年 7 月 14 日より前に発生するアクティビティについては、発信者は [Unknown resource] (不明なリソース) としてリストされます。

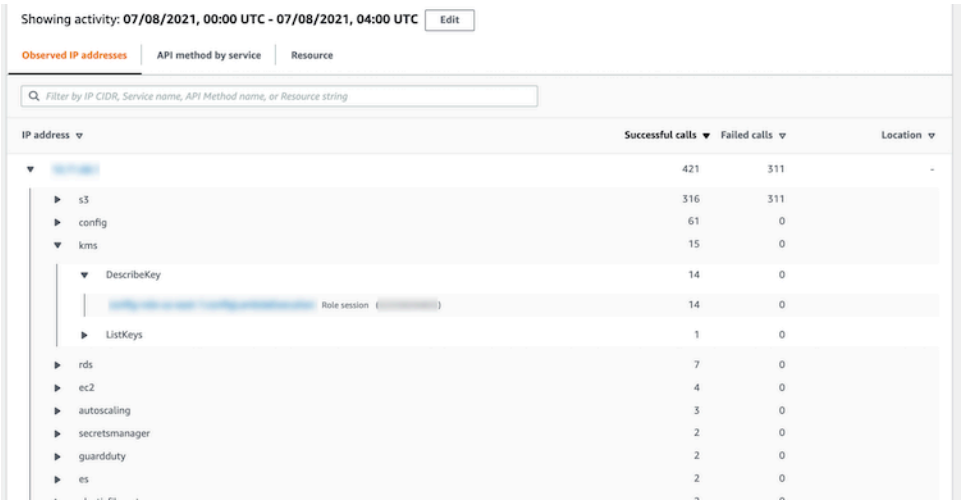
アクティビティの詳細には、次のタブが含まれます。

[Observed IP addresses] (観察された IP アドレス)

API コールを発行するために使用される IP アドレスのリストが最初に表示されます。

各 IP アドレスを展開して、その IP アドレスから発行された API コールのリストを表示できます。API コールは、それらを呼び出したサービス別にグループ化されます。S3 バケットについては、サービスは常に Amazon S3 です。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。

その後、各 API コールを展開して、その IP アドレスからの発信者のリストを表示できます。プロファイルに応じて、発信者は、ユーザー、ロール、ロールセッション、または AKID である場合があります。

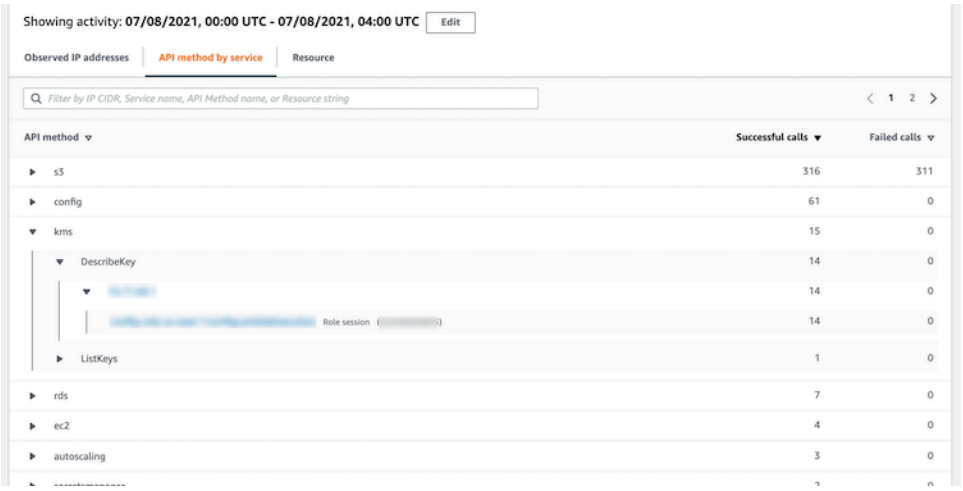


[API method by service] (サービス別の API メソッド)

発行された API コールのリストが最初に表示されます。API コールは、コールを発行したサービス別にグループ化されます。S3 バケットについては、サービスは常に Amazon S3 です。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。

各 API メソッドを展開して、コールが発行された際の発行元となった IP アドレスのリストを表示できます。

その後、各 IP アドレスを展開して、その IP アドレスからその API コールを発行した AKID のリストを表示できます。

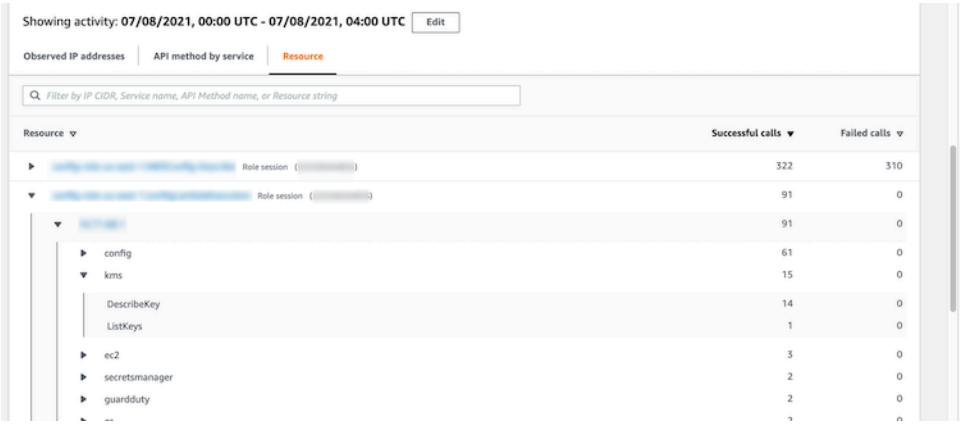


リソースまたはアクセスキー ID

API コールの発行に使用されたユーザー、ロール、ロールセッション、または AKID のリストが最初に表示されます。

各発信者を展開して、発信者が API コールを発行した際の発行元となった IP アドレスのリストを表示できます。

その後、各 IP アドレスを展開して、その IP アドレスからその発信者によって発行された API コールのリストを表示できます。API コールは、コールを発行したサービス別にグループ化されます。S3 バケットについては、サービスは常に Amazon S3 です。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。



アクティビティの詳細の内容 (IP アドレス)

IP アドレスについては、アクティビティの詳細には次の情報が含まれます。

- 各タブは、選択した時間範囲中に発行された一連の API コールに関する情報を表示します。API コールは、コールを発行したサービス別にグループ化されます。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。
- 各エントリについて、アクティビティの詳細では、成功したコールと失敗したコールの数が表示されます。

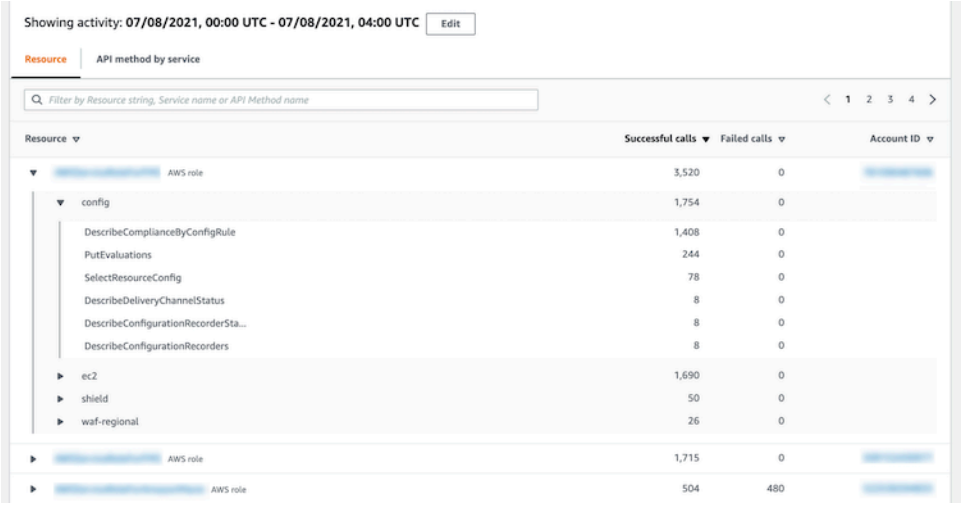
アクティビティの詳細には、次のタブが含まれます。

リソース

IP アドレスから API コールを発行したリソースのリストが最初に表示されます。

リストには、各リソースについて、リソース名、タイプ、および AWS アカウントが含まれます。

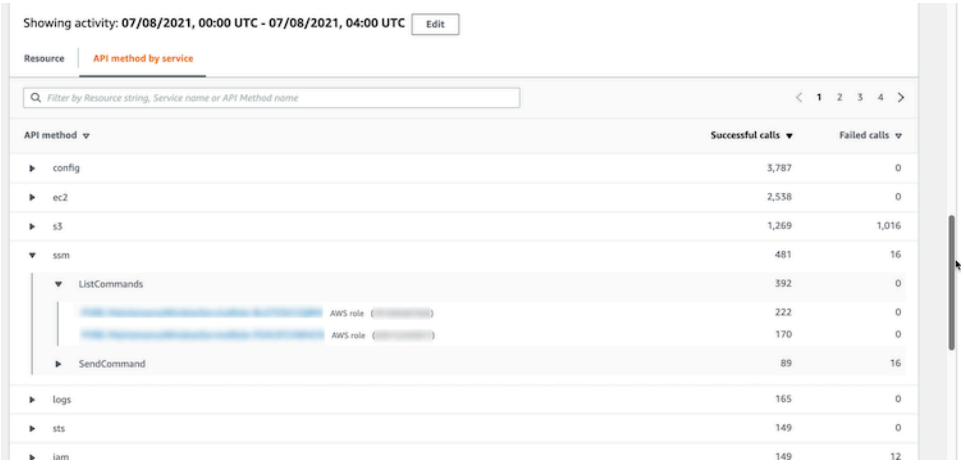
各リソースを展開して、リソースが IP アドレスから発行した API コールのリストを表示できます。API コールは、コールを発行したサービス別にグループ化されます。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。



[API method by service] (サービス別の API メソッド)

発行された API コールのリストが最初に表示されます。API コールは、コールを発行したサービス別にグループ化されます。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。

各 API コールを展開して、選択した期間中に IP アドレスから API コールを発行したリソースのリストを表示できます。



アクティビティの詳細のソート

アクティビティの詳細はいずれかのリストの列でソートすることができます。

最初の列を使用してソートすると、最上位のリストのみがソートされます。下位レベルのリストは常に成功した API コールの数でソートされます。

アクティビティの詳細のフィルタリング

フィルタリングオプションを使用して、アクティビティの詳細に表示されるアクティビティの特定のサブセットまたは側面に焦点を当てることができます。

すべてのタブで、最初の列のいずれかの値でリストをフィルタリングできます。

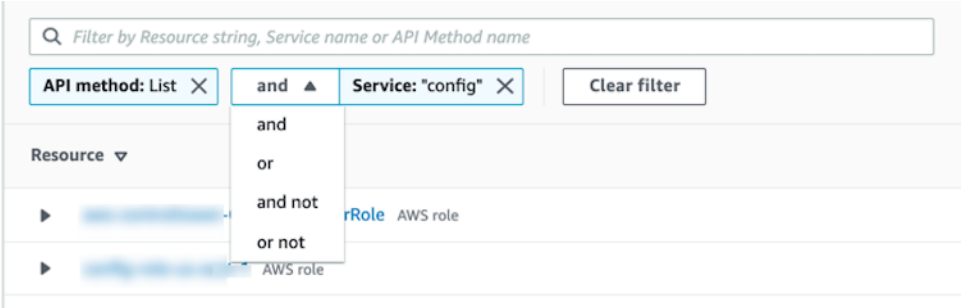
フィルターを追加するには

1. フィルターボックスを選択します。
2. [Properties] (プロパティ) から、フィルタリングに使用するプロパティを選択します。
3. フィルタリングに使用する値を入力します。フィルターは部分的な値をサポートします。例えば、API メソッドでフィルタリングする場合、**`Instance`** でフィルタリングすると、結果には名前に `Instance` が含まれるすべての API 操作が含まれます。したがって、`ListInstanceAssociations` と `UpdateInstanceInformation` の両方が一致します。

   サービス名、API メソッド、および IP アドレスについては、値を指定するか、組み込みのフィルターを選択できます。

   [Common API substrings] (一般的な API サブストリング) については、`List`、`Create`、`Delete` などの操作のタイプを表すサブストリングを選択します。各 API メソッド名は、操作タイプで始まります。

   [CIDR patterns] (CIDR パターン) については、パブリック IP アドレス、プライベート IP アドレス、または特定の CIDR パターンに一致する IP アドレスのみを含めるように選択できます。
4. 複数のフィルターがある場合は、ブールオプションを選択して、これらのフィルターの接続方法を設定します。



5. 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。

6. すべてのフィルターをクリアするには、[Clear filter] (フィルターをクリア) を選択します。

アクティビティの詳細の時間範囲の選択

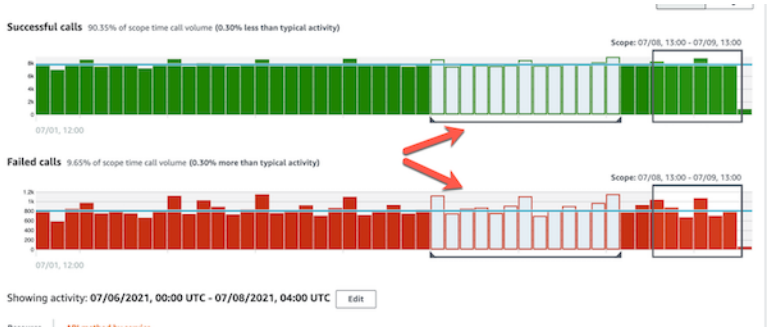
アクティビティの詳細を最初に表示する場合、時間範囲はスコープ時間または選択した時間間隔のいずれかになります。アクティビティの詳細の時間範囲を変更できます。

アクティビティの詳細の時間範囲を変更するには

1. [編集] を選択します。
2. [Edit time window] (時間枠を編集) で、使用する開始時刻と終了時刻を選択します。

   時間枠をプロファイルのデフォルトのスコープ時間に設定するには、[Set to default scope time] (デフォルトのスコープ時間に設定) を選択します。
3. [Update time window] (時間枠を更新) を選択します。

アクティビティの詳細の時間範囲は、プロファイルパネルチャートで強調表示されます。



未処理のログのクエリ

Amazon Security Lake と Amazon Detective の統合により、Security Lake に保存されている未処理のログデータを検索して取得できます。この統合の詳細については、「Amazon Security Lake との統合」を参照してください。

この統合を使用すると、Security Lake がネイティブにサポートしている以下のソースからログとイベントを収集およびクエリできます。

- AWS CloudTrail 管理イベント
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs

> **Note**
>
> Detective で未処理のデータログのクエリを実行する場合、追加料金はかかりません。Amazon Athena AWS を含むその他のサービスの使用料は、引き続き公表されている料金で適用されます。

未処理のログのクエリを実行するには

1. スコープ時間の詳細表示を選択します。
2. ここで、[未処理のログをクエリ] を開始できます。
3. [未処理のログのプレビュー] テーブルでは、Security Lake からのデータのクエリを実行して取得したログとイベントを表示できます。未処理のイベントログの詳細については、Amazon Athena に表示されるデータを確認してください。

   [未処理のログをクエリ] テーブルで、[クエリリクエストをキャンセル]、[Amazon Athena で結果を表示]、[結果をダウンロード] (カンマ区切り値 (.csv) ファイル) を実行できます。

Detective にログが表示されるにもかかわらず、クエリで結果が返されない場合は、次の理由が考えられます。

- 未処理のログは、Security Lake のログテーブルに表示される前に、Detective で利用できるようになる場合があります。後ほどもう一度試してください。」
- Security Lake ログが欠落している可能性があります。長時間待った場合は、Security Lake で ログが欠落していることを示しています。Security Lake 管理者に連絡して、問題を解決してください。

ジオロケーションのアクティビティの詳細

[Newly observed geolocations] (新しく観察されたジオロケーション) のアクティビティの詳細には、スコープ時間中にジオロケーションから発行された API コールが表示されます。API コールには、ジオロケーションから発行されたすべてのコールが含まれます。これらは、検出結果またはプロファイルエンティティを使用したコールに限られません。S3 バケットについては、アクティビティコールは S3 バケットに対して実行される API コールです。

Detective は MaxMind GeoIP データベースを使用してリクエストの場所を特定します。 MaxMind 国や IP の種類などの要因によって精度は異なりますが、国レベルでは非常に高い精度でデータを報告

します。詳細については MaxMind、「MaxMind IP ジオロケーション」を参照してください。GeoIP データのいずれかが正しくないと思われる場合は、「GeoIP2データの修正」MaxMind でMaxmindに修正リクエストを送信できます。

API コールは、コールを発行したサービス別にグループ化されます。S3 バケットについては、サービスは常に Amazon S3 です。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。

アクティビティの詳細を表示するには、以下のいずれかを実行します。

- マップ上で、ジオロケーションを選択します。
- リストで、ジオロケーションの [Details] (詳細) を選択します。

アクティビティの詳細は、ジオロケーションのリストを置き換えます。ジオロケーションのリストに戻るには、[Return to all results] (すべての結果に戻る) を選択します。

なお、Detective は、2021 年 7 月 14 日から API コールのサービス名の保存および表示を開始しました。その日付より前に発生するアクティビティについては、サービス名は [Unknown service] (不明なサービス) となります。

アクティビティの詳細の内容

各タブには、スコープ時間中にジオロケーションから発行されたすべての API コールに関する情報が表示されます。

各 IP アドレス、リソース、および API メソッドについて、リストでは API コールの成功回数と失敗回数が表示されます。

アクティビティの詳細には、次のタブが含まれます。

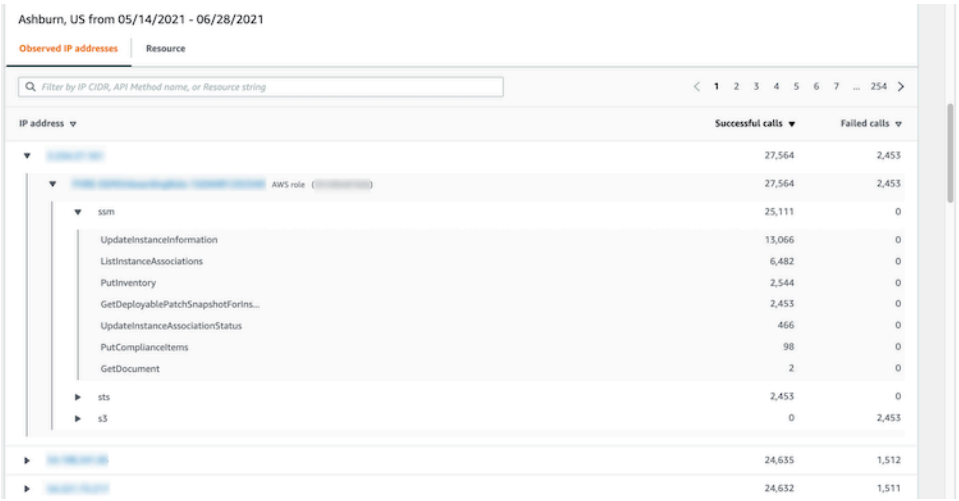
[Observed IP addresses] (観察された IP アドレス)

選択したジオロケーションから API コールを発行するために使用された IP アドレスのリストが最初に表示されます。

各 IP アドレスを展開して、その IP アドレスから API コールを発行したリソースを表示できます。リストには、リソース名が表示されます。プリンシパル ID を表示するには、名前の上にカーソルを合わせます。

その後、各リソースを展開して、その IP アドレスからそのリソースによって発行された特定の API コールを表示できます。API コールは、コールを発行したサービス別にグループ化されま

す。S3 バケットについては、サービスは常に Amazon S3 です。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。

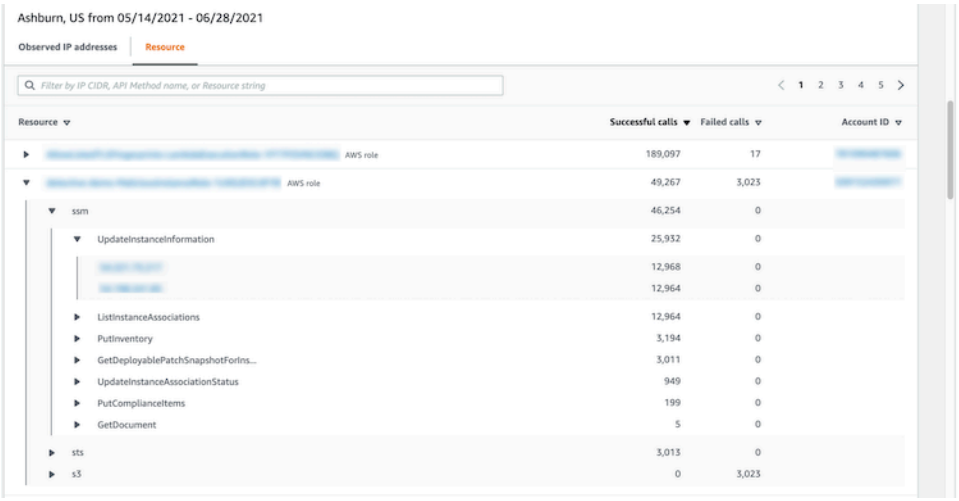


[リソース]

選択したジオロケーションから API コールを発行したリソースのリストが最初に表示されます。リストには、リソース名が表示されます。プリンシパル ID を表示するには、名前の上で一時停止します。各リソースについて、[リソース] タブには関連する AWS アカウントも表示されます。

各ユーザーまたはロールを展開して、そのリソースによって発行された API コールのリストを表示できます。API コールは、コールを発行したサービス別にグループ化されます。S3 バケットについては、サービスは常に Amazon S3 です。Detective がコールを発行したサービスを特定できない場合、そのコールは [Unknown service] (不明なサービス) の下に一覧表示されます。

その後、各 API コールを展開して、リソースが API コールを発行した際の発行元である IP アドレスのリストを表示できます。



アクティビティの詳細のソート

アクティビティの詳細はいずれかのリストの列でソートすることができます。

最初の列を使用してソートすると、最上位のリストのみがソートされます。下位レベルのリストは常に成功した API コールの数でソートされます。

アクティビティの詳細のフィルタリング

フィルタリングオプションを使用して、アクティビティの詳細に表示されるアクティビティの特定のサブセットまたは側面に焦点を当てることができます。

すべてのタブで、最初の列のいずれかの値でリストをフィルタリングできます。

フィルターを追加するには

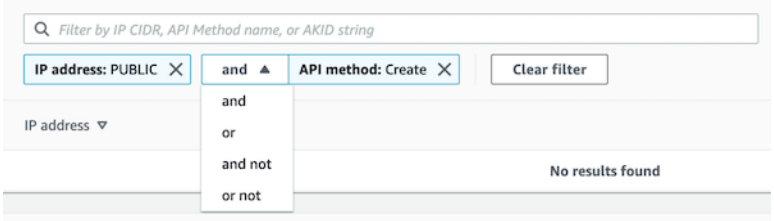
1. フィルターボックスを選択します。
2. [Properties] (プロパティ) から、フィルタリングに使用するプロパティを選択します。
3. フィルタリングに使用する値を入力します。フィルターは部分的な値をサポートします。例えば、API メソッドでフィルタリングする場合、**`Instance`** でフィルタリングすると、結果には名前に `Instance` が含まれるすべての API 操作が含まれます。したがって、`ListInstanceAssociations` と `UpdateInstanceInformation` の両方が一致します。

   サービス名、API メソッド、および IP アドレスについては、値を指定するか、組み込みのフィルターを選択できます。

[Common API substrings] (一般的な API サブストリング) については、`List`、`Create`、`Delete` などの操作のタイプを表すサブストリングを選択します。各 API メソッド名は、操作タイプで始まります。

[CIDR patterns] (CIDR パターン) については、パブリック IP アドレス、プライベート IP アドレス、または特定の CIDR パターンに一致する IP アドレスのみを含めるように選択できます。

4. 複数のフィルターがある場合は、ブールオプションを選択して、これらのフィルターの接続方法を設定します。



5. 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。
6. すべてのフィルターをクリアするには、[Clear filter] (フィルターをクリア) を選択します。

[全体的な VPC フロー量] のアクティビティの詳細

EC2 インスタンスについては、[Overall VPC flow volume] (全体的な VPC のフロー量) のアクティビティの詳細には、選択した時間範囲中の EC2 インスタンスと IP アドレス間のインタラクションが表示されます。

Kubernetes ポッドの場合、[全体的な VPC フロー量] には、すべての送信先 IP アドレスについて、Kubernetes ポッドによって割り当てられた IP アドレスに出入りするバイト総数が表示されます。`hostNetwork:true` の場合、Kubernetes ポッドの IP アドレスは一意ではなくなります。この場合、パネルには、同じ設定を持つ他のポッドへのトラフィックと、それらのポッドをホストしているノードが表示されます。

IP アドレスについては、[Overall VPC flow volume] (全体的な VPC のフロー量) のアクティビティの詳細には、選択した時間範囲中の IP アドレスと EC2 インスタンス間のインタラクションが表示されます。

単一の時間間隔のアクティビティの詳細を表示するには、チャートで時間間隔を選択します。

現在のスコープ時間のアクティビティの詳細を表示するには、[display details for scope time] (スコープ時間の詳細を表示) を選択します。

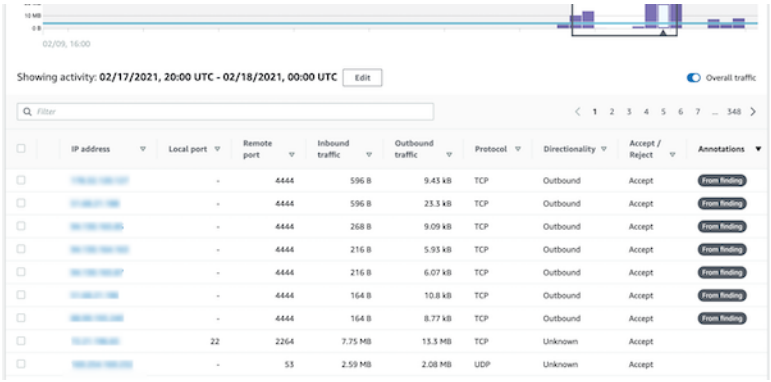
アクティビティの詳細の内容

コンテンツには、選択した時間範囲中のアクティビティが反映されます。

EC2 インスタンスについては、アクティビティの詳細には、IP アドレス、ローカルポート、リモートポート、プロトコル、および方向の一意の各組み合わせのエントリが含まれます。

IP アドレスについては、アクティビティの詳細には、EC2 インスタンス、ローカルポート、リモートポート、プロトコル、および方向の一意の各組み合わせのエントリが含まれます。

各エントリには、インバウンドトラフィックの量、アウトバウンドトラフィックの量、およびアクセスリクエストが受け入れられたか否かが表示されます。検出結果のプロファイルの [Annotations] (注釈) 列を確認することで、IP アドレスが現在の検出結果に関連付けられているかどうかを知ることができます。



アクティビティの詳細のソート

テーブル内の任意の列でアクティビティの詳細をソートすることができます。

デフォルトでは、アクティビティの詳細は注釈でソートされ、次にインバウンドトラフィックでソートされます。

アクティビティの詳細のフィルタリング

特定のアクティビティに焦点を当てるには、次の値でアクティビティの詳細をフィルタリングできます。

- IP アドレスまたは EC2 インスタンス
- ローカルポートまたはリモートポート
- [Direction] (方向)
- [プロトコル]

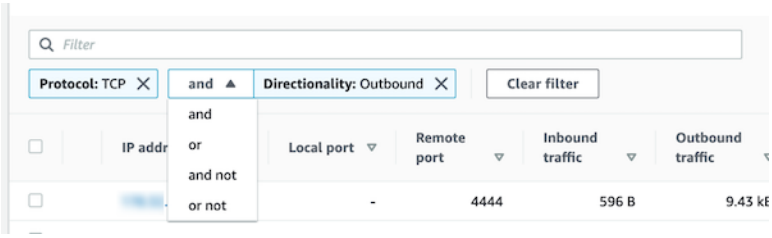
- リクエストが受け入れられたか拒否されたか

フィルターを追加および削除するには

1. フィルターボックスを選択します。
2. [Properties] (プロパティ) から、フィルタリングに使用するプロパティを選択します。
3. フィルタリングに使用する値を入力します。フィルターは部分的な値をサポートします。

   IP アドレスでフィルタリングするには、値を指定するか、組み込みフィルターを選択します。

   [CIDR patterns] (CIDR パターン) については、パブリック IP アドレス、プライベート IP アドレス、または特定の CIDR パターンに一致する IP アドレスのみを含めるように選択できます。
4. 複数のフィルターがある場合は、ブールオプションを選択して、これらのフィルターの接続方法を設定します。



5. 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。
6. すべてのフィルターをクリアするには、[Clear filter] (フィルターをクリア) を選択します。

アクティビティの詳細の時間範囲の選択

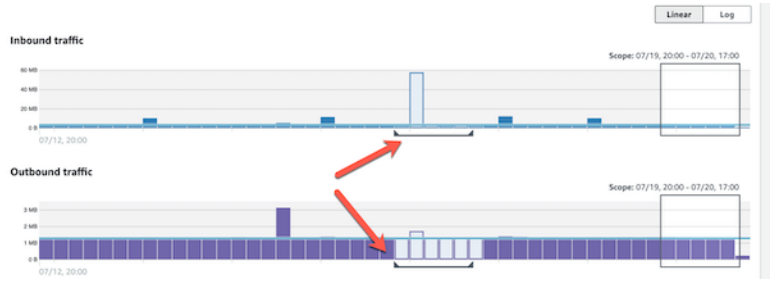
アクティビティの詳細を最初に表示する場合、時間範囲はスコープ時間または選択した時間間隔のいずれかになります。アクティビティの詳細の時間範囲を変更できます。

アクティビティの詳細の時間範囲を変更するには

1. [編集] を選択します。
2. [Edit time window] (時間枠を編集) で、使用する開始時刻と終了時刻を選択します。

   時間枠をプロファイルのデフォルトのスコープ時間に設定するには、[Set to default scope time] (デフォルトのスコープ時間に設定) を選択します。
3. [Update time window] (時間枠を更新) を選択します。

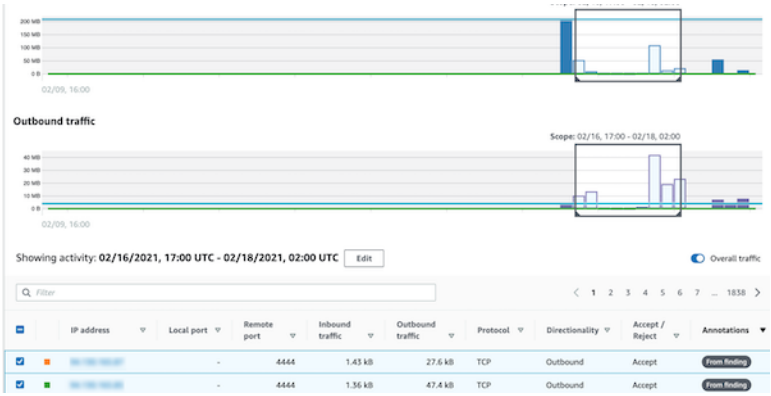
アクティビティの詳細の時間範囲は、プロファイルパネルチャートで強調表示されます。



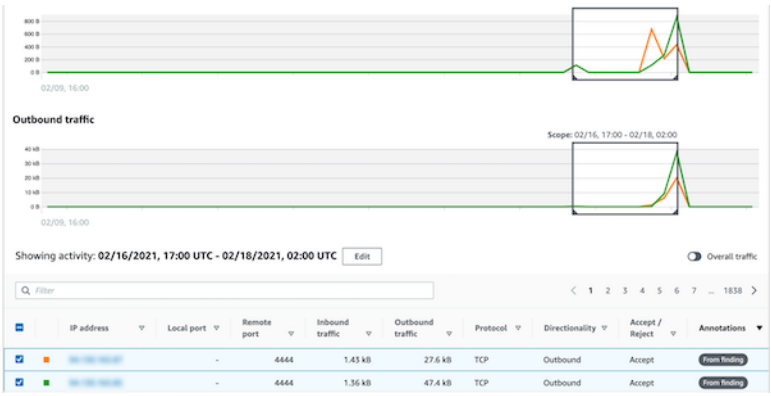
選択した行のトラフィック量の表示

関心のある行を特定すると、主要なグラフで、それらの行のトラフィック量を時間の経過に合わせて表示できます。

グラフに追加する行ごとに、チェックボックスを選択します。選択した各行について、インバウンドチャートまたはアウトバウンドのグラフに量が線で表示されます。



選択したエントリのトラフィック量を重点的に確認するには、全体的な量を非表示にします。全体的なトラフィックを表示したり、非表示にしたりするには、[Overall traffic] (全体的なトラフィック) を切り替えます。



EKS クラスターの VPC フロートラフィックを表示する

Detective は、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターを通過するトラフィックを表す Amazon Virtual Private Cloud (Amazon VPC) フローログを可視化します。Kubernetes リソースの場合、VPC フローログの内容は、EKS クラスターにデプロイされた Container Network Interface (CNI) によって異なります。

デフォルト設定の EKS クラスターは Amazon VPC CNI プラグインを使用します。詳細については、「Amazon EKS ユーザーガイド」の「Working with the Amazon VPC CNI plugin for Kubernetes Amazon EKS add-on」を参照してください。Amazon VPC CNI プラグインは、ポッドの IP アドレスを使用して内部トラフィックを送信し、送信元 IP アドレスを外部通信用ノードの IP アドレスに変換します。Detective は、内部トラフィックをキャプチャして正しいポッドに関連付けることができますが、外部トラフィックについては同じことを行うことはできません。

Detective にポッドの外部トラフィックを可視化させたい場合は、外部送信元ネットワークアドレス変換 (Source Network Address Translation: SNAT) を有効にします。SNAT の有効化には制限と欠点があります。詳細については、「Amazon EKS ユーザーガイド」の「Pods の SNAT」を参照してください。

別の CNI プラグインを使用する場合は、Detective が `hostNetwork:true` 設定のポッドを可視化する際に制限を受けます。これらのポッドの場合、[VPC フロー] パネルにはポッドの IP アドレスの全トラフィックが表示されます。このトラフィックには、ホストノード上の`hostNetwork:true` 設定の全ポッドとホストノード自体のトラフィックが含まれます。

Detective は、 [VPC フロー] パネルに、次の EKS クラスター設定の EKS ポッドのトラフィックを表示します。

- Amazon VPC CNI プラグインを使用するクラスター。このクラスターには、VPC 内でトラフィックを送信する `hostNetwork:false` 設定の任意のポッドも含まれています。
- Amazon VPC CNI プラグインと設定 `AWS_VPC_K8S_CNI_EXTERNALSNAT=true` を使用するクラスターの場合: VPC外でトラフィックを送信する `hostNetwork:false` を持つ任意のポッド。
- `hostNetwork:true` 設定を持つ任意のポッド。本ノードのトラフィックは、`hostNetwork:true` 設定を持つ他のポッドのトラフィックと混在します。

Detective は、以下のトラフィックを [VPC フロー] パネルに表示しません。

- Amazon VPC CNI プラグインと `AWS_VPC_K8S_CNI_EXTERNALSNAT=false` 設定を使用するクラスターの場合: VPC 外でトラフィックを送信する `hostNetwork:false` 設定を持つ任意のポッド。

- Amazon VPC CNI Plugin for Kubernetes を使用していないクラスターの場合: `hostNetwork:false` 設定を持つ任意のポッド。
- 同じノードでホストされている別のポッドにトラフィックを送信する任意のポッド。

共有されている Amazon VPC の VPC フロートラフィックを表示する

Detective は、共有 VPC の Amazon Virtual Private Cloud (Amazon VPC) フローログを可視化します。

- Detective メンバーアカウントに共有 Amazon VPC が含まれており、その共有 VPC を使用している他の非 Detective アカウントがある場合は、Detective はその VPC からのすべてのトラフィックを監視し、VPC 内のすべてのトラフィックフローを視覚化します。
- 共有 Amazon VPC 内に Amazon EC2 インスタンスがあり、共有所有者が Detective メンバーでない場合は、Detective は VPC からのトラフィックをモニタリングしません。VPC 内のトラフィックフローを表示する場合は、Amazon VPC 所有者を Detective グラフのメンバーとして追加する必要があります。

EKS クラスターに関係する全 Kubernetes API アクティビティ

[EKS クラスターを含む Kubernetes API アクティビティ全体] のアクティビティの詳細には、選択した時間範囲に発行された Kubernetes API コール (コール) の成功回数と失敗回数が表示されます。

単一の時間間隔のアクティビティの詳細を表示するには、チャートで時間間隔を選択します。

現在のスコープ時間のアクティビティの詳細を表示するには、[Display details for scope time] (スコープ時間の詳細を表示) を選択します。

アクティビティの詳細の内容 (クラスター、ポッド、ユーザー、ロール、ロールセッション)

クラスター、ポッド、ユーザー、ロール、またはロールセッションについては、アクティビティの詳細には次の情報が含まれます。

- 各タブは、選択した時間範囲中に発行された一連の API コールに関する情報を表示します。

  クラスターの場合、API コールはクラスター内で行われました。

  ポッドの場合、API コールはポッドを対象としていました。

  ユーザー、ロール、ロールセッションの場合、API コールは、そのユーザー、ロール、またはロールセッションとして認証された Kubernetes ユーザーによって発行されました。

- 各エントリについて、アクティビティの詳細では、呼び出しの成功回数、失敗回数、未許可回数、および禁止回数が表示されます。
- 詳細には、IP アドレス、Kubernetes 呼び出しのタイプ、呼び出しの影響を受けたエンティティ、呼び出しを行ったサブジェクト (サービスアカウントまたはユーザー) も含まれます。アクティビティの詳細から、IP アドレス、サブジェクト、および影響を受けるエンティティのプロファイルにピボットできます。

アクティビティの詳細には、次のタブが含まれます。

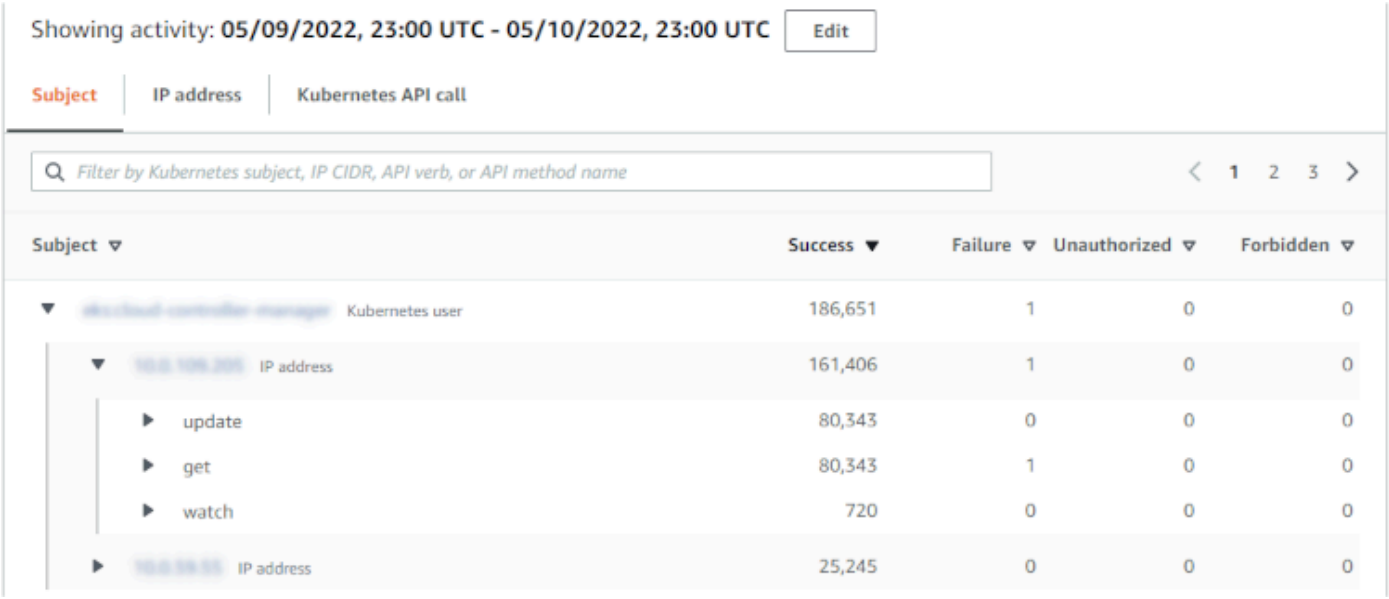
件名

API コールを発行するために使用されたサービスアカウントとユーザーのリストが最初に表示されます。

個々のサービスアカウントとユーザーを展開することで、API コールの発行元となったアカウントまたはユーザーの IP アドレスのリストを表示できます。

次に、各 IP アドレスを展開すると、そのアカウントまたはユーザーがその IP アドレスから行った Kubernetes API コールを表示できます。

Kubernetes API コールを展開すると、実行されたアクションを識別するための`requestURI` が表示されます。



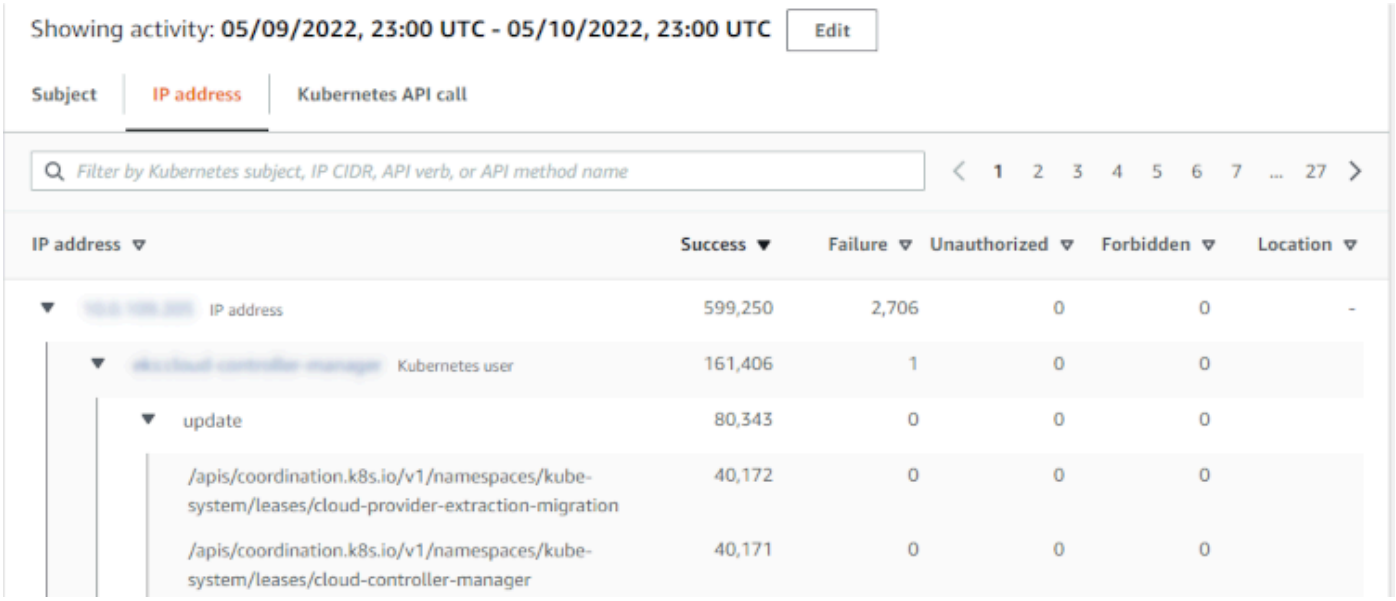
IP アドレス

API コールの発行に使用した IP アドレスのリストが最初に表示されます。

各呼び出しを展開すると、呼び出しを行った Kubernetes サブジェクト (サービスアカウントとユーザー) のリストが表示されます。

次に、各サブジェクトを拡張すると、そのサブジェクトが時間範囲中に実行した API コールのタイプのリストが表示されます。

API コールを展開すると、実行されたアクションを識別するための requestURI が表示されます。



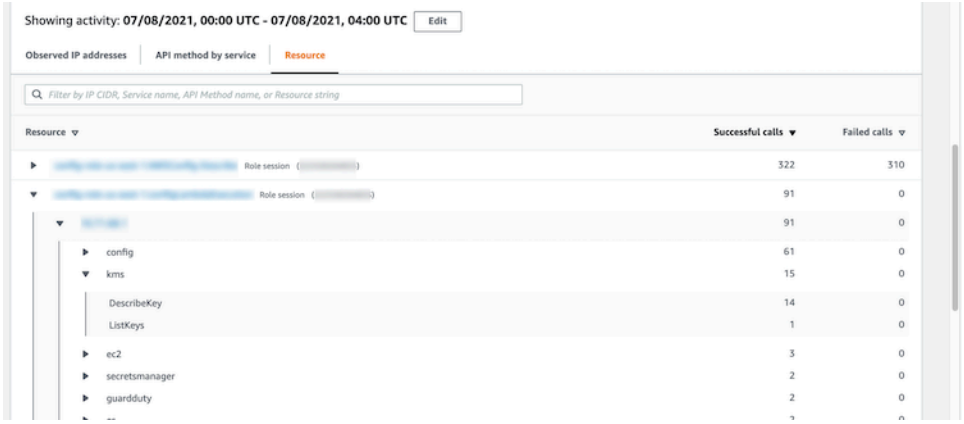
Kubernetes API コール

Kubernetes API コールの動詞のリストが最初に表示されます。

API の各動詞を展開すると、そのアクションに関連付けられた requestURI が表示される。

次に、各 requestURI を展開すると、API コールを行った Kubernetes サブジェクト (サービスアカウントとユーザー) が表示されます。

サブジェクトを展開すると、そのサブジェクトが API コールに使用した IP が表示されます。



アクティビティの詳細のソート

アクティビティの詳細はいずれかのリストの列でソートすることができます。

最初の列を使用してソートすると、最上位のリストのみがソートされます。下位レベルのリストは常に成功した API コールの数でソートされます。

アクティビティの詳細のフィルタリング

フィルタリングオプションを使用して、アクティビティの詳細に表示されるアクティビティの特定のサブセットまたは側面に焦点を当てることができます。

すべてのタブで、最初の列のいずれかの値でリストをフィルタリングできます。

アクティビティの詳細の時間範囲の選択

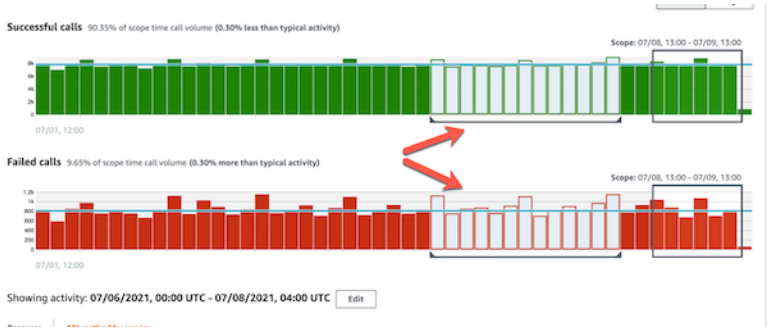
アクティビティの詳細を最初に表示する場合、時間範囲はスコープ時間または選択した時間間隔のいずれかになります。アクティビティの詳細の時間範囲を変更できます。

アクティビティの詳細の時間範囲を変更するには

1. [編集] を選択します。
2. [Edit time window] (時間枠を編集) で、使用する開始時刻と終了時刻を選択します。

   時間枠をプロファイルのデフォルトのスコープ時間に設定するには、[Set to default scope time] (デフォルトのスコープ時間に設定) を選択します。
3. [Update time window] (時間枠を更新) を選択します。

アクティビティの詳細の時間範囲は、プロファイルパネルチャートで強調表示されます。



調査中のプロファイルパネルのガイダンスの使用

各プロファイルパネルは、調査を実施し、関連するエンティティのアクティビティを分析するときに発生する特定の質問に対する回答を提供するように設計されています。

各プロファイルパネルのために提供されるガイダンスは、これらの回答を見つけるのに役立ちます。

プロファイルパネルのガイダンスは、パネル自体に表示される一文から始まります。このガイダンスは、パネルで表示されるデータの簡単な説明を提供します。

パネルに関してより詳細なガイダンスを表示するには、パネルの見出しから [More info] (詳細情報) を選択します。この拡張ガイダンスがヘルプペインに表示されます。

ガイダンスは、次のタイプの情報を提供できます。

- パネルコンテンツの概要
- 関連する質問に回答するためにパネルを使用する方法
- 回答に基づいて推奨される次のステップ

エンティティプロファイルまたは検出結果の概要への直接移動

次のいずれかのオプションを使用して、Amazon Detective のエンティティプロファイルまたは検出結果の概要に直接移動できます。

- Amazon から AWS Security Hub、 GuardDuty または結果から対応する Detective GuardDuty の検索結果プロファイルにピボットできます。
- 検出結果またはエンティティを識別し、使用するスコープ時間を設定する Detective URL をアセンブルできます。

エンティティプロファイルへのピボット、 GuardDuty Amazonからの概要の検索、または AWS Security Hub

Amazon GuardDuty コンソールから、結果に関連するエンティティのエンティティプロファイルに移動できます。

GuardDuty AWS Security Hub およびコンソールから、結果の概要に移動することもできます。検出結果の概要には、関係するエンティティのエンティティプロファイルへのリンクも表示されます。

これらのリンクは、調査プロセスを合理化するのに役立ちます。Detective を迅速に使用して、関連するエンティティのアクティビティを表示したり、次のステップを決定したりできます。その後、検出情報が偽陽性である場合にはその検出結果をアーカイブしたり、さらに調査して問題の範囲を特定したりできます。

Amazon Detective コンソールにピボットする方法

GuardDuty 調査リンクはすべての調査結果で使用できます。 GuardDuty また、エンティティプロファイルに移動するか、結果の概要に移動するかを選択できます。

コンソールから Detective にピボットするには GuardDuty

1. https://console.aws.amazon.com/guardduty/ GuardDuty でコンソールを開きます。
2. 必要に応じて、左側のナビゲーションペインで [Findings] (検出結果) を選択します。
3. [結果] ページで、 GuardDuty 結果を選択します。

   検出結果のリストの右側に検索結果の詳細のペインが表示されます。
4. 検出結果の詳細のペインで、[Investigate in Detective] (Detective で調査) を選択します。

   GuardDuty Detective で調査できるアイテムのリストが表示されます。

   リストには、IP アドレスや EC2 インスタンスなどの関連エンティティと検出結果の両方が含まれます。
5. エンティティまたは検出結果を選択します。

   新しいタブで Detective コンソールが開きます。コンソールが開き、エンティティまたは検出結果プロファイルが表示されます。

   Detective を有効にしていない場合、コンソールが開き、Detective の概要を示すランディングページが表示されます。そこから、Detective を有効にすることができます。

Security Hub コンソールから Detective にピボットするには

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub でコンソールを開きます。
2. 必要に応じて、左側のナビゲーションペインで [Findings] (検出結果) を選択します。
3. Security Hub 結果ページで、 GuardDuty 結果を選択します。
4. 詳細のペインで、[Investigate in Detective] (Detective で調査) を選択してから、[Investigate finding] (検出結果を調査) を選択します。

   [Investigate finding] (検出結果を調査) を選択すると、Detective コンソールが新しいタブで開きます。コンソールが開き、検出結果の概要が表示されます。

Detective コンソールは、集約リージョンからピボットした場合でも、常に検出結果が派生したリージョンに開きます。集計の検索の詳細については、AWS Security Hub ユーザーガイドの Aggregating findings across Regions を参照してください。

Detective を有効にしていない場合、コンソールを開くと Detective のランディングページが表示されます。そこから、Detective を有効にすることができます。

ピボットのトラブルシューティング

ピボットを使用するには、次のいずれかが当てはまる必要があります。

- アカウントは、Detective とピボット元のサービスの両方の管理者アカウントである必要があります。
- 動作グラフへのアクセス権を管理者アカウントに付与するクロスアカウントロールを引き受けました。

管理者アカウントの連携に関する推奨事項の詳細については、「Amazon との推奨連携」GuardDuty および AWS Security Hub「」を参照してください。

ピボットが機能しない場合は、次の点を確認してください。

- 検出結果は、動作グラフで有効になっているメンバーアカウントに属していますか? 関連付けられたアカウントがメンバーアカウントとして動作グラフに招待されていない場合、動作グラフにはそのアカウントのデータは含まれません。

  招待されたメンバーアカウントが招待を承諾しなかった場合、動作グラフにはそのアカウントのデータは含まれません。
- 検出結果はアーカイブされていますか? Detective はからアーカイブされた結果を受信しません。GuardDuty
- 検出結果は、Detective が動作グラフにデータを取り込み始める前に発生したものですか? Detective が取り込むデータに検出結果が存在しない場合、動作グラフにはそのデータが含まれません。
- その検出結果は正しいリージョンからのものですか? 各動作グラフは、リージョンに固有のものです。動作グラフには、他のリージョンのデータは含まれません。

URL を使用したエンティティプロファイルまたは検出結果の概要への移動

Amazon Detective でエンティティプロファイルまたは検出結果の概要に移動するには、そのプロファイルへの直接リンクを提供する URL を使用できます。URL は、検出結果またはエンティティを識別します。また、プロファイルで使用するスコープ時間を指定することもできます。Detective は、最長 1 年間の履歴イベントデータを保持します。

プロファイル URL の形式

> **Note**
>
> 古い形式の URL を使用した場合でも、Detective によって新しい URL に自動的にリダイレクトされます。古い形式の URL は次のとおりです。
> https://console.aws.amazon.com/detective/home?region=*Region*#*type*/*namespace*/*instanceID*?*parameters*

新しい形式のプロファイル URL は次のとおりです。

- エンティティの場合 - https://console.aws.amazon.com/detective/home?region=*Region*#*entities*/*namespace*/*instanceID*?*parameters*
- 検出結果の場合 - https://console.aws.amazon.com/detective/home?region=*Region*#*findings*/*instanceID*?*parameters*

URL には、次の値が必要です。

Region

使用するリージョン。

type

ナビゲート先のプロファイルの項目のタイプ。

- `entities` - エンティティプロファイルに移動していることを示します
- `findings` - 検出結果の概要に移動していることを示します

####

エンティティについては、名前空間はエンティティタイプの名前です。

- `AwsAccount`

- AwsRole
- AwsRoleSession
- AwsUser
- Ec2Instance
- FederatedUser
- IpAddress
- S3Bucket
- UserAgent
- FindingGroup
- KubernetesSubject
- ContainerPod
- ContainerCluster
- ContainerImage

instanceID

検出結果またはエンティティのインスタンス識別子。

- 結果の場合、 GuardDuty GuardDuty 検出結果の識別子。
- AWS アカウントの場合、アカウント ID。
- AWS ロールとユーザーの場合、ロールまたはユーザーのプリンシパル ID。
- フェデレーティッドユーザーについては、フェデレーティッドユーザーのプリンシパル ID です。プリンシパル ID は *<identityProvider>*:*<username>* または *<identityProvider>*:*<audience>*:*<username>* のいずれかです。
- IP アドレスについては、IP アドレスです。
- ユーザーエージェントについては、ユーザーエージェント名。
- EC2 インスタンスについては、インスタンス ID です。
- ロールセッションについては、セッション識別子です。セッション識別子は、*<rolePrincipalID>*:*<sessionName>* の形式を使用します。
- S3 バケットについては、バケット名です。
- UUID の場合。たとえば FindingGroups、ca6104bc-a315-4b15-bf88-1c1e60998f83
- EKS リソースの場合: 次の形式を使用します。
  - EKS クラスター: *<clusterName>~<accountId>~EKS*
  - Kubernetes ポッド: *<podUid>~<clusterName><accountId>~EKS*

- Kubernetes サブジェクト: *<subjectName>~<clusterName>~<accountId>*
- コンテナイメージ: *<registry>/<repository>:<tag>@<digest>*

検出結果またはエンティティは、動作グラフで有効になっているアカウントに関連付けられている必要があります。

URL には、スコープ時間を設定するために使用される次のオプションのパラメータを含めることもできます。スコープ時間とプロファイルでのその使用方法の詳細については、the section called “スコープ時間の管理” を参照してください。

`scopeStart`

プロファイルで使用するスコープ時間の開始時刻。開始日時は過去 365 日以内の日時である必要があります。

値はエポックタイムスタンプです。

開始時刻を指定したが、終了時刻を指定しない場合、スコープ時間は現在の時刻で終了します。

`scopeEnd`

プロファイルで使用するスコープ時間の終了時刻。

値はエポックタイムスタンプです。

終了時刻を指定したが、開始時刻を指定しない場合、スコープ時間には終了時刻より前のすべての時間が含まれます。

スコープ時間を指定しない場合は、デフォルトのスコープ時間が使用されます。

- 検出結果については、デフォルトのスコープ時間は、検出結果のアクティビティが観察された最初の時刻と最後の時刻を使用します。
- エンティティについては、デフォルトのスコープ時間は直近 24 時間です。

Detective の URL の例を次に示します。

```
https://console.aws.amazon.com/detective/home?region=us-east-1#entities/
IpAddress/192.168.1.1?scopeStart=1552867200&scopeEnd=1552910400
```

この URL の例では、次の手順について説明します。

- IP アドレス 192.168.1 のエンティティプロファイルを表示します。
- 2019 年 3 月 18 日 (月) 午前 0 時 (GMT) に開始し、2019 年 3 月 18 日 (月) 正午 (GMT) に終了するスコープ時間を使用します。

URL のトラブルシューティング

URL が想定されるプロファイルを表示しない場合は、まず URL が正しい形式を使用していること、および正しい値を入力したことを確認します。

- URL の前半に正しい `findings` または `entities` を指定しましたか?
- 正しい名前空間を指定しましたか?
- 正しい識別子を入力しましたか?

値が正しい場合は、以下を確認することもできます。

- 検出結果またはエンティティは、動作グラフで有効になっているメンバーアカウントに属していますか? 関連付けられたアカウントがメンバーアカウントとして動作グラフに招待されていない場合、動作グラフにはそのアカウントのデータは含まれません。

  招待されたメンバーアカウントが招待を承諾しなかった場合、動作グラフにはそのアカウントのデータは含まれません。
- 検出結果については、その検出結果はアーカイブされていますか? Detective は Amazon からアーカイブされた調査結果を受け取りません。 GuardDuty
- 検出結果またはエンティティは、Detective が動作グラフにデータを取り込み始める前に発生したものですか? Detective が取り込むデータに検出結果またはエンティティが存在しない場合、動作グラフにはそのデータが含まれません。
- その検出結果またはエンティティは正しいリージョンからのものですか? 各動作グラフは、リージョンに固有のものです。動作グラフには、他のリージョンのデータは含まれません。

Splunk に対する検出結果の Detective URL の追加

Splunk Trumpet プロジェクトでは、サービスから Splunk にデータを送信できます。 AWS

Trumpet プロジェクトを設定して、Amazon の調査結果のDetective URL を生成できます。 GuardDuty その後、これらの URL を使用して、対応する Detective 検出結果プロファイルに Splunk から直接ピボットできます。

Trumpet プロジェクトは https://github.com/splunk/ から入手できます。 GitHub splunk-aws-project-trumpet

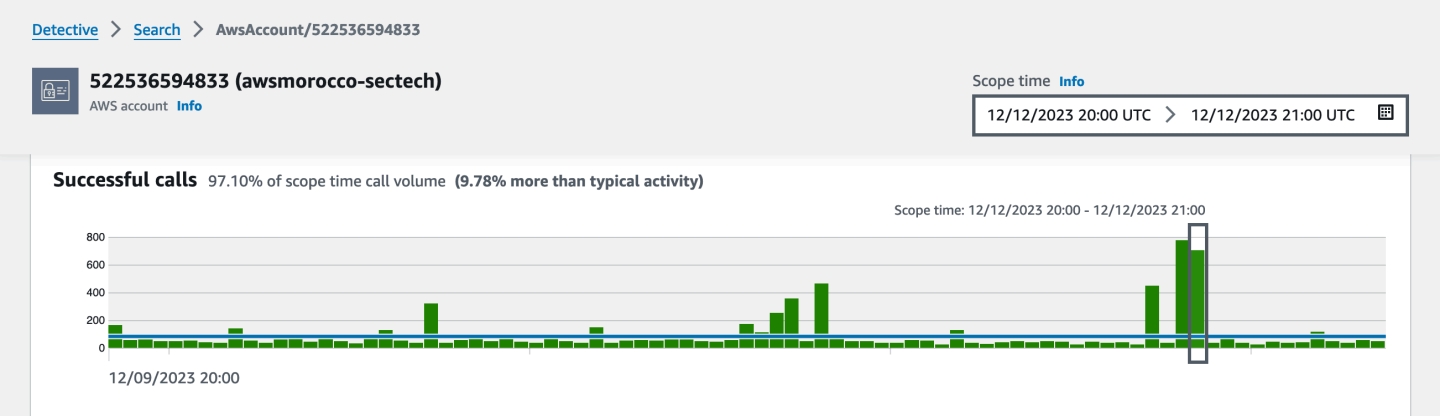
Trumpet プロジェクトの設定ページで、「AWS CloudWatch イベント」から「 GuardDuty Detective URL」を選択します。

プロファイル内の移動

エンティティプロファイルには、1 つ以上のタブセットが含まれています。各タブには、1 つまたは複数のプロファイルパネルが含まれています。各プロファイルパネルには、動作グラフのデータから生成されたテキストとビジュアライゼーションが含まれています。

プロファイルタブを下方向にスクロールしても、次の情報はプロファイルの上部に表示されたままとなります。

- エンティティタイプ
- エンティティ識別子
- スコープ時間



スコープ時間の管理

エンティティプロファイルに表示されるデータを制限するために使用されるスコープ時間をカスタマイズします。

エンティティプロファイルに表示されるグラフ、タイムライン、および他のデータはすべて、現在の時間範囲に基づいています。時間範囲は、エンティティの全アクティビティを実行した時間の範囲

です。これは Amazon Detective コンソールの各プロファイルの右上に表示されます。これらのグラフ、タイムライン、および他のビジュアライゼーションに表示されるデータは、スコープ時間に基づいています。一部のプロファイルパネルについては、コンテキストを提供するためにスコープ時間の前後の時間が追加されます。Detective では、すべてのタイムスタンプはデフォルトで UTC で表示されます。ローカルタイムゾーンを選択するには、[タイムスタンプの設定] の値を変更します。[タイムスタンプの設定] を更新する方法については、「the section called “タイムスタンプ形式を設定する”」を参照してください。

Detective の分析では、時間範囲を使用して、異常なアクティビティがないかをチェックします。分析プロセスは、スコープ時間中のアクティビティを取得し、それをスコープ時間前の 45 日間のアクティビティと比較します。また、その 45 日間の時間枠を使用して、アクティビティのベースラインを生成します。

検出結果の概要では、スコープ時間は検出結果が最初と最後に観察された時刻を反映します。検出結果の概要についての詳細は、「the section called “検出結果の概要”」を参照してください。

調査を進める過程で、範囲時間を調整できます。例えば、元の分析が 1 日のアクティビティに基づいている場合、それを 1 週間または 1 か月に拡張することができます。期間を延長することで、アクティビティが通常のパターンに適合しているか、異常であるかをより良く理解するのに役立つことがあります。

現在のエンティティに関連する検出結果と一致するようにスコープ時間を設定することもできます。

スコープ時間を変更すると、Detective は分析を繰り返し、新しいスコープ時間に基づいて表示されたデータを更新します。

時間範囲は、1 時間より短くしたり、1 年より長くしたりすることはできません。開始時刻と終了時刻は、時間の単位で設定する必要があります。

特定の開始日時と終了日時の設定

Detective コンソールからスコープ時間の開始日と終了日を設定できます。

新しいスコープ時間について特定の開始時刻と終了時刻を設定するには

1. https://console.aws.amazon.com/detective/ で Amazon Detective コンソールを開きます。
2. エンティティプロファイルで、スコープ時間を選択します。
3. [Edit scope time] (スコープ時間を編集) パネルの [Start] (開始) で、スコープ時間の新しい開始日時を選択します。新しい開始時刻については、時間のみを選択します。

4. [End] (終了) で、スコープ時間の新しい終了日時を選択します。新しい終了時刻については、時間のみを選択します。終了時刻は、開始時刻より 1 時間以上後である必要があります。
5. 編集が終了したら、変更を保存して表示されたデータを更新するには、[Update scope time] (スコープ時間を更新) を選択します。

時間範囲の長さを編集する

スコープ時間の長さを設定すると、Detective は、現在の時刻を開始時刻として、その長さの時間をスコープ時間として設定します。

時間範囲の長さを編集するには

1. https://console.aws.amazon.com/detective/ で Amazon Detective コンソールを開きます。
2. エンティティプロファイルで、スコープ時間を選択します。
3. [Edit scope time] (スコープ時間を編集) パネルの [Historical] (履歴) の横で、スコープ時間の時間の長さを選択します。

   時間範囲を指定すると、[Start] (開始) および [End] (終了) の設定が更新されます。
4. 編集が終了したら、変更を保存して表示されたデータを更新するには、[Update scope time] (スコープ時間を更新) を選択します。

スコープ時間の検出結果の時間枠としての設定

各検出結果には時間枠が関連付けられています。これは、検出結果が観察された最初と最後の時刻を反映するものです。検出結果の概要を表示すると、時間範囲が検出結果の時間枠に変わります。

エンティティプロファイルから、スコープ時間を関連する検出結果の時間枠に合わせて調整できます。これにより、その時間に発生したアクティビティを調査できます。

スコープ時間を検出結果の時間枠に合わせて調整するには、[Associated findings] (関連する検出結果) パネルで、使用する検出結果を選択します。

Detective は、検出結果の詳細情報を入力し、スコープ時間を検出結果の時間枠に設定します。

概要ページでの時間範囲の設定

[概要] ページを確認しながら、過去 365 日間の任意の 24 時間枠のアクティビティを表示する [時間範囲] の値を調整できます。

概要ページで時間範囲を設定するには

1. https://console.aws.amazon.com/detective/ で Amazon 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 [概要] を選択します。
3. [概要] の横にある [時間範囲] パネルで、[開始日時] の値を変更できます。開始日時は過去 365 日以内の日時である必要があります。

   [開始日時] を変更すると、[終了日時] が、選択した開始時刻から 24 時間後の日時に自動的に更新されます。

   > **Note**
   >
   > Detective を使用すると、最長 1 年間の履歴イベントデータにアクセスできるようになりました。Detective のソースデータについて詳しくは、「動作グラフで使用されるソースデータ」を参照してください。

4. 編集が終了したら、変更を保存して表示されたデータを更新するには、[Update scope time] (スコープ時間を更新) を選択します。

関連する検出結果の詳細の表示

各エンティティプロファイルには、関連する検出結果のパネルが含まれています。このパネルは、現在のスコープ時間中にエンティティが関係した検出結果を一覧表示します。エンティティが侵害されたことを示す兆候の 1 つに、そのエンティティが複数の検出結果に関係していることが挙げられます。検出結果のタイプは、関心のあるアクティビティのタイプについてのインサイトを提供することもできます。

関連付けられた検出結果のパネルは、エンティティの詳細のプロファイルパネルのすぐ下に表示されます。

この表には、各検出結果について以下の情報が含まれています。

- 検出結果のタイトル。検出結果の概要へのリンクでもあります。
- AWS 結果に関連するアカウント。アカウントプロファイルへのリンクでもあります
- 検出結果のタイプ
- 最初に検出結果が観察された時刻
- 最後に検出結果が観察された時刻

- 検出結果の重要度

ある検出結果について、検出結果の詳細を表示するには、その検出結果のラジオボタンを選択します。Detective は、ページの右側にある検出結果の詳細パネルにデータを自動的に入力します。また、Detective は、スコープ時間を検出結果の時間枠に変更します。これにより、その時間内に発生したアクティビティに注力できます。

検出結果の概要からエンティティプロファイルに移動した場合、その検出結果が自動的に選択され、その検出結果の詳細が表示されます。

検出結果の詳細から検出結果の概要に戻るには、[See all related entities] (関連するすべてのエンティティを表示) を選択します。

検出結果をアーカイブすることもできます。「the section called “調査結果をアーカイブする GuardDuty ”」を参照してください。

大量のエンティティの詳細の表示

[behavior graph] (動作グラフ) で、Amazon Detective はエンティティ間の関係を追跡します。たとえば、各動作グラフは、 AWS AWS ユーザーがいつロールを作成するか、EC2 インスタンスがいつIP アドレスに接続するかを追跡します。

ある期間中にエンティティの関係が過多である場合、Detective はすべての関係を保存できません。これが現在のスコープ時間中に発生すると、Detective はその旨を通知します。Detective は、大量のエンティティの発生リストも提供します。

大量のエンティティとは

特定の時間間隔において、エンティティは、非常に多数の接続の発信元または発信先になる場合があります。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。

Detective は、各時間間隔で対応できる接続数の制限を維持しています。エンティティがその制限を超えると、Detective はその時間間隔の接続を破棄します。

例えば、制限が時間間隔あたり 100,000,000 接続であると仮定します。EC2 インスタンスが 1 つの時間間隔で 100,000,000 を超える IP アドレスによって接続されている場合、Detective はその時間間隔からの接続を破棄します。

ただし、関係のもう一方の端にあるエンティティに基づいて、そのアクティビティを分析できる場合があります。この例を続行するため、EC2 インスタンスは数百万の IP アドレスによって接続されて

いる場合がありますが、単一の IP アドレスははるかに少ない EC2 インスタンスに接続されます。各 IP アドレスのプロファイルは、IP アドレスの接続先である EC2 インスタンスに関する詳細を提供します。

プロファイルにおける大量のエンティティ通知の表示

エンティティが大量である時間間隔がスコープ時間に含まれている場合、Detective は、検出結果またはエンティティプロファイルの先頭に通知を表示します。検出結果プロファイルについては、この通知は関係するエンティティに関するものです。

この通知には、大量の時間間隔を持つ関係のリストが含まれます。各リストエントリには、関係の説明と、大量の時間間隔の開始が含まれます。

大量の時間間隔は、疑わしいアクティビティを示唆している可能性があります。同時に発生した他のアクティビティを理解するために、大量の時間間隔を重点的に調査できます。大量のエンティティ通知には、スコープ時間をその時間間隔に設定するオプションが含まれています。

スコープ時間を大量の時間間隔に設定するには

1. 大量のエンティティ通知で、時間間隔を選択します。
2. ポップアップメニューで、[Apply scope time] (スコープ時間を適用) を選択します。

現在のスコープ時間についての大量エンティティのリストの表示

[High-volume entities] (大量のエンティティ) ページには、現在のスコープ時間中の大量の時間間隔とエンティティのリストが含まれています。

[High-volume entities] (大量のエンティティ) ページを表示するには

1. https://console.aws.amazon.com/detective/ で Amazon Detective コンソールを開きます。
2. Detective ナビゲーションペインで、[High-volume entities] (大量のエンティティ) を選択します。

リストの各エントリには、次の情報が含まれています。

- 大量の時間間隔の開始
- エンティティの識別子とタイプ
- 関係の説明 (「IP アドレスから接続された EC2 インスタンス」など)

任意の列でリストをフィルタリングしたり、ソートしたりできます。関係するエンティティのエンティティプロファイルに移動することもできます。

エンティティのプロファイルに移動するには

1. [High-volume entities] (大量のエンティティ) リストで、移動元の行を選択します。
2. [View profile with high-volume scope time] (大量のスコープ時間でプロファイルを表示) を選択します。

このオプションを使用してエンティティプロファイルに移動すると、スコープ時間は次のように設定されます。

- スコープ時間は、大量の時間間隔の 30 日前に開始されます。
- スコープ時間は、大量の時間間隔の終了時に終了します。

調査結果とエンティティの管理

Amazon Detective には、結果の検索、エクスポート、管理に役立つ重要な機能がいくつか用意されています。これらの機能は、調査結果を特定の環境に合わせて調整したり、価値の低い結果から生じるノイズを減らしたり、 AWS 独自の環境に対する脅威に焦点を当てたりするのに役立ちます。このページのトピックを確認して、これらの機能を使用して Detective の調査結果の価値を高める方法を理解してください。

コンテンツ

検出結果またはエンティティの検索

Amazon Detective の検索機能を使用すると、検出結果またはエンティティを検索できます。検索結果から、エンティティプロファイルまたは検出結果の概要に移動できます。検索で 10,000 件を超える結果が返された場合、上位 10,000 件の結果のみが表示されます。ソート順を変更すると、返される結果も変わります。

検索結果をカンマ区切り値 (CSV) ファイルにエクスポートすることができます。このファイルには、検索ページに返されたデータが含まれます。詳細については、「the section called “Detective からのデータのエクスポート”」を参照してください。

検索の完了

検索を完了するには、検索するエンティティのタイプを選択します。次に、正確な識別子、またはワイルドカード文字 * または ? を含む識別子を指定します。IP アドレスの範囲を検索するには、CIDR またはドット表記を使用することもできます。次の検索文字列の例を参照してください。

IP アドレスの例:

- `1.0.*.*`
- `1.0.133.*`
- `1.0.0.0/16`
- `0.239.48.198/31`

他のタイプのエンティティの例:

- `Admin`
- `ad*`
- `ad*n`
- `ad*n*`
- `adm?n`
- `a?m*`
- `*min`

すべてのエンティティタイプについて、次の識別子がサポートされています。

- 検出結果については、検出結果の識別子または検出結果の Amazon リソースネーム (ARN)。
- AWS アカウントの場合、アカウント ID。
- AWS AWS ロールとユーザーの場合は、プリンシパル ID、名前、または ARN のいずれか。
- コンテナクラスターについては、クラスター名または ARN。
- コンテナイメージについては、コンテナイメージのリポジトリまたは完全ダイジェスト。
- コンテナポッドまたはタスクについては、ポッドの名前、またはポッドの UID。
- EC2 インスタンスについては、インスタンス識別子または ARN。
- 検出結果グループについては、検出結果グループの識別子。
- IP アドレス、については、CIDR 表記またはドット表記でのアドレス。
- Kubernetes サブジェクト (サービスアカウントまたはユーザー) については、名前。
- ロールセッションについては、次のいずれかの値を使用して検索できます。
  - ロールセッション識別子。

    ロールセッション識別子は、*<rolePrincipalID>*:*<sessionName>* の形式を使用します。

    例: `AROA12345678910111213:MySession`。
  - ロールセッション ARN
  - セッション名
  - 引き受けたロールのプリンシパル ID
  - 引き受けたロールの名前
- S3 バケットについては、バケット名またはバケット ARN。

- フェデレーティッドユーザーについては、プリンシパル ID またはユーザー名。プリンシパル ID は *<identityProvider>*:*<username>* または *<identityProvider>*:*<audience>*:*<username>* のいずれかです。
- ユーザーエージェントについては、ユーザーエージェント名。

検出結果またはエンティティを検索するには

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. ナビゲーションペインで、[検索] を選択します。
3. [タイプを選択] メニューから、探している項目のタイプを選択します。

   [User] (ユーザー) を選択すると、 AWS ユーザーまたはフェデレーティッドユーザーのいずれかを検索できることに注意してください。

   [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。例のいずれかのプロファイルを表示するには、その識別子を選択します。
4. 検索する識別子を、そのとおりに入力するか、またはワイルドカード文字を使って入力します。

   検索では大文字と小文字は区別されません。
5. [Search] (検索) を選択するか、Enter キーを押します。

検索結果の使用

検索を完了すると、Detective は最大 10,000 件の一致する結果のリストを表示します。一意の識別子を使用する検索では、一致する結果は 1 つのみとなります。

結果から、エンティティプロファイルまたは検出結果の概要に移動するには、識別子を選択します。

検出結果、ロール、ユーザー、および EC2 インスタンスについては、関連するアカウントが検索結果に含まれます。アカウントのプロファイルに移動するには、アカウントの識別子を選択します。

検索のトラブルシューティング

Detective で検出結果またはエンティティが見つからない場合は、まず正しい識別子が入力されていることを確認してください。識別子が正しければ、次の事項も確認してください。

- 検出結果またはエンティティは、動作グラフで有効になっているメンバーアカウントに属していますか? 関連付けられたアカウントがメンバーアカウントとして動作グラフに招待されていない場合、動作グラフにはそのアカウントのデータは含まれません。

  招待されたメンバーアカウントが招待を承諾しなかった場合、動作グラフにはそのアカウントのデータは含まれません。
- 検出結果については、その検出結果はアーカイブされていますか? Detective は Amazon からアーカイブされた調査結果を受け取りません。 GuardDuty
- 検出結果またはエンティティは、Detective が動作グラフにデータを取り込み始める前に発生したものですか? Detective が取り込むデータに検出結果またはエンティティが存在しない場合、動作グラフにはそのデータが含まれません。
- その検出結果またはエンティティは正しいリージョンからのものですか? 各動作グラフはに固有のものです。 AWS リージョン動作グラフには、他のリージョンのデータは含まれません。

Detective からのデータのエクスポート

Amazon Detective の [概要] ページと検索結果ページからデータをエクスポートできます。データは、カンマ区切り値 (CSV) 形式でエクスポートされます。エクスポートされたデータのファイル名は `detective-page-panel-yyyy-mm-dd.csv` の形式パターンを取ります。CSV インポートをサポートする他の AWS サービス、サードパーティアプリケーション、またはスプレッドシートプログラムを使用してデータを操作することで、セキュリティ調査を強化できます。

> **Note**
>
> エクスポートが現在進行中の場合、追加のデータをエクスポートするときは、進行中のエクスポートが完了するまで待ってください。

データを含むカンマ区切り値 (CSV) ファイルをエクスポートするには、Detective の以下のパネルとページを使用します。

- [概要] ページ
  - [API コール量が最も多いロールとユーザー] パネル
  - [トラフィック量が最も多い EC2 インスタンス] パネル
  - [Kubernetes ポッドの作成数が最も多い EKS クラスター] パネル

- [検索します] ページ — 検索で 10,000 件を超える結果が返された場合、上位 10,000 件の結果のみがエクスポートされます。ソート順を変更すると、返される結果も変わります。

Amazon GuardDuty の検索結果をアーカイブする

Amazon で検出された結果の調査が完了したら、Amazon GuardDuty Detective からの結果をアーカイブできます。これにより、 GuardDuty に戻って更新を行う手間が省けます。検出結果のアーカイブは、調査が完了したことを示唆するものです。

GuardDuty GuardDuty検出結果に関連付けられているアカウントの管理者アカウントでもある場合にのみ、Detective 内から結果をアーカイブできます。 GuardDuty管理者アカウントではない状態で結果をアーカイブしようとすると、 GuardDuty エラーが表示されます。

GuardDuty 結果をアーカイブするには

1. Detective コンソールの検出結果の詳細のパネルで、[Archive finding] (検出結果をアーカイブ) を選択します。
2. 確認を求められたら、[Archive] (アーカイブ) を選択します。

GuardDuty GuardDuty アーカイブされた結果はコンソールで表示できます。詳細については、Amazon GuardDuty ユーザーガイドの「抑制ルール」を参照してください。

アカウントの管理

各動作グラフには、1 つ以上のアカウントのデータが含まれています。アカウントが 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を選択できます。動作グラフには、最大 1,200 個のメンバーアカウントを含めることができます。

と統合されている場合 AWS Organizations、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。その Detective 管理者アカウントが、組織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、組織動作グラフのメンバーアカウントとして任意の組織アカウントを有効にすることができます。組織アカウントは、自身を組織動作グラフから削除することはできません。

また、管理者アカウントは、動作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受け入れると、Detective はその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、動作グラフから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 はそのメンバーアカウントのデータを動作グラフに取り込み、抽出するようになります。

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。行動グラフで各アカウントのデータ量を追跡する方法については、「Amazon Detective コストの予測と監視」を参照してください。

コンテンツ

Detective でのアカウントに関する制約と推奨事項

Amazon Detective でアカウントを管理する場合、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最大数

Detective は、動作グラフごとに最大 1,200 個のメンバーアカウントを受け入れます。

アカウントとリージョン

AWS Organizations を使用してアカウントを管理する場合、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になります。組織管理アカウントは、各リージョンの Detective 管理者アカウントを個別に指定することもできます。また、Detective 管理者アカウントは、各リージョンの組織動作グラフとメンバーアカウントを個別に管理できます。

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 1 つのリージョンでのみ作成されます。管理者アカウントはリージョンごとに Detective を有効にする必要があり、リージョンごとに個別の動作グラフを持ちます。次に、管理者アカウントは各アカウントを招待し、そのリージョンのメンバーアカウントとして関連付けます。

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 との連携、 GuardDuty

AWS Security Hub と Amazon GuardDuty との統合をスムーズに行うために、これらすべてのサービスで同じアカウントを管理者アカウントにすることをお勧めします。

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

必要なアクセス許可を管理者アカウントに付与する

動作グラフを管理するために必要なアクセス許可を管理者アカウントに確実に付与するには、IAM プリンシパルに `AmazonDetectiveFullAccess` マネージドポリシーをアタッチします。

組織のアップデートを Detective に反映する

組織に変更を加えても、Detective にはすぐには反映されません。

組織アカウントの新規作成や削除など、変更のほとんどは、Detective に通知されるまでに最大 1 時間かかることがあります。

Organizations 内の指定の Detective 管理者アカウントへの変更は、反映されるまでの時間が短くなります。

Organizations を使用した動作グラフアカウント管理への移行

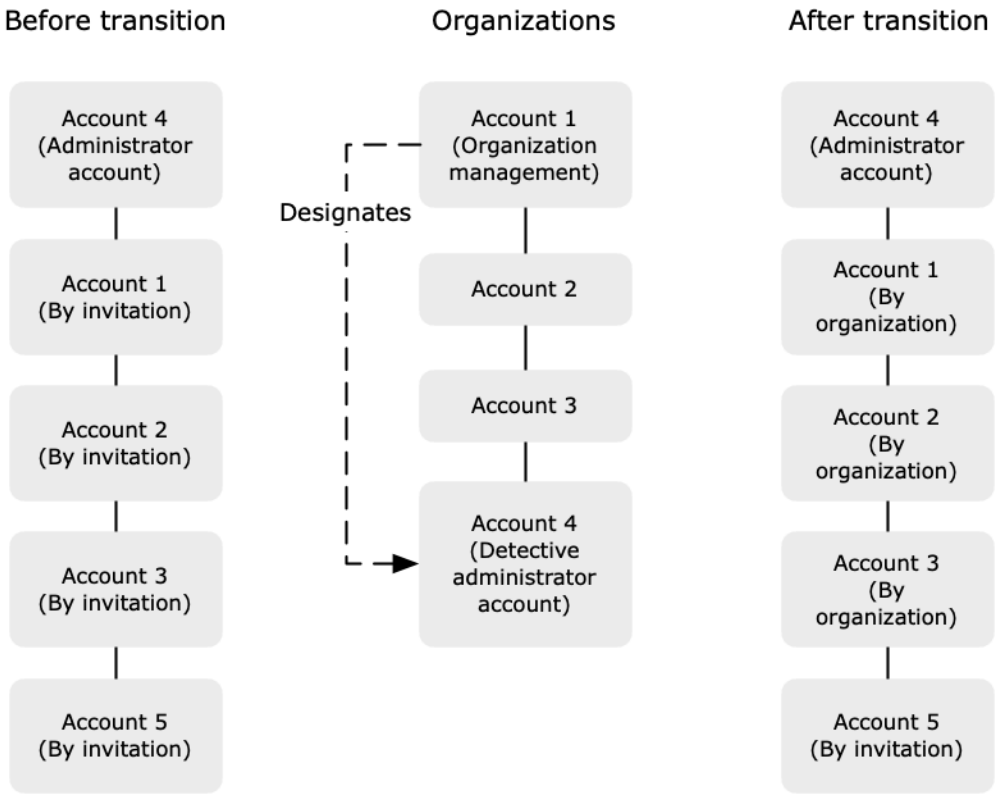
手動の招待を承諾したメンバーアカウントを持つ既存の動作グラフが存在している可能性があります。に登録している場合は、手動で招待する代わりに AWS Organizations、次の手順に従って Organizations を使用してメンバーアカウントを有効化および管理してください。

1. 組織の Detective 管理者アカウントを指定します。これにより、組織動作グラフが作成されます。

   Detective 管理者アカウントが既に動作グラフを持っている場合、その動作グラフは組織動作グラフになります。
2. 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します。

   組織動作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。

次の図表は、移行前の動作グラフの構造、Organizations 内の設定、および移行後の動作グラフのアカウント構造について、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で、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" を参照してください。

移行を簡単にするために、Detective では、現在の管理者アカウントを組織の Detective 管理者アカウントとして選択することを推奨しています。

Organizations に Detective の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組織管理者アカウントを Detective の管理者アカウントとして使用する必要があります。

そうしないと、初めて組織管理アカウントではない Detective 管理者アカウントを指定したとき、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指定します。

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、組織動作グラフの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" を参照してください。

Detective 管理者アカウントは、[アカウント] ページで組織内のすべてのアカウントを表示することができます。

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る場合、その動作グラフは組織動作グラフになります。その動作グラフのメンバーアカウントに既になっている組織アカウントは、自動的にメンバーアカウントとして有効になります。それ以外の組織アカウントのステータスは [メンバーではありません] です。

組織アカウントのタイプは、以前は招待によるメンバーアカウントだった場合でも、[By organization] (組織別) になります。

組織に所属していないメンバーアカウントのタイプは、[招待による] になります。

また、[アカウント管理] ページの [新しい組織アカウントを自動的に有効にする] というオプションは、アカウントが組織に追加された時点で自動的に有効化されるように設定できます。the section called “新しい組織アカウントを自動的に有効にする” 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 [アカウント管理] ページを表示すると、メッセージと一緒に [すべての組織アカウントを有効化] ボタンが表示されます。[すべての組織アカウントを有効化] を選択すると、Detective は次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。

メンバーアカウントリストには、[すべての組織アカウントを有効化] オプションも表示されます。

組織の Detective 管理者アカウントの指定

組織動作グラフでは、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、それぞれの組織のDetective 管理者アカウントを指定します。 AWS リージョン

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、Detective の委任管理者アカウントにもなります。 AWS Organizations例外は、組織管理アカウントが自らを Detective 管理者アカウントとして指定している場合です。組織の管理アカウントを、Organizations の委任された管理者アカウントにすることはできません。

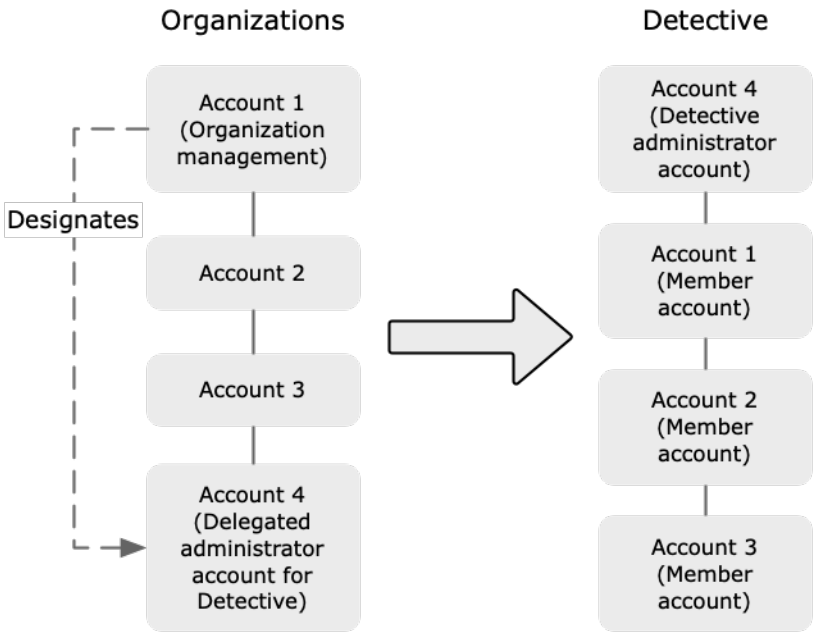
委任された管理者アカウントを Organizations に作成すると、組織管理アカウントは、委任された管理者アカウントか自らのいずれかのみを、Detective 管理者アカウントとして選択することができます。この委任された管理者アカウントをすべてのリージョンで選択することが推奨されます。

組織動作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。その動作グラフが組織動作グラフです。

Detective 管理者アカウントが既存の動作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動作グラフになります。

Detective 管理者アカウントは、組織動作グラフの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。



また、Detective 管理者アカウントは、組織に属さないアカウントに招待を送信することができます。詳細については、「the section called “組織メンバーアカウントの管理”」および「the section called “招待されたアカウントの管理”」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、現在の Detective 管理者アカウントを削除することができます。Detective 管理者アカウントを削除する場合、Detective はそのアカウントを現在のリージョンからのみ削除します。Organizations で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の Detective 管理者アカウントを削除すると、Detective は組織動作グラフを削除します。削除された Detective 管理者アカウントでは、Detective は無効になっています。

Detective の委任された現在の管理者アカウントを削除するには、Organizations API を使用します。Organizations での 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動作グラフをすべて削除します。組織管理アカウントが Detective 管理者アカウントである組織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許可

組織管理アカウントが Detective 管理者アカウントを設定できるようにするには、`AmazonDetectiveOrganizationsAccess`マネージドポリシーを AWS Identity and Access Management (IAM) エンティティにアタッチします。

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することができます。

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 を有効にする] ページで管理できます。

Detective 管理者アカウントを指定するには ([Detective を有効にする] ページ)

1. https://console.aws.amazon.com/detective/ で Amazon Detective コンソールを開きます。
2. [開始する] を選択します。
3. [管理者アカウントに必要なアクセス許可] パネルで、選択したアカウントに必要なアクセス許可を付与します。これにより、そのアカウントは Detective 管理者になり、Detective のすべてのアクションにフルアクセスできます。管理者として操作を行うには、`AmazonDetectiveFullAccess` ポリシーをプリンシパルにアタッチすることを推奨します。

4. [IAM からポリシーをアタッチする] を選択すると、推奨するポリシーが IAM コンソールに直接表示されます。
5. IAM コンソールにアクセス許可があるかどうかに応じて、次の手順を実行します。
   - IAM コンソールで操作するアクセス許可がある場合は、Detective に使用するプリンシパルに推奨ポリシーをアタッチします。
   - IAM コンソールを操作するアクセス許可がない場合は、ポリシーの Amazon リソースネーム (ARN) をコピーして IAM 管理者に提供してください。これにより、IAM 管理者がお客様に代わってポリシーをアタッチできます。
6. [Detective 管理者] で Detective 管理者アカウントを選択します。

   選択できるオプションは、Organizations での Detective の委任された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 での Detective の委任された管理者アカウントを持っていない場合は、アカウントのアカウント識別子を入力して Detective 管理者アカウントとして指定します。

     手動の招待プロセスによる管理者アカウントと動作グラフが残っている可能性もあります。その場合は、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。

     Organizations for Amazon GuardDuty、 AWS Security Hubまたは Amazon Macie に委任された管理者アカウントをお持ちの場合、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ます。また、これらとは別のアカウントを入力することもできます。
   - Organizations での委任された管理者アカウントを持っている場合は、そのアカウントか、自分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。この委任された管理者アカウントをすべてのリージョンで選択することが推奨されます。
7. [Delegate (委任)] を選択します。

Detective を有効にしている場合、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、[全般] ページで 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指定するには ([全般] ページ)

1. https://console.aws.amazon.com/detective/ で Amazon 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、[設定] の [全般] を選択します。

3. [マネージドポリシー] パネルでは、Detective がサポートするすべてのマネージドポリシーの詳細を確認できます。Detective でユーザーに実行させたいアクションに応じて、必要なアクセス許可をアカウントに付与できます。管理者として操作を行うには、`AmazonDetectiveFullAccess` ポリシーをプリンシパルにアタッチすることを推奨します。
4. IAM コンソールにアクセス許可があるかどうかに応じて、次の手順を実行します。

   - IAM コンソールで操作するアクセス許可がある場合は、Detective に使用するプリンシパルに推奨ポリシーをアタッチします。
   - IAM コンソールを操作するアクセス許可がない場合は、ポリシーの Amazon リソースネーム (ARN) をコピーして IAM 管理者に提供してください。これにより、IAM 管理者がお客様に代わってポリシーをアタッチできます。

   選択できるオプションは、Organizations での Detective の委任された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 での Detective の委任された管理者アカウントを持っていない場合は、アカウントのアカウント識別子を入力して Detective 管理者アカウントとして指定します。

     手動の招待プロセスによる管理者アカウントと動作グラフが残っている可能性もあります。その場合は、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。

     Organizations for Amazon GuardDuty、 AWS Security Hubまたは Amazon Macie に委任された管理者アカウントをお持ちの場合、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ます。また、これらとは別のアカウントを入力することもできます。
   - Organizations での委任された管理者アカウントを持っている場合は、そのアカウントか、自分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。この委任された管理者アカウントをすべてのリージョンで選択することが推奨されます。
5. [Delegate (委任)] を選択します。

Detective 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 コールまたは AWS Command Line Interfaceを使用します。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。

組織での Detective の委任された管理者アカウントを既に持っている場合は、そのアカウントまたは自分のアカウントのどちらかを選択する必要があります。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。

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

- Detective API: `EnableOrganizationAdminAccount` オペレーションを使用します。Detective 管理者アカウントの AWS アカウント識別子を指定する必要があります。アカウント識別子を取得するには、`ListOrganizationAdminAccounts` オペレーションを使用します。
- 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することができます。

Detective 管理者アカウントを削除すると、そのアカウントに対し、Detective が無効になり、組織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。

> **Important**
>
> Detective 管理者アカウントを削除しても、Organizations で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 を有効にする] ページ)

1. https://console.aws.amazon.com/detective/ で Amazon Detective コンソールを開きます。
2. [開始する] を選択します。
3. [委任された管理者] で [Amazon Detective を無効化] を選択します。

4. 確認ダイアログボックスで、「**disable**」と入力してから、[Amazon Detective を無効化] を選択します。

Detective 管理者アカウントを削除するには ([全般] ページ)

1. https://console.aws.amazon.com/detective/ で Amazon 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、[設定] の [全般] を選択します。
3. [委任された管理者] で [Amazon Detective を無効化] を選択します。
4. 確認ダイアログボックスで、「**disable**」と入力してから、[Amazon Detective を無効化] を選択します。

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

Detective 管理者アカウントを削除するには、API コールまたは AWS CLIを使用します。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、そのアカウントに対し、Detective が無効になり、組織動作グラフが削除されます。

> **Important**
>
> Detective 管理者アカウントを削除しても、Organizations で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 (Detective API) を削除するには AWS CLI

- Detective API: `DisableOrganizationAdminAccount` オペレーションを使用します。

  Detective API を使用して Detective 管理者アカウントを削除する場合、API コール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。
- 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
```

委任された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しても、Organizations での委任された管理者アカウントは自動的に削除されることはありません。Detective 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。

委任された管理者アカウントを削除すると、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すべての組織動作グラフが削除されます。また、それらのリージョンのアカウントに対し、Detective も無効になります。

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: `DeregisterDelegatedAdministrator` オペレーションを使用します。Detective 管理者アカウントのアカウント識別子と、Detective のサービスプリンシパル `detective.amazonaws.com` を指定する必要があります。
- 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
```

アカウントで使用可能なアクション

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

- すべて - アカウントは、同じ Detective 管理者アカウントに管理されているすべてのアカウントに対してこの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。

Detective 管理者アカウントは、組織動作グラフの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。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。または、手動で組織アカウントを有効にすることもできます。

管理者アカウントは、アカウントを、動作グラフのメンバーアカウントになるよう招待できます。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。

組織動作グラフ以外の動作グラフでは、メンバーアカウントはすべて招待されたアカウントです。

次の表は、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 の特徴と機能へのアクセスを制限できます。

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	Self (管理者アカウントを表示する)	Self (管理者アカウントを表示する)
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が削除される 組織アカウントとの関連付けが解除される	すべて	–	Self
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	すべて (設定がすべてのメンバーアカウントに適用される)	すべて (設定がすべてのメンバーアカウントに適用される)	–	–
Detective を無効化する	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)
動作グラフデータを表示する	すべて	すべて	–	–
オプションのデータソースパッケージを有効または無効にする	すべて	すべて	–	–

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。このリストに含まれる可能性があるものは以下のとおりです。

- 管理者アカウントによって動作グラフのメンバーになるように招待されたアカウント。これらのアカウントのタイプは [招待による] です。
- 組織アカウントのメンバーシップ (組織動作グラフの場合)。これらのアカウントのタイプは [組織別] です。

結果には、招待を辞退したメンバーアカウントや、管理者アカウントが動作グラフから削除したメンバー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)

招待するアカウントの場合、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かどうかを確認しています。また、Detective は、アカウントを有効にしたのが 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。招待メール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。

Invited (招待済み)

招待されたアカウントのステータス。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。

メンバーではありません

組織動作グラフの組織アカウントのステータス。この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ていません。

有効

招待されたアカウントの場合、アカウントは招待を承諾してメンバーとなり、動作グラフにデータを提供しています。

組織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このアカウントをメンバーアカウントとして有効にしました。このアカウントは、動作グラフにデータを提供しています。

有効になっていません

招待されたアカウントの場合は、メンバーアカウントは招待を承諾しましたが、有効にすることができていません。

組織動作グラフの組織アカウントの場合は、Detective 管理者アカウントがこのアカウントを有効にしようとしましたが、有効にできていません。

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は、 GuardDuty 48時間以上Amazonの顧客になっていません。
- 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表示 (コンソール)

を使用して、アカウントのリストを表示したり、絞り込んだりできます。 AWS Management Console

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以下のアカウントが含まれます。

   - お客様のアカウント
   - 動作グラフにデータを提供するよう招待したアカウント
   - 組織動作グラフにおけるすべての組織アカウント

   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 ID。
   - アカウント名 (組織アカウントの場合)。
   - アカウントタイプ ([招待別] または [組織別])。
   - アカウントのルートユーザーのメールアドレス (招待されたアカウントの場合)。
   - アカウントのステータス。
   - アカウントの日次データ量。ただし、Detective は、メンバーアカウントとして有効になっていないアカウントのデータ量を取得することはできません。
   - 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。
- ステータスが [有効] のアカウントを表示するには、[有効] を選択します。
- [有効] 以外のステータスのアカウントを表示するには、[有効になっていません] を選択します。

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を一覧表示する (Detective API、 AWS CLI)

API コールまたはを使用して、 AWS Command Line Interface 行動グラフ内のメンバーアカウントのリストを表示できます。

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 オペレーションを使用します。

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: ListMembers オペレーションを使用します。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。

  組織動作グラフのメンバーアカウントとして有効にしなかった組織アカウントや、動作グラフとの関連付けを解除した組織アカウントは、ListMembers では表示されませんので、注意してください。
- 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: GetMembers オペレーションを使用します。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
```

メンバーアカウントとしての組織アカウントの管理

Detective 管理者アカウントは、組織動作グラフの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。

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。または、手動で組織アカウントを有効にすることもできます。

さらに、Detective 管理者アカウントは、組織アカウントと組織動作グラフとの関連付けを解除することもできます。

コンテンツ

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、自動的に組織動作グラフのメンバーアカウントとして新しい組織アカウントを有効にするように Detective を設定することができます。

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] ページのリストに追加されます。組織アカウントの場合、[Type] (タイプ) は [By organization] (組織別) になります。

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。ステータスは、[Not a member] (メンバーではない) です。

組織アカウントの自動的な有効化を選択すると、Detective は、組織に追加された新しいアカウントをメンバーアカウントとして有効化するようになります。有効になっていない既存の組織アカウントは有効になりません。

Detective がメンバーアカウントとして組織アカウントを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 個です。動作グラフに既に 1,200 個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 が有効になっていないアカウントを 48 時間以上有効にすることはできません。

- Detective は、アカウントを有効にすると動作グラフのデータ量が許容最大数を超えるようなアカウントを有効にすることはできません。

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)

[アカウント管理] ページの [新しい組織アカウントを自動的に有効にする] 設定により、アカウントが組織に追加された時点で自動的に有効化されるようにするかどうかを設定できます。

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. https://console.aws.amazon.com/detective/ で Amazon 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. [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にする (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設定するには、管理者アカウントは Detective API または AWS Command Line Interfaceを使用します。

設定を表示・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` オペレーションを使用します。

組織アカウントを自動的に有効にする現在の設定を表示するには

- Detective API: `DescribeOrganizationConfiguration` オペレーションを使用します。

  新しい組織アカウントを自動的に有効化されるようにすると、この応答として、`AutoEnable` が `true` になります。
- 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: UpdateOrganizationConfiguration オペレーションを使用します。新しい組織アカウントを自動的に有効にするには、AutoEnable を true に設定します。
- 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
```

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

新しい組織アカウントを自動的に有効化しない場合は、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は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設定

組織動作グラフにすでに最大数である 1,200 個の有効なアカウントがある場合、その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。その場合、組織アカウントのステータスは [メンバーではありません] のままになります。

組織アカウントを有効にすると、Detective はそのアカウントが 48 GuardDuty 時間以上Amazonの顧客であった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、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チェックします。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 [有効になっていません] です。

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 [有効] に更新されます。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 [有効になっていません] のままになります。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チェックに合格するとすぐに、Detective はメンバーアカウントのステータスを自動的に [有効] に変更します。

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 (コンソール)

[アカウント管理] ページで、メンバーアカウントとして組織アカウントを有効にできます。

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

1. https://console.aws.amazon.com/detective/ で Amazon 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、[有効になっていません] を選択します。
4. 有効化対象として、特定の組織アカウントを選択することも、すべての組織アカウントを選択することもできます。

   選択した組織アカウントを有効にするには:

   a. 有効にする個々の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化] を選択します。

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 API、 AWS CLI)

Detective API またはを使用して、 AWS Command Line Interface 組織アカウントを組織行動グラフのメンバーアカウントとして有効にできます。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` オペレーションを使用します。

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には (Detective API、 AWS CLI)

- Detective API: `CreateMembers` オペレーションを使用します。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、アカウント識別子を指定します。組織動作グラフ内の組織アカウントは招待されません。メールアドレスや、招待に関するその他の情報を指定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
```

組織アカウントとメンバーアカウントの関連付けを解除する

組織動作グラフ内の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、そのアカウントと組織動作グラフ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 [メンバーではありません] に変わります。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を解除する (コンソール)

[アカウント管理] ページで、メンバーアカウントとして組織アカウントの関連付けを解除できます。

1. https://console.aws.amazon.com/detective/ で Amazon 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. 有効アカウントのリストを表示するには、[有効] を選択します。
4. 関連付けを解除するには、各アカウントのチェックボックスをオンにします。
5. [アクション] を選択します。次に、[アカウントを無効化] を選択します。

   関連付けを解除したアカウントのアカウントステータスが [メンバーではありません] に変わります。

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

Detective API またはを使用して、 AWS Command Line Interface 行動グラフ内の組織アカウントをメンバーアカウントとして関連付けることを解除できます。

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 オペレーションを使用します。

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

- Detective API: DeleteMembers オペレーションを使用します。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、アカウントを、動作グラフのメンバーアカウントになるよう招待できます。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。

組織動作グラフ以外の動作グラフでは、メンバーアカウントはすべて招待されたアカウントです。

Detective 管理者アカウントは、組織アカウント以外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。

管理者アカウントは、動作グラフから、招待されたメンバーアカウントを削除することもできます。

コンテンツ

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、アカウントを招待できます。動作グラフには、最大 1,200 個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. 追加するメンバーアカウントごとに、 AWS 管理者アカウントがアカウント識別子とルートユーザーの電子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 が 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認すると、Detective はそのメンバーアカウントが 48 GuardDuty 時間以上Amazonの顧客であった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 [有効になっていません] です。

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 [有効] に更新されます。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 [有効になっていません] のままになります。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ための要件があ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 [有効] に変更します。

   たとえば、メンバーアカウントが有効になり GuardDuty 、Detective がデータ量が多すぎないことを確認したり、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用のスペースを確保したりすると、メンバーアカウントのステータスは [有効] に変わります。

   複数のアカウントのステータスが [有効になっていません] である場合、Detective は招待された順序でアカウントを有効にします。ステータスが [有効になっていません] であるアカウントを有効にするかどうかをチェックするプロセスは、1 時間ごとに実行されます。

   管理者アカウントは、自動プロセスが実行されるまで待つのではなく、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 “ステータスがが [有効になっていません] であるメンバーアカウントの有効化” を参照してください。

   Detective は、2021 年 5 月 12 日から、ステータスが [有効になっていません] である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。それ以前にステータスが [有効になっていません] であったアカウントは、自動的に有効になることはありません。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)

動作グラフへのデータ提供を求めて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. https://console.aws.amazon.com/detective/ で Amazon 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. [アクション] 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. 「AWS アカウント ID」には、 AWS アカウント ID を入力します。

   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. 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. https://console.aws.amazon.com/detective/ で Amazon 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. [アクション] 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. 招待を選択します。

メンバーアカウントを行動グラフに招待する (Detective API、) AWS CLI

Detective API またはを使用して、 AWS Command Line Interface 行動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` オペレーションを使用します。

メンバーアカウントを行動グラフに招待するには (Detective API、 AWS CLI)

- Detective API: `CreateMembers` オペレーションを使用します。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
```

複数の地域にわたるメンバーアカウントのリストの追加 (Python スクリプトオン GitHub)

Detective は、 GitHub 以下のことを可能にするオープンソーススクリプトを提供しています。

- 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 スクリプトの設定と使用方法については、を参照してください。the section called “Amazon Detective の Python スクリプト”

ステータスがが [有効になっていません] である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 [有効になっていません] に設定します。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は、 GuardDuty 48時間以上Amazonの顧客になっていません。
- 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。

ステータスが [有効になっていません] である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。

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。

ステータスが [有効になっていません] であるメンバーアカウントを手動で有効にすることを試みることもできます。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、ステータスが [有効になっていません] であるメンバーアカウントを有効にすることを試みることができます。

ステータスが [有効になっていません] であるメンバーアカウントの有効化 (コンソール)

メンバーアカウントリストには、ステータスが [有効になっていません] である、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。

ステータスが [有効になっていません] であるメンバーアカウントを有効化するには

1. https://console.aws.amazon.com/detective/ で Amazon 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 [有効になっていません] であるメンバーアカウントのみを有効にできます。
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は、ステータスが [有効] に変わります。

有効になっていないメンバーアカウントを有効にする (Detective API、 AWS CLI)

API コールまたはを使用して、有効化されていない 1 つのメンバーアカウントを有効化できます。 AWS Command Line Interface 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` オペレーションを使用します。

ステータスが [有効になっていません] であるメンバーアカウントを有効化するには

- Detective API: `StartMonitoringMember` API 動作を使用します。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 ID を使用します。
- AWS CLI: コマンドラインで `start-monitoring-member` コマンドを実行します。

```
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された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）および AWS GovCloud （米国西部）リージョンを除き AWS、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された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されたメンバーアカウントの削除 (コンソール)

を使用して、 AWS Management Console 招待されたメンバーアカウントを行動グラフから削除できます。

メンバーアカウントを削除するには (コンソール)

1. https://console.aws.amazon.com/detective/ で Amazon 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. アカウントリストで、削除する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. [アクション] を選択します。次に、[アカウントを無効化] を選択します。

行動グラフから招待されたメンバーアカウントを削除する (Detective API、 AWS CLI)

Detective API またはを使用して、 AWS Command Line Interface 招待されたメンバーアカウントを行動グラフから削除できます。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` オペレーションを使用します。

招待されたメンバーアカウントを行動グラフから削除するには (Detective API、 AWS CLI)

- Detective API: `DeleteMembers` オペレーションを使用します。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
```

複数の地域にわたる招待メンバーアカウントのリストの削除 (Python スクリプトオン GitHub)

Detective ではオープンソースのスクリプトを提供しています。 GitHub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や使用方法については、を参照してください。the section called “Amazon Detective の Python スクリプト”

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

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、所属している動作グラフの管理者アカウントを確認できます。

動作グラフに招待されたメンバーアカウントは、招待を確認したり、招待に応答したりできます。また、動作グラフからアカウントを削除することもできます。

組織アカウントは、組織動作グラフのメンバーアカウントになれるかどうかを自らでは制御できません。組織動作グラフの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できるのは、Detective 管理者アカウントです。

コンテンツ

- 動作グラフの招待への応答
- 動作グラフからのアカウントの削除

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:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
```

```
}
```

組織動作グラフ内の組織アカウントは招待を送信されず、そのアカウントと組織動作グラフとの関連付けを解除できないことに注意してください。他の動作グラフに属していない組織アカウントは、`ListInvitations` へのアクセス許可のみが必要です。`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。招待を管理したり、メンバーシップの関連付けを解除したりするアクセス許可は、招待されたメンバー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、またはメンバーアカウントから AWS Command Line Interface、各自の行動グラフへの招待を確認できます。

動作グラフの招待の表示 (コンソール)

行動グラフの招待状は、から表示できます。 AWS Management Console

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、[マイ管理者アカウント] には組織動作グラフも表示されます。

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。
- 承諾した招待のステータスは [有効] または [有効になっていません] のいずれかとなります。

ステータスが [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 [有効になっていません] 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 [無効] に設定されます。その間、Detective は、 GuardDuty 有効になっているかどうか、有効になっている場合は、アカウントによって行動グラフのデータ量が Detective クォータを超え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 [有効] に更新します。それ以外の場合、ステータスは [有効になっていません] のままとなります。

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 [有効] に更新します。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: `ListInvitations` オペレーションを使用します。
- 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

招待を承諾する際、アカウントのステータスは、最初は [有効になっていません] に設定されていますが、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 がこのチェックを行うには、アカウントで 48 GuardDuty 時間以上Amazonが有効になっ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 [有効] に更新します。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行動グラフのデータ量が検出クォータを超える場合、 GuardDuty または有効にしていない場合は、ステータスは [有効化されていません] のままになります。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)

を使用して、Detective コンソールへのリンクを含む招待メールに返信できます。 AWS Management Console 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. https://console.aws.amazon.com/detective/ で Amazon 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。

ビヘイビアグラフへの招待への応答 (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。

ビヘイビアグラフへの招待を受け入れるには (Detective API) AWS CLI

- Detective API: `AcceptInvitation` オペレーションを使用します。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
```

ビヘイビアグラフへの招待を拒否するには (Detective API、 AWS CLI)

- Detective API: `RejectInvitation` オペレーションを使用します。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。

招待されたアカウントのみが動作グラフから自らのアカウントを削除できます。組織アカウントは、招待されたアカウントを組織動作グラフから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 を使用して行動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. https://console.aws.amazon.com/detective/ で Amazon 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。

行動グラフからアカウントを削除する (Detective API、 AWS CLI)

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

行動グラフ (Detective API) からアカウントを削除するには AWS CLI

- Detective API: DisassociateMembership オペレーションを使用します。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
```

アカウントアクションが動作グラフに及ぼす影響

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 が無効化される

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

- 動作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。

動作グラフからメンバーアカウントが削除される

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、そのアカウントは [マイメンバーアカウント] リストから削除されます。

組織動作グラフの組織アカウントでは、アカウントステータスが [メンバーではありません] に変わります。

組織からメンバーアカウントが削除される

組織から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。

- そのアカウントは、組織動作グラフの [マイメンバーアカウント] リストから削除されます。
- 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 アカウントが停止されました

管理者アカウントが停止されると AWS、そのアカウントは Detective の動作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。

メンバーアカウントが停止されると 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、アカウントは削除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、その Detective におけるアクセス許可が復元されます。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開されると、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 アカウントは閉鎖されました

AWS アカウントが閉鎖されると、Detectiveは次のように閉鎖に対応します。

- 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 アカウントのポリシーデータは、管理者アカウント閉鎖の発効日から 90 日間保持されます。90 AWS 日間の期間が終了すると、アカウントのすべてのポリシーデータが完全に削除されます。

- 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 ルール付きの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 ポリシーデータを保持している限り、閉鎖したアカウントを再度開くと、 AWS アカウントをサービス管理者として再割り当てし、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**
>
> 各地域のお客様向け: AWS GovCloud (US)
>
> - アカウントを閉鎖する前に、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、当該アカウントへのアクセス権を失います。

Amazon Detective Python スクリプトを使用してアカウントを管理する

Amazon Detective では、リポジトリにオープンソースの Python スクリプトのセットが用意されています。 GitHub amazon-detective-multiaccount-scripts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

スクリプトには、管理者アカウントと、 AWS 追加または削除するすべてのメンバーアカウントにある既存のロールが必要です。

> **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 ポリシーについて推奨されているベストプラクティスは、適用範囲を最も絞り込んだロールを使用することです。グラフの作成、メンバーの作成、グラフへのメンバーの追加というスクリプトワークフローを実行するために必要なアクセス許可は、次のとおりです。

- 探偵:CreateGraph
- 探偵:CreateMembers
- 探偵:DeleteGraph
- 探偵:DeleteMembers

- 探偵:ListGraphs
- 探偵:ListMembers
- 探偵:AcceptInvitation

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。
- 必要な権限を上記に追加 (推奨) するか、AmazonDetectiveFullAccess管理ポリシーを選択してください。
- 前述の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には、`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、`EnableDetective`という名前のプロファイルのインスタンスロールが作成されました。

   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) からダウンロードします。
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. GitHub (https://github.com/aws-samples/ amazon-detective-multiaccount-scripts) からスクリプトソースコードをダウンロードします。
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`

プラットフォーム	セットアップ手順
	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 からスクリプトソースコードを複製します。

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

AWS 管理者アカウントのアカウント ID。

roleName

AWS 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

AWS 管理者アカウントのアカウント ID。

roleName

AWS 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。

Amazon Security Lake との統合

Amazon Security Lake は、完全マネージド型のセキュリティデータレイクサービスです。Security Lake を使用すると、 AWS 環境、SaaS プロバイダー、オンプレミスソース、クラウドソース、およびサードパーティーソースのセキュリティデータを、 AWS アカウントに保存されている専用のデータレイクに自動的に一元化できます。Security Lake はセキュリティデータの分析に役立つため、組織全体のセキュリティ体制をより完全に把握できます。Security Lake を使用すると、ワークロード、アプリケーション、データの保護を強化することもできます。

Amazon Security Lake と Amazon Detective の統合により、Security Lake に保存されている未処理のログデータを検索して取得できます。

この統合を使用すると、Security Lake がネイティブにサポートしている以下のソースからログとイベントを収集できます。Detective は、最大ソースバージョン 2 (OCSF 1.1.0) をサポートします。

- AWS CloudTrail 管理イベントバージョン 1.0 以降
- Amazon Virtual Private Cloud (Amazon VPC) フローログバージョン 1.0 以降
- Amazon Elastic Kubernetes Service (Amazon EKS) 監査ログバージョン 2.0。Amazon EKS 監査ログをソースとして使用するには、IAM アクセス許可`ram:ListResources`に を追加する必要があります。詳細については、「アカウント に必要な IAM アクセス許可を追加する」を参照してください。

Security Lake がネイティブにサポートされている AWS サービスから OCSF スキーマにログとイベントを自動的に変換する方法の詳細については、「Amazon Security Lake ユーザーガイド」を参照してください。

Detective を Security Lake と統合すると、Detective は AWS CloudTrail 管理イベントと Amazon VPC フローログに関連する raw ログを Security Lake から取得し始めます。詳細については、「未処理のログのクエリ」を参照してください。

Detective を Security Lake と統合するには、次の手順を実行します。

1. 開始する前に

   Organizations 管理アカウントを使用する場合は、組織の委任された Security Lake 管理者を指定する必要があります。Security Lake が有効になっていることを確認し、Security Lake が AWS CloudTrail 管理イベントと Amazon Virtual Private Cloud (Amazon VPC) フローログからログとイベントを収集していることを確認します。

Security Reference Architecture に従って、Detective はログアーカイブアカウントの使用を推奨し、Security Lake デプロイに Security Tooling アカウントを使用することを延期します。

2. Security Lake サブスクライバーを作成する

   Amazon Security Lake からのログとイベントを使用するには、Security Lake サブスクライバーである必要があります。Detective アカウント管理者にクエリアクセス権を付与するには、次の手順に従います。

3. 必要な AWS Identity and Access Management (IAM) アクセス許可を IAM ID に追加します。
   - Security Lake との Detective 統合を作成するには、次のアクセス許可を追加します。
     - これらの AWS Identity and Access Management (IAM) アクセス許可を IAM アイデンティティにアタッチします。詳細については、「アカウントに必要な IAM アクセス許可を追加する」セクションを参照してください。
     - この IAM ポリシーを、 AWS CloudFormation サービスロールを渡すために使用する予定の IAM プリンシパルに追加します。詳細については、「IAM プリンシパルにアクセス許可を追加する」セクションを参照してください。
   - Detective を Security Lake と既に統合している場合は、統合を使用するには、これらの (IAM) アクセス許可を IAM ID にアタッチします。詳細については、「アカウントに必要な IAM アクセス許可を追加する」セクションを参照してください。
4. リソース共有 ARN の招待を受け入れ、統合を有効する

AWS CloudFormation テンプレートを使用して、Security Lake サブスクライバーのクエリアクセスを作成および管理するために必要なパラメータを設定します。スタックを作成する詳細な手順については、AWS CloudFormation 「 テンプレートを使用してスタックを作成する」を参照してください。スタックの作成が完了したら、統合を有効にします。

Detective コンソールを使用して Amazon Detective を Amazon Security Lake と統合する方法のデモンストレーションについては、次の動画をご覧ください。Amazon Detective と Amazon Security Lake の統合 - セットアップ方法

開始する前に

Security Lake は と統合 AWS Organizations して、組織内の複数のアカウントにわたるログ収集を管理します。組織の Security Lake を使用するには、 AWS Organizations まず管理アカウントで組織の委任された Security Lake 管理者を指定する必要があります。次に、委任された Security Lake 管理

者は、Security Lake を有効にし、組織内のメンバーアカウントのログとイベントの収集を有効にする必要があります。

Security Lake を Detective と統合する前に、Security Lake 管理者アカウントで Security Lake が有効になっていることを確認してください。Security Lake を有効にする方法の詳細な手順については、『Amazon Security Lake ユーザーガイド』の「ご利用開始にあたって」を参照してください。

また、Security Lake が AWS CloudTrail 管理イベントと Amazon Virtual Private Cloud (Amazon VPC) フローログからログとイベントを収集していることを確認します。Security Lake でのログ収集の詳細については、「Amazon Security Lake ユーザーガイド」の「 AWS のサービスからのデータ収集」を参照してください。

ステップ 1: Security Lake サブスクライバーを作成する

Amazon Security Lake からのログとイベントを使用するには、Security Lake サブスクライバーである必要があります。サブスクライバーは、Security Lake が収集するデータにクエリを実行して、アクセスできます。クエリアクセス権を持つサブスクライバーは、Amazon Athena などのサービスを使用して、Amazon Simple Storage Service (Amazon S3) バケット内の AWS Lake Formation テーブルを直接クエリできます。 Amazon Athena サブスクライバーになるには、Security Lake 管理者がデータレイクにクエリを実行できるサブスクライバーアクセスを提供する必要があります。管理者がこれを行う方法については、『Amazon Security Lake ユーザーガイド』の「クエリアクセス権限を持つサブスクライバーの作成」を参照してください。

Detective アカウント管理者にクエリアクセス権を付与するには、次の手順に従います。

Security Lake で Detective サブスクライバーを作成するには

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで、[統合] を選択します。
3. Security Lake のサブスクライバーペインで、[アカウント ID] と [外部 ID] の値を書き留めます。

   Security Lake 管理者にこれらの ID を使用して次のことを行うように依頼します。

   - Security Lake で Detective サブスクライバーを作成する。
   - サブスクライバーにクエリアクセス権限が付与されるように設定する。
   - Security Lake クエリサブスクライバーが Lake Formation の許可が付与された状態で作成されていることを確認する。Security Lake コンソールのデータアクセス方法として Lake Formation を選択します。

Security Lake 管理者によってサブスクライバーが作成されると、Security Lake ではそのサブスクライバーに対して Amazon リソース共有 ARN を生成します。管理者にこの ARN を送信するよう依頼してください。

4. Security Lake 管理者から提供されたリソース共有 ARN を [Security Lake サブスクライバー] ペインに入力します。
5. Security Lake 管理者からリソース共有 ARN を受け取ったら、[Security Lake サブスクライバー] ペインの [リソース共有 ARN] ボックスにその ARN を入力します。

ステップ 2: 必要な IAM アクセス許可をアカウントに追加する

Detective と Security Lake の統合を有効にするには、次の AWS Identity and Access Management (IAM) アクセス許可ポリシーを IAM アイデンティティにアタッチする必要があります。

以下のインラインポリシーをロールにアタッチします。独自の Amazon S3 バケットを使用して Athena クエリ結果を保存する場合は、`athena-results-bucket` を Amazon S3 バケット名に置き換えてください。Detective に Amazon S3 バケットを自動的に生成させて Athena クエリの結果を保存する場合は、IAM ポリシーから `S3ObjectPermissions` 全体を削除します。

このポリシーを IAM ID にアタッチするために必要なアクセス許可がない場合は、 AWS 管理者にお問い合わせください。必要な権限が付与されているにもかかわらず問題が発生した場合は、『IAM ユーザーガイド』の「一般的な IAM の問題のトラブルシューティング」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ObjectPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
```

```
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<athena-results-bucket>",
        "arn:aws:s3:::<athena-results-bucket>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/
amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "lakeformation:GetDataAccess",
        "ram:ListResources"
      ],
      "Resource": "*"
    },
    {
       "Effect": "Allow",
        "Action": [
          "ssm:GetParametersByPath"
        ],
        "Resource": [
```

```
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/ResourceShareArn",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/S3Bucket",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/TableNames",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/DatabaseName",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/StackId"
        ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "securitylake.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

ステップ 3: リソース共有 ARN の招待を受け入れ、統合を有効する

Security Lake から未処理のデータログにアクセスするには、Security Lake 管理者が作成した Security Lake アカウントからのリソース共有招待を承諾する必要があります。また、クロスアカウントテーブル共有を設定するための AWS Lake Formation 権限も必要です。さらに、未処理のクエリログを受信できる Amazon Simple Storage Service (Amazon S3) バケットを作成する必要があります。

次のステップでは、 AWS CloudFormation テンプレートを使用して、リソース共有 ARN 招待の受け入れ、必要な AWS Glue クローラー リソースの作成、 AWS Lake Formation 管理者権限の付与を行うスタックを作成します。

AWS CloudFormation スタックを作成するには

1. CloudFormation テンプレートを使用して新しい CloudFormation スタックを作成します。詳細については、「AWS CloudFormation テンプレートを使用したスタックの作成」を参照してください。
2. スタックの作成が完了したら、[統合を有効にする] を有効にします。

AWS CloudFormation テンプレートを使用したスタックの作成

Detective には AWS CloudFormation テンプレートが用意されています。これを使用して、Security Lake サブスクライバーのクエリアクセスを作成および管理するために必要なパラメータを設定できます。

ステップ 1: AWS CloudFormation サービスロールを作成する

AWS CloudFormation テンプレートを使用してスタックを作成するには、 AWS CloudFormation サービスロールを作成する必要があります。サービスロールを作成するために必要な権限がない場合は、Detective 管理者アカウントを持つ管理者に連絡してください。 AWS CloudFormation サービスロールの詳細については、「AWS CloudFormation サービスロール」を参照してください。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. [Select trusted entity] (信頼されたエンティティの選択) で、[AWS のサービス] を選択します。
4. [AWS CloudFormation] を選択します。[次へ] を選択します。
5. ロールの名前を入力します。例えば `CFN-DetectiveSecurityLakeIntegration` です。
6. 以下のインラインポリシーをロールにアタッチします。を AWS アカウント ID <Account ID>に置き換えます。

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

```
            "Sid": "CloudFormationPermission",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateChangeSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:aws:transform/*"
            ]
        },
        {
            "Sid": "IamPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:PassRole",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::<ACCOUNT ID>:role/*",
                "arn:aws:iam::<ACCOUNT ID>:policy/*"
            ]
        },
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket*",
                "s3:PutBucket*",
                "s3:GetBucket*",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "LambdaPermissions",
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:TagResource",
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
            ]
        },
        {
            "Sid": "CloudwatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        },
        {
            "Sid": "KmsPermission",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
        }
    ]
}
```

ステップ 2: IAM プリンシパルにアクセス権限を追加する

前のステップで作成した CloudFormation サービスロールを使用してスタックを作成するには、次のアクセス許可が必要です。 CloudFormation サービスロールを渡すために使用する予定の IAM プリン

シパルに、次の IAM ポリシーを追加します。この IAM プリンシパルを引き受けてスタックを作成します。IAM ポリシーを追加するために必要な権限がない場合は、Detective 管理者アカウントを持つ管理者に連絡してください。

> **Note**
>
> 次のポリシーでは、このポリシーで使用される CFN-DetectiveSecurityLakeIntegration は、前述の Creating an AWS CloudFormation サービスロールステップで作成したロールを指します。異なる場合は、前のステップで入力したロール名に変更してください。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
            "Sid": "PassRole",
            "Effect": "Allow",
            "Action":
            [
               "iam:GetRole",
               "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
       },
       {
           "Sid": "RestrictCloudFormationAccess",
           "Effect": "Allow",
           "Action": [
               "cloudformation:CreateStack",
               "cloudformation:DeleteStack",
               "cloudformation:UpdateStack"
           ],
           "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
           "Condition": {
               "StringEquals": {
                   "cloudformation:RoleArn": [
                       "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
                   ]
               }
```

```
            }
        },
        {
            "Sid": "CloudformationDescribeStack",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:GetStackPolicy"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
        },
        {
            "Sid": "CloudformationListStacks",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        }
    ]
}
```

ステップ 3: AWS CloudFormation コンソールでカスタム値を指定する

1. Detective から AWS CloudFormation コンソールに移動します。
2. (オプション) [スタック名] にを入力します。スタック名は自動入力されます。スタック名は既存のスタック名と競合しない名前に変更できます。
3. 以下のパラメータを入力します。

    - AthenaResultsBucket – 値を入力しない場合、このテンプレートは Amazon S3 バケットを生成します。独自のバケットを使用するには、バケット名を入力して Athena クエリ結果を保存します。独自のバケットを使用する場合、バケットがリソース共有 ARN と同じリージョンにあることを確認します。また、選択した LakeFormationPrincipals に、そのバケット

に対してオブジェクトを書き込んだり、そのバケットからオブジェクトを読み取ったりするアクセス権限があることを確認してください。バケットのアクセス権限の詳細については、『Amazon Athena ユーザーガイド』の「クエリ結果と最近のクエリ」を参照してください。

- DTRegion — このフィールドは事前に入力されています。このフィールドの値は変更しないでください。
- LakeFormationPrincipals – Security Lake 統合を使用するためのアクセスを許可する IAM プリンシパルの ARN (IAM ロール ARN など) をカンマで区切って入力します。これらは、Detective を使用するセキュリティアナリストやセキュリティエンジニアである可能性があります。

  ステップ [Step 2: Add the required IAM permissions to your account] で IAM アクセス権限をアタッチした IAM プリンシパルのみを使用できます。
- ResourceShareARN – このフィールドは事前に入力されています。このフィールドの値は変更しないでください。

4. アクセス許可

   IAM ロール – Creating an AWS CloudFormation Service Role ステップで作成したロールを選択します。現在の IAM ロールに Creating an AWS CloudFormation Service Role ステップで必要なすべてのアクセス権限がある場合は、任意で空白のままにできます。
5. [同意します] ボックスをすべて確認してチェックし、[スタックの作成] ボタンをクリックします。詳細については、作成される次の IAM リソースを確認してください。

```
* ResourceShareAcceptorCustomResourceFunction
    - ResourceShareAcceptorLambdaRole
    - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
    - SsmParametersLambdaRole
    - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
    - GlueDatabaseLambdaRole
    - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
    - GlueTablesLambdaRole
    - GlueTablesLogsAccessPolicy
```

ステップ 4: Amazon S3 バケットポリシーを **LakeFormationPrincipals** 内の IAM プリンシパルに追加する

(オプション) このテンプレートで AthenaResultsBucket を生成する場合は、以下のポリシーを LakeFormationPrincipals 内の IAM プリンシパルにアタッチする必要があります。

```
{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}
```

をAthenaResultsBucket名前athena-results-bucketに置き換えます。
AthenaResultsBucketは AWS CloudFormation コンソールにあります。

1. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。
2. スタックをクリックします。
3. [リソース] タブをクリックします。
4. 論理 ID AthenaResultsBucket を検索し、その物理 ID をコピーします。

CloudFormation スタックの削除

既存のスタックを削除しないと、同じリージョンでの新しいスタックの作成が失敗します。
CloudFormation コンソールまたは AWS CLI を使用して CloudFormation スタックを削除できます。

AWS CloudFormation スタックを削除するには (コンソール)

1. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。
2. CloudFormation コンソールの スタック ページで、削除するスタックを選択します。スタックは現在実行中である必要があります。
3. [スタックの詳細] ペインで、[削除] を選択します。
4. プロンプトが表示されたら、[スタックの削除] を選択します。

> **Note**
>
> いったんスタックの削除が開始されると、スタックの削除オペレーションは停止できません。スタックは DELETE_IN_PROGRESS 状態になります。

スタックの削除操作が完了すると、スタックの状態が DELETE_COMPLETE になります。

スタック削除エラーのトラブルシューティング

Delete ボタンをクリックFailed to delete stackした後にメッセージでアクセス許可エラーが表示される場合、IAM ロールにはスタックを削除する CloudFormation アクセス許可がありません。スタックを削除するには、アカウント管理者にお問い合わせください。

CloudFormation スタックを削除するには (AWS CLI)

AWS CLI インターフェイスで次のコマンドを入力します。

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
      arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

CFN-DetectiveSecurityLakeIntegration は、Creating an AWS CloudFormation Service Role ステップで作成したサービスロールです。

統合設定の変更

Detective と Security Lake の統合に使用したパラメーターのいずれかを変更する場合は、そのパラメーターを編集してから統合を再度有効にします。 AWS CloudFormation テンプレートを編集して、次のシナリオでこの統合を再度有効にできます。

- Security Lake サブスクリプションを更新するため、新しいサブスクライバーを作成するか、Security Lake 管理者が既存のサブスクリプションのデータソースを更新する。
- 別の Amazon S3 バケットを指定して、未処理のクエリログを保存する。
- 異なる Lake Formation プリンシパルを指定する。

Detective と Security Lake の統合を再度有効にすると、リソース共有 ARN を編集し、IAM アクセス許可を表示できます。IAM アクセス許可を編集するには、Detective から IAM コンソールに移動しま

す。テンプレートに以前に入力した値を編集することもできます AWS CloudFormation 。統合を再度有効にするには、既存の CloudFormation スタックを削除して再作成する必要があります。

Detective と Security Lake の統合を再度有効にするには

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで、[統合] を選択します。
3. 統合は、次のいずれかの手順で編集できます。
   - [Security Lake] ペインで [編集] を選択します。
   - [Security Lake] ペインで [表示] を選択します。[表示] ページで [編集] を選択します。
4. 新しいリソース共有 ARN を入力し、リージョンのデータソースにアクセスします。
5. 現在の IAM アクセス許可を確認し、IAM アクセス許可を編集する場合は IAM コンソールに移動します。
6. CloudFormation テンプレートの値を編集します。
   1. 新しいスタックを作成する前に、既存のスタックを削除します。既存のスタックを削除せずに、同じリージョンで新しいスタックを作成しようとすると、リクエストが失敗します。詳細については、「 CloudFormation スタックの削除」を参照してください。

   1. 新しい CloudFormation スタックを作成します。詳細については、「AWS CloudFormation テンプレートを使用したスタックの作成」を参照してください。
7. [統合を有効にする] を選択します。

統合の無効化

Detective と Security Lake の統合を無効にすると、Security Lake からのログやイベントデータのクエリを実行できなくなります。

Detective と Security Lake の統合を無効にするには

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで、[統合] を選択します。
3. 既存のスタックを削除します。詳細については、「 CloudFormation スタックの削除」を参照してください。
4. [Security Lake 統合を無効にする] ペインで [無効] を選択します。

サポートされている AWS リージョン

Detective は、次の AWS リージョンで Security Lake と統合できます。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (オハイオ)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
米国東部 (バージニア北部)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
米国西部 (北カリフォルニア)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
米国西部 (オレゴン)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
アジアパシフィック (ムンバイ)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
アジアパシフィック (ソウル)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS
アジアパシフィック (シンガポール)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
アジアパシフィック (シドニー)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS
アジアパシフィック (東京)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
カナダ (中部)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS
欧州 (フランクフルト)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
欧州 (アイルランド)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS
欧州 (ロンドン)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
欧州 (パリ)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
欧州 (ストックホルム)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
南米 (サンパウロ)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

Detective での未処理のログのクエリ

Detective を Security Lake と統合すると、Detective は AWS CloudTrail 管理イベントと Amazon Virtual Private Cloud (Amazon VPC) フローログに関連する raw ログを Security Lake から取得し始めます。

> **Note**
>
> Detective で未処理のログのクエリを実行する場合、追加料金はかかりません。Amazon Athena を含む他の AWS のサービスの使用料金は、引き続き公開料金で適用されます。

AWS CloudTrail 管理イベントは、次のプロファイルで使用できます。

- AWS アカウント
- AWS ユーザー
- AWS ロール
- AWS ロールセッション
- Amazon EC2 インスタンス
- Amazon S3 バケット

- IP アドレス
- Kubernetes クラスター
- Kubernets ポッド
- Kubernets の件名
- IAM ロール
- IAM ロールセッション
- IAM ユーザー

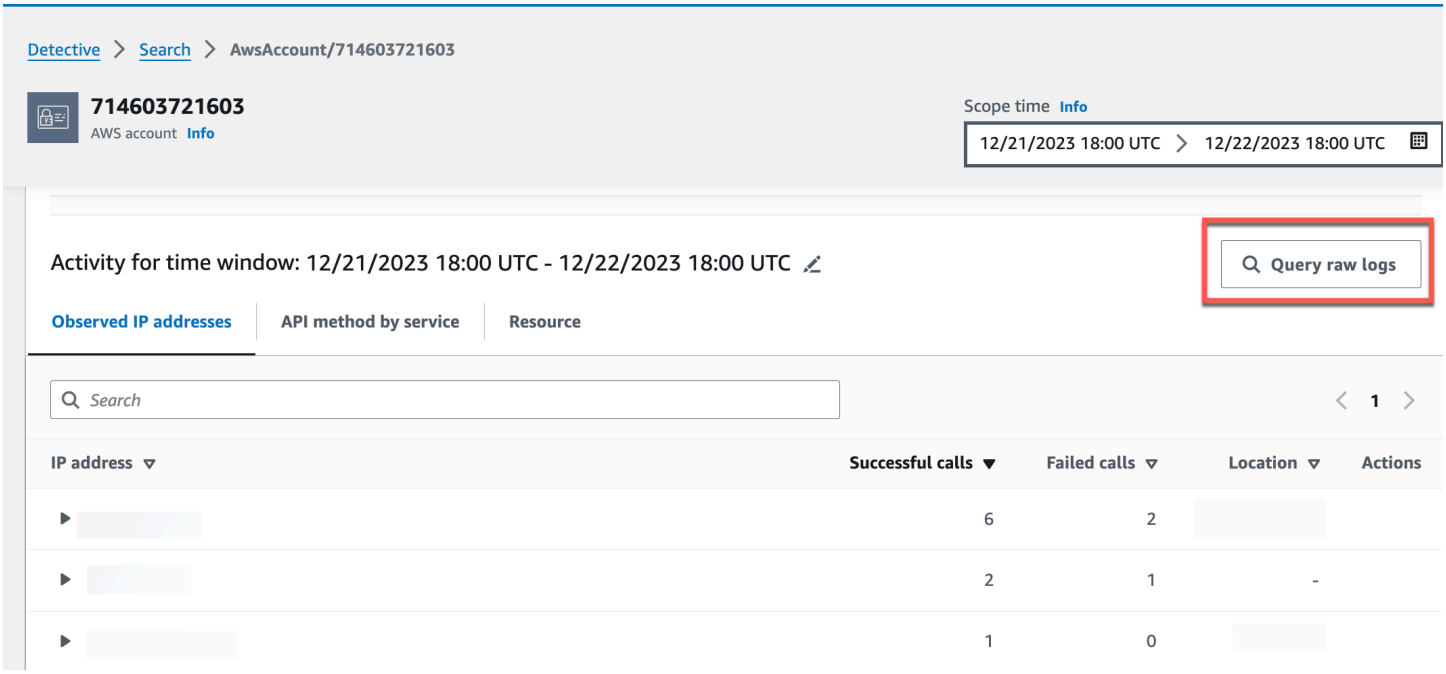
Amazon VPC フローログは、以下のプロファイルで使用できます。

- Amazon EC2 インスタンス
- Kubernetes ポッド

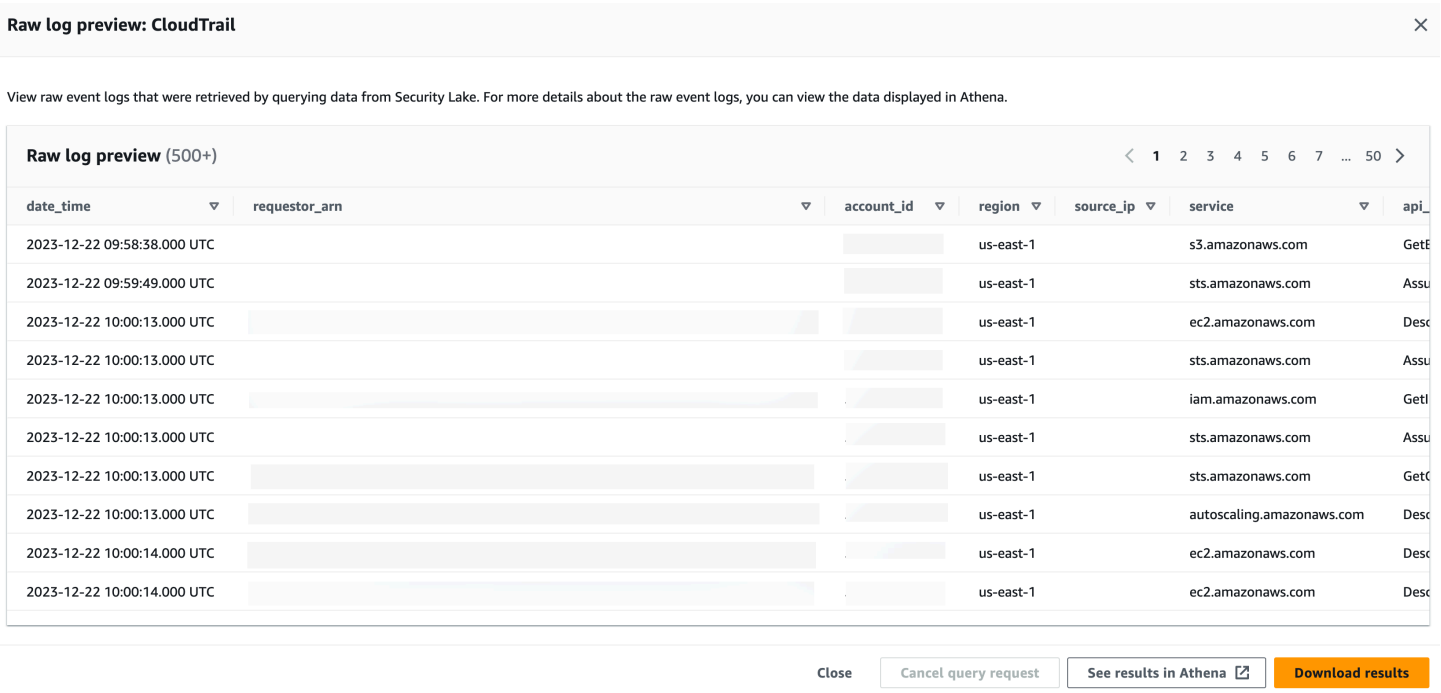
Detective コンソールを使用して Amazon Detective を Amazon Security Lake と統合する方法のデモンストレーションについては、次の動画をご覧ください。Amazon Detective と Amazon Security Lake の統合 - 使用方法

AWS アカウントの未処理のログのクエリを実行するには

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで、[検索] を選択して `AWS account` を検索します。
3. [全体的な API 呼び出し量] セクションで、スコープ時間の詳細表示を選択します。
4. ここで、[未処理のログをクエリ] を開始できます。



[未処理のログのプレビュー] テーブルでは、Security Lake からのデータのクエリを実行して取得したログとイベントを表示できます。未処理のイベントログの詳細については、Amazon Athena に表示されるデータを確認してください。



[未処理のログをクエリ] テーブルで、[クエリリクエストをキャンセル]、[Amazon Athena で結果を表示]、[結果をダウンロード] (カンマ区切り値 (.csv) ファイル) を実行できます。

Detective にログが表示されるにもかかわらず、クエリで結果が返されない場合は、次の理由が考えられます。

- 未処理のログは、Security Lake のログテーブルに表示される前に、Detective で利用できるようになる場合があります。後ほどもう一度試してください。」
- Security Lake ログが欠落している可能性があります。長時間待った場合は、Security Lake でログが欠落していることを示しています。Security Lake 管理者に連絡して、問題を解決してください。

例

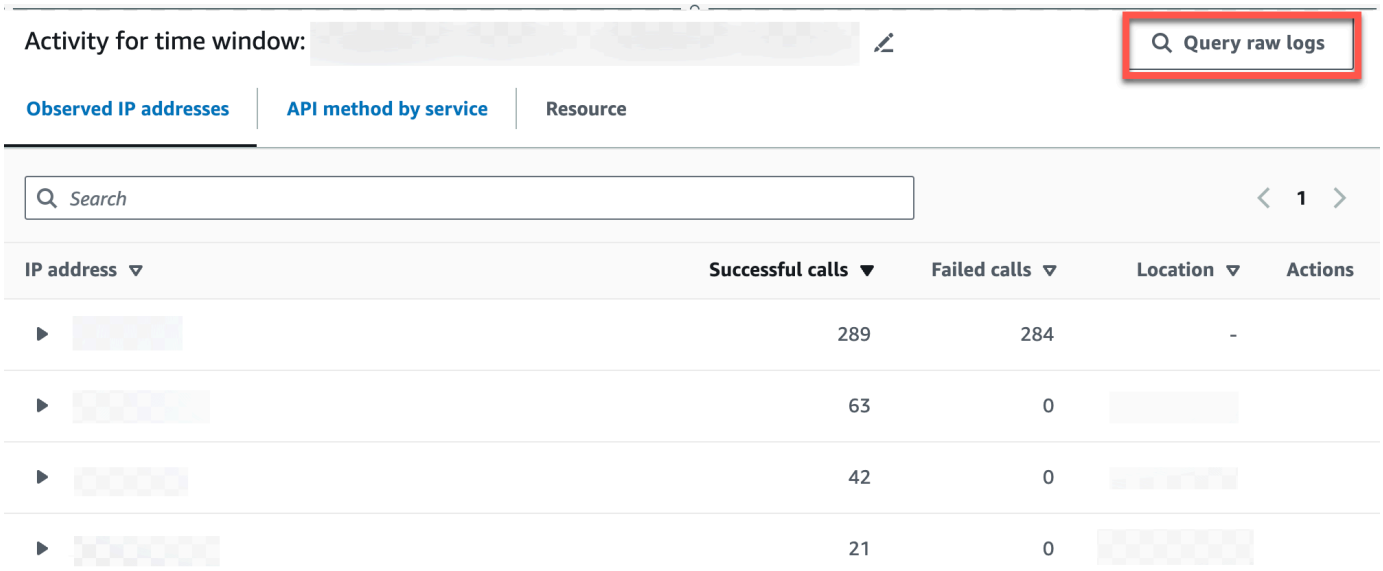
- AWS ロールの raw ログをクエリする
- Amazon EKS クラスターの raw ログをクエリする
- Amazon EC2 インスタンスの未処理ログのクエリの実行

AWS ロールの raw ログをクエリする

新しい位置情報での AWS ロールのアクティビティを把握したい場合は、Detective コンソールで確認できます。

AWS ロールの未処理のログのクエリを実行するには

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. Detective Summary ページ「新しく観測された位置情報」セクションで、 AWS ロールを書き留めます。
3. ナビゲーションペインで、[検索] を選択して `AWS role` を検索します。
4. AWS ロールでは、リソースを展開して、そのリソースによってその IP アドレスから発行された特定の API コールを表示します。
5. 調査する API コールの横にある拡大鏡アイコンを選択し、[未処理のログのプレビュー] テーブルを開きます。

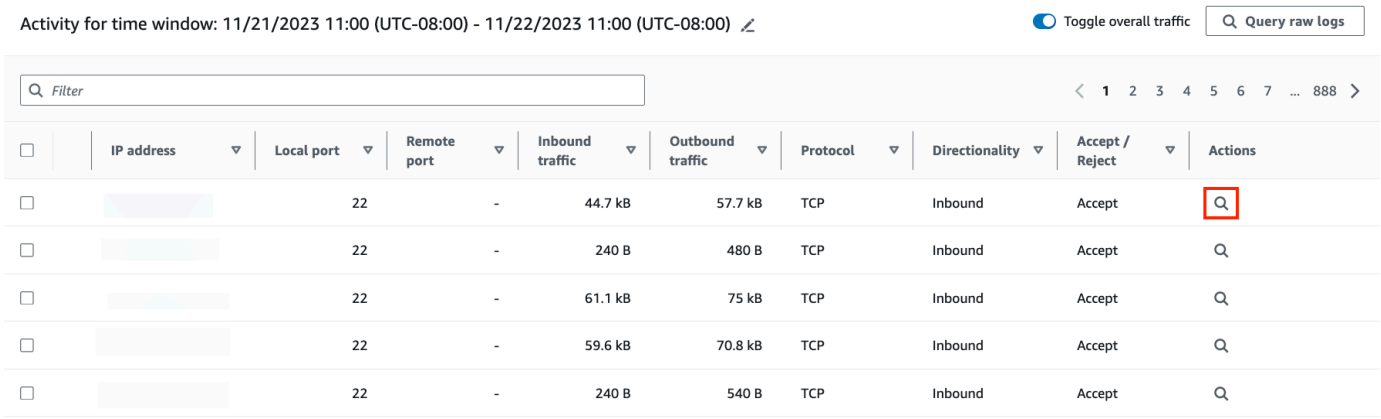


Amazon EKS クラスターの raw ログをクエリする

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. 「Detective Summary」ページ「最も多くポッドが作成されたコンテナクラスター」セクションから、Amazon EKS クラスターに移動します。
3. Amazon EKS クラスターの詳細ページで、Kubernets API アクティビティタブを選択します。
4. この Amazon EKS クラスターに関連する全体的な Kubernets API アクティビティセクションで、スコープ時間の詳細の表示を選択します。
5. ここで、[未処理のログをクエリ] を開始できます。

Amazon EC2 インスタンスの未処理ログのクエリの実行

1. https://console.aws.amazon.com/detective/ で Detective コンソールを開きます。
2. ナビゲーションペインで、[検索] を選択して `Amazon EC2 instance` を検索します。
3. [全体的な VPC フロー量]ペインで、調査する API コールの横にある拡大鏡アイコンを選択し、[未処理のログのプレビュー] テーブルを開きます。
4. ここで、[未処理のログをクエリ] を開始できます。



[未処理のログのプレビュー] テーブルでは、Security Lake からのデータのクエリを実行して取得したログとイベントを表示できます。未処理のイベントログの詳細については、Amazon Athena に表示されるデータを確認してください。

[未処理のログをクエリ] テーブルで、[クエリリクエストをキャンセル]、[Amazon Athena で結果を表示]、[結果をダウンロード] (カンマ区切り値 (.csv) ファイル) を実行できます。

Amazon Detective のセキュリティ

AWS クラウドセキュリティは最優先事項です。 AWS 顧客は、最もセキュリティに敏感な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の恩恵を受けることができます。

セキュリティは、 AWS お客様とお客様との間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内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 AWS AWS クラウド内で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があります。 AWS また、安全に使用できるサービスも提供します。

  AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。

  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。
- クラウドのセキュリティ — お客様の責任は、 AWS 使用するサービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、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 AWS リソースの監視と保護に役立つ他のサービスの使い方についても学びます。

コンテンツ

Amazon Detective でのデータ保護

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

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

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

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

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。

コンテンツ

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。AWSAWS Key Management Service 開発者ガイドの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、1 年 (約 365 日) ごとに自動的にローテーションします。『AWS Key Management Service 開発者ガイド』のキー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、 AWS のサービス AWS 管理者がリソースへのアクセスを安全に制御できるようにするものです。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 AWS のサービス は追加料金なしで使用できるアプリです。

コンテンツ

対象者

AWS Identity and Access Management (IAM) の使用方法は、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 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。サービスのユーザーがどの Detective 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。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 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 を参照してください。

アイデンティティを使用した認証

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

ID ソースを通じて提供された認証情報を使用して、フェデレーション ID AWS としてサインインできます。 AWS IAM Identity Center フェデレーテッド ID の例としては、(IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google や Facebook の認証情報などがあります。フェデレーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。 AWS フェデレーションを使用してアクセスすると、間接的にロールを引き継ぐことになります。

ユーザーのタイプによっては、 AWS Management Console AWS またはアクセスポータルにサインインできます。へのサインインについて詳しくは AWS、『AWS サインイン ユーザーガイド』の「AWS アカウントにサインインする方法」を参照してください。

AWS プログラムからアクセスする場合は、認証情報を使用してリクエストに暗号署名するためのソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨方法を使用して自分

でリクエストに署名する方法の詳細については、IAM ユーザーガイドの「 AWS API リクエストへの署名」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、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) AWS を使用することを推奨しています。詳細については、『AWS IAM Identity Center ユーザーガイド』の「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」を参照してください。

AWS アカウント root ユーザー

を作成するときは AWS アカウント、 AWS のサービス アカウント内のすべてのリソースに完全にアクセスできる 1 つのサインイン ID から始めます。この ID は AWS アカウント root ユーザーと呼ばれ、アカウントの作成に使用したメールアドレスとパスワードでサインインすることでアクセスされます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して特定の権限を持つ社内の AWS アカウント ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

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

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳

細については、『IAM ユーザーガイド』の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、 AWS アカウント 特定の権限を持つ社内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。 AWS Management Console ロールを切り替えることで、の IAM ロールを一時的に引き受けることができます。 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 を使用してロールを引き受けることができます。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」 を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、ロールをプロキシとして使用する代わりに AWS のサービス、ポリシーをリソースに直接アタッチできるものもあります。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 — AWS のサービス AWS のサービス他の機能を使用するものもあります。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。

- 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、あなたはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 AWS のサービス を呼び出したプリンシパルの権限をリクエスト元と組み合わせて使用して AWS のサービス、ダウンストリームサービスにリクエストを行います。FASリクエストは、AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、『IAM ユーザーガイド』の「AWS のサービスに権限を委任するロールの作成」を参照してください。
- サービスにリンクされたロール — サービスにリンクされたロールは、にリンクされているサービスロールの一種です。 AWS のサービスサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。 AWS アカウント サービスにリンクされたロールはに表示され、そのサービスが所有します。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

- Amazon EC2 で実行されるアプリケーション — IAM ロールを使用して、EC2 インスタンスで実行され、 AWS API AWS CLI リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 AWS インスタンスにロールを割り当て、そのロールを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るインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

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

ポリシーを使用したアクセスの管理

AWS ポリシーを作成して AWS ID またはリソースにアタッチすることで、アクセスを制御します。ポリシーとは、ID またはリソースに関連付けると権限を定義するオブジェクトです。 AWS AWS プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決

まります。ほとんどのポリシーは JSON AWS ドキュメントとして保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

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

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

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

アイデンティティベースのポリシー

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

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

リソースベースのポリシー

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

リンシパルには、アカウント、ユーザ、ロール、フェデレーティッドユーザ、またはを含めることができます。 AWS のサービス

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。IAM AWS の管理ポリシーをリソースベースのポリシーで使用することはできません。

アクセスコントロールリスト (ACL)

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

ACL をサポートするサービスの例としては AWS WAF、Amazon S3、、および Amazon VPC があります。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 あまり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権限を設定できます。

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

リシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

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

Amazon Detective で IAM が機能する仕組み

デフォルトでは、ユーザーおよびロールには、Amazon Detective リソースを作成または変更する許可はありません。また、 AWS Management Console AWS CLI、または AWS API を使用してタスクを実行することもできません。Detective 管理者は、IAM ユーザーとロールに、必要な指定されたリソースに対して特定の API 操作を実行する権限を付与する AWS Identity and Access Management (IAM) ポリシーを持っている必要があります。続いて、管理者はそれらのアクセス許可が必要なプリンシパルに、そのポリシーをアタッチしなければなりません。

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ができます。管理者アカウントは、ビヘイビアグラフを使用して、それらのアカウントに関連する結果やリソースの優先順位付けや調査を行うこともできます。

  管理者アカウントでないユーザーが異なるタイプのタスクを実行できるようにす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 などが IAM AWS のサービス とどのように連携するかを大まかに把握するには、『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。

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 ポリシー要素のリファレンス」を参照してください。

アクション

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

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

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

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んなリソースにどんな条件でアクションを実行できるかということです。

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

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

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

ARN の形式の詳細については、「Amazon リソースネーム (ARN) AWS とサービス名前空間」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"
]
```

たとえば、 AWS 同じアカウントが複数の動作グラフのメンバーアカウントに招待される場合があります。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んなリソースにどんな条件でアクションを実行できるかということです。

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

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

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

AWS グローバル条件キーとサービス固有の条件キーをサポートします。 AWS すべての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。 AWS すべての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 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” を参照してください。

Detective IAM ロール

IAM ロールは、 AWS 特定の権限を持つアカウント内のエンティティです。

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は、AWS STS AssumeRoleGetFederationTokenやなどの API オペレーションを呼び出して取得します。

Detective では、一時認証情報の使用をサポートしています。

サービスリンクロール

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

サービスにリンクされた Detective の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”」を参照してください。

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

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。また、 AWS Management Console AWS CLI、または AWS API を使用してタスクを実行することもできません。

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権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。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 ベースのポリシーは、ユーザーのアカウントで誰かが Detective リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーから始めて、最小権限の権限に移行する — ユーザーとワークロードへの権限の付与を開始するには、AWS 多くの一般的なユースケースで権限を付与する管理ポリシーを使用してください。これらのポリシーは、で利用できます。 AWS アカウント AWS ユースケースに固有のカスタマー管理ポリシーを定義して、権限をさらに減らすことをお勧めします。詳細については、『IAM ユーザーガイド』の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権権限とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。サービスアクションがなどの特定の用途で使用された場合は AWS のサービス、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 AWS CloudFormation。詳細については、『IAM ユーザーガイド』の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語

(JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、『IAM ユーザーガイド』の「IAM Access Analyzer ポリシーの検証」を参照してください。

- 多要素認証 (MFA) が必要 — IAM ユーザーまたは root ユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA をオンにしてください。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アタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、またはまたは API を使用してこのアクションを完了するための権限が含まれています。 AWS CLI AWS

```
{
    "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:DeleteG
    "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"}
        }
    } ]
}
```

AWS Amazon Detective の管理ポリシー

AWS 管理ポリシーは、によって作成および管理されるスタンドアロンのポリシーです。 AWS AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス権限を割り当てることができるように、多くの一般的な使用事例にアクセス許可を与えるように設計されています。

AWS 管理ポリシーでは、 AWS すべての顧客が使用できるようになっているため、特定のユースケースでは最小権限のアクセス権限が付与されない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されている権限は変更できません。 AWS 管理ポリシーで定義されている権限を更新すると AWS 、その更新はポリシーがアタッチされているすべてのプリンシパル ID (ユー

ザー、グループ、ロール) に影響します。 AWS AWS 管理ポリシーが更新される可能性が最も高いのは、新しい API 操作が既存のサービスで開始されたときや、新しい API AWS のサービス 操作が使用可能になったときです。

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」を参照してください。

AWS 管理ポリシー:AmazonDetectiveFullAccess

`AmazonDetectiveFullAccess` ポリシーは IAM ID にアタッチできます。

このポリシーは、プリンシパルにすべての Amazon 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。ユーザーは、アカウントで Detective を有効にする前に、このポリシーを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。また、 GuardDuty 調査結果をアーカイブすることもできます。このポリシーは、Detective コンソールが登録されているアカウントのアカウント名を表示するために必要な権限を提供します。 AWS Organizations

許可の詳細

このポリシーには、以下の許可が含まれています。

- `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、これらのアクセス許可は、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`— 校長が Detective GuardDuty 内から調査結果を取得してアーカイブできるようにします。
- `securityhub` — プリンシパルが Detective 内から Security Hub からの検出結果を取得することを許可します。

```
{
    "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:GetFindings",
                "guardduty:ListDetectors"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "securityHub:GetFindings"
            ],
            "Resource": "*"
         }
    ]
}
```

AWS 管理ポリシー:AmazonDetectiveMemberAccess

IAM エンティティに、AmazonDetectiveMemberAccess ポリシーをアタッチできます。

このポリシーは、Amazon Detective へのメンバーアクセスと、コンソールへのスコープ付きアクセスを提供します。

このポリシーにより、以下のことが可能になります。

- Detective グラフメンバーシップへの招待を表示し、招待を承諾または拒否できます。
- Detective でのアクティビティがこのサービスの使用コストにどのように影響するかについて、[使用状況] ページで確認できます。
- メンバーシップからの脱退をグラフで確認できます。

このポリシーは、Detective コンソールへのスコープ付きアクセスを可能にする読み取り専用アクセス許可を付与します。

許可の詳細

このポリシーには、以下の許可が含まれています。

- `detective` — メンバーが Detective にアクセスできるようにします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS マネージドポリシー: AmazonDetectiveInvestigatorAccess

IAM エンティティに AmazonDetectiveInvestigatorAccess ポリシーをアタッチできます。

このポリシーは、調査員に Detective サービスへのアクセスと、Detective コンソール UI の依存関係へのスコープ付きアクセスを提供します。このポリシーによって、Detective で Detective 調査を有効にする権限が IAM ユーザーと IAM ロールに付与されます。セキュリティ指標に関する分析と洞察を提供する調査レポートを使用して、検出結果などの侵害の指標を特定できます。このレポートは、Detective の行動分析と機械学習を使用して確定された重要度別にランク付けされています。このレポートを使用すると、リソースの修復の優先順位を付けることができます。

許可の詳細

このポリシーには、以下の許可が含まれています。

- detective — プリンシパルが Detective アクションにアクセスすることを許可し、Detective の調査を有効にするとともに、検出結果グループの概要を有効化できます。
- guardduty— 校長が Detective GuardDuty 内から調査結果を取得してアーカイブできるようにします。
- securityhub — プリンシパルが Detective 内から Security Hub からの検出結果を取得することを許可します。
- organizations— プリンシパルが組織内のアカウントに関する情報をそこから取得できるようにします。 AWS Organizations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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
```

```
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
```

```
        "securityHub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 管理ポリシー: AmazonDetectiveOrganizationsAccess

IAM エンティティに AmazonDetectiveOrganizationsAccess ポリシーをアタッチできます。

このポリシーは、組織内で Amazon Detective を有効化および管理するためのアクセス許可を付与します。Detective を組織全体で有効にし、Detective の委任された管理者アカウントを決定できます。

許可の詳細

このポリシーには、以下の許可が含まれています。

- detective – プリンシパルに Detective のアクションへのアクセスを許可します。
- iam— Detective がEnableOrganizationAdminAccount を呼び出したときに、サービスリンクロールが作成されるように指定します。
- organizations— AWS Organizationsプリンシパルが組織内のアカウントに関する情報をから取得できるようにします。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。 AWS サービスの統合を有効にし、指定されたメンバーアカウントを委任管理者として登録および登録解除できるようにします。また、プリンシパルが Amazon Detective、Amazon、Amazon、Amazon Macie などの他のセキュリティサービスの委任管理者アカウントを取得できるようにします。 GuardDuty AWS Security Hub

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

```
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

AWS マネージドポリシー: AmazonDetectiveServiceLinkedRole

IAM エンティティに AmazonDetectiveServiceLinkedRole ポリシー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、サービスリンク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”」を参照してください。

このポリシーは、サービスリンクロールが組織のアカウント情報を取得できるようにする管理アクセス許可を付与します。

許可の詳細

このポリシーには、以下の許可が含まれています。

- 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:DescribeAccount",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 管理ポリシーのDetective アップデート

このサービスが変更の追跡を開始して以降の Detective AWS の管理ポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、「 ドキュメン履歴ページ」ページで RSS フィードをサブスクライブしてください。

変更	説明	日付
AmazonDetectiveInvestigatorAccess - 既存のポリシーの更新	Detective の調査と検出結果グループの概要アクションを AmazonDetectiveInvestigatorAccess ポリシーに追加しました。 これらのアクションにより、Detective 調査の開始、取得、更新が可能になり、Detective 内から検出結果グループの概要を取得できます。	2023 年 11 月 26 日
AmazonDetectiveFullAccess と AmazonDetectiveInvestigatorAccess — 既存のポリシーに対する更新	Detective の AmazonDetectiveFullAccess および AmazonDetectiveInvestigatorAccess ポリシーに Security Hub GetFindings アクションを追加されました。 これらのアクションにより、Detective 内から、Security Hub からの検出結果を取得できます。	2023 年 5 月 16 日

変更	説明	日付
AmazonDetectiveOrganizationsAccess - 新しいポリシー	Detective に AmazonDetectiveOrganizationsAccess ポリシーが追加されました。 このポリシーは、組織内で Detective を有効化および管理するためのアクセス許可を付与します。	2023 年 3 月 2 日
AmazonDetectiveMemberAccess - 新しいポリシー	Detective に AmazonDetectiveMemberAccess ポリシーが追加されました。 このポリシーは、メンバーが、Detective にアクセスできるようにするとともにコンソール UI の依存関係にスコープ付きでアクセスできるようにします。	2023 年 1 月 17 日
AmazonDetectiveFullAccess – 既存ポリシーの更新	Detective GuardDuty GetFindings AmazonDetectiveFullAccess がポリシーにアクションを追加しました。 これらのアクションにより、Detective GuardDuty 内から結果を取得できます。	2023 年 1 月 17 日
AmazonDetectiveInvestigatorAccess - 新しいポリシー	Detective に AmazonDetectiveInvestigatorAccess ポリシーが追加されました。 このポリシーにより、プリンシパルは Detective で調査を行うことができます。	2023 年 1 月 17 日

変更	説明	日付
AmazonDetectiveServiceLinkedRole - 新しいポリシー	Detective で、サービスリンクロールに新しいポリシーが追加されました。 このポリシーは、サービスリンク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 AWS は管理ポリシーの変更を追跡し始めました。	2021 年 5 月 10 日

Detective のサービスリンクロールの使用

Amazon Detective は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスリンクロールは、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、サービスがユーザーに代わって他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスリンクロールを使用すると、必要な設定を手動で追加する必要がないため、 Detective の設定が簡単になります。Detective は、サービスリンク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。定義したアクセス許可には、信頼ポリシーと許可ポリシーが含まれます。この許可ポリシーを他の IAM エンティティにアタッチ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、Detective リソースへの意図しないアクセスによる許可の削除が防止され、 リソースは保護されます。

サービスリンク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「サービスリンクロール」列が「はい」になっているサービスを検索してください。サービスのサービスリンクロールに関するドキュメンテーションを表示するには、[Yes] (はい) リンクを選択します。

Detective のサービスリンクロールにおけるアクセス許可

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AWSServiceRoleForDetective。これにより、Detective がユーザーに代わって AWS Organizations 情報にアクセスできるようになります。

AWSServiceRoleForDetective サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `detective.amazonaws.com`

AWSServiceRoleForDetective サービスにリンクされたロールは、 マネージドポリシー を使用しますAmazonDetectiveServiceLinkedRolePolicy。

AmazonDetectiveServiceLinkedRolePolicy ポリシーの更新の詳細については、「Amazon Detective updates to AWS managed policies」を参照してください。このポリシーの変更に関する自動アラートについては、Detective ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

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、アクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスリンクロールのアクセス権限) を参照してください。

Detective のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。、 AWS Management Console、 AWS CLIまたは AWS API で組織の 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作成されます。

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 により、サービスリンクロールが再び自動的に作成されます。

Detective のサービスリンクロールの編集

Detective では、 AWSServiceRoleForDetective サービスにリンクされた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した後は、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「サービスリンクロールの編集」を参照してください。

Detective のサービスリンクロールの削除

サービスリンクロールが必要な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、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。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 のサービスでこの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、数分待ってから操作を再試行してください。

が使用する Detective リソースを削除するには AWSServiceRoleForDetective

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” 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。

サービスにリンクされたロールを IAM で手動削除するには

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

Detective のサービスリンクロールをサポートするリージョン

Detective は、Detective サービスが利用可能なすべてのリージョンで、サービスリンク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 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。 AWS Identity and Access Management(IAM) を使用する際にアクセス拒否の問題や同様

の問題が発生した場合は、IAM ユーザーガイドの「IAM のトラブルシューティング」トピックを参照してください。

Detective でアクションを実行する権限がない

アクションを実行する権限がないと表示された場合、管理者に連絡して支援を受ける必要があります。 AWS Management Console 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。

私には IAM を実行する権限がありません:PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Detective にロールを渡すことができるようにする必要があります。

新しいサービスロールやサービスにリンクされたロールを作成する代わりに、 AWS のサービス 既存のロールをそのサービスに渡すことができるものもあります。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、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権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

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

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

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

AWS 自分のアカウント外の人が私のDetective リソースにアクセスできるようにしたい

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

詳細については、以下を参照してください:

- 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 を参照してください。
- AWS アカウント 所有しているリソース全体のリソースへのアクセスを提供する方法については、『IAM ユーザーガイド』の「AWS アカウント 所有する別の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスを第三者に提供する方法については AWS アカウント、IAM ユーザーガイドの「AWS アカウント 第三者が所有するリソースへのアクセスの提供」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「外部で認証されたユーザー (ID フェデレーション) へのアクセス権限」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Amazon Detective でのログ記録とモニタリング

Amazon Detective が統合されています AWS CloudTrail。 CloudTrail 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 CloudTrail のロギングの使用方法の詳細については、を参照してくださいthe section called “によるDetective API 呼び出しのロギング CloudTrail”。

Amazon Detective のコンプライアンス検証

Amazon Detective AWS は保証プログラムの対象です。詳細については、「Health Information Trust Alliance Common Security Framework (HITRUST) CSF」「」を参照してください。

AWS 特定のコンプライアンスプログラムの対象となる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別の AWS 対象範囲内 」を参照してください。一般的な情報については、「AWS」を参照してください。

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

AWS には、コンプライアンスに役立つ以下のリソースが用意されています。

- 「セキュリティ & コンプライアンスクイックリファレンスガイド」 – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、 AWSでセキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイするための手順が記載されています。
- AWS Config 開発者ガイドのルールに基づくリソースの評価 — AWS Config このサービスでは、リソース構成が社内慣行、業界のガイドライン、規制にどの程度準拠しているかを評価します。
- AWS Security Hub— AWS このサービスでは、内部のセキュリティ状態を包括的に把握できるため、 AWS セキュリティ業界の標準やベストプラクティスに準拠しているかどうかを確認できます。

Amazon Detective の回復力

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

AWS リージョンとアベイラビリティーゾーンの詳細については、「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

Detective は、 AWS グローバルインフラストラクチャに加えて、Amazon DynamoDB と Amazon Simple Storage Service (Amazon S3) に組み込まれている耐障害性を利用しています。

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

Amazon Detective; はマネージド型サービスであり、 AWS グローバルネットワークセキュリティによって保護されています。 AWS AWS セキュリティサービスとインフラストラクチャを保護する方法については、「AWS クラウドセキュリティ」を参照してください。 AWS インフラストラクチャセキュリティのベストプラクティスを使用して環境を設計するには、「Security Pillar AWS Well-Architected Framework におけるインフラストラクチャ保護」を参照してください。

AWS 公開されている API 呼び出しを使用して、ネットワーク経由で Detective; にアクセスします。クライアントは以下をサポートする必要があります:

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

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

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を説明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必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な考慮事項とお考えください。

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。

招待状を送信した管理者アカウントのアカウント識別子を確認してください。 AWS 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 コストの予測とモニタリング

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。

Detective AWS CloudTrail はロギングもサポートしています。

コンテンツ

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されます。

- アカウントで Detective を手動で有効にし、そのアカウントが動作グラフの管理者アカウントになった場合。
- アカウントが AWS Organizations内の組織の Detective 管理者アカウントとして指定され、Detective が初めて有効になった場合。
- Detective 管理者アカウントが指定される前に既に Detective が有効になっていた場合。その場合、そのアカウントでもう 30 日間の無料トライアルが開始されることはありません。
- アカウントが、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になった場合。
- 組織アカウントが Detective 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た場合。

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。Detective のアクティビティを追跡する方法、使用状況を監視する方法、予測コストを確認する方法については、「Amazon Detective コストの予測とモニタリング」を参照してください。料金の詳細については、「Detective の料金」を参照してください。

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”」および「the section called “メンバーアカウントの使用量の追跡”」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 では、オプションのデータソースを 30 日間無料で試用することもできます。この無料トライアルは、Detective を初めて有効にしたときにコア Detective データソース用に提供されていた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 日以内に無効にした場合、Detective は、そのデータソースパッケージが再び有効にされたとき、そのデータソースパッケージの無料トライアルを 1 回だけ自動的にリセットします。

オプションのデータソースパッケージを有効または無効にする方法については、「Detective のオプションデータソースのタイプ」を参照してください。

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。

管理者アカウントは、Detective コンソールの [使用状況] ページで、過去 30 日間に取り込まれたデータ量を [データソース別]または [アカウント別] に表示できます。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. [データソース別] タブか [アカウント別] タブを選択して、使用状況をいずれかで表示します。

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ルート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” 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” を参照してください。

ソースパッケージ別に取り込まれたデータ量

[ソースパッケージ別] を選択すると、取り込まれたデータ量が、動作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別にリスト表示されます。

すべてのアカウントが、自身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、メンバーごとの使用状況をソースパッケージ別にリスト表示する追加のパネルも表示することができます。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、過去 30 日間にDetective コアソース (CloudTrail ログ、VPC フローログ、 GuardDuty 結果) から取り込まれたデータ量が表示されます。

EKS 監査ログ

EKS 監査ログのパネルには、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量が表示されます。このソースパッケージのパネルは、動作グラフで EKS 監査ログが有効になっている場合にのみ表示されます。

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”」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。
4. 共有 Amazon VPC を使用している場合、Detective はモニタリングアクティビティに基づいて予測コストを計算します。環境固有の調査にかかる予測コストについては、確認することをお勧めします。
   a. Detective メンバーアカウントに共有 Amazon VPC が含まれており、その共有 VPC を使用している他の非 Detective アカウントがある場合、Detective はその VPC からのすべてのトラフィックを監視します。使用量とコストが増加し、Detective は VPC 内のすべてのトラフィックフローを視覚化します。
   b. 共有 Amazon VPC 内に EC2 インスタンスがあり、共有所有者が Detective メンバーでない場合、Detective は VPC からのトラフィックをモニタリングしないため、使用量とコストが削減されます。VPC 内のトラフィックフローを表示する場合は、Amazon VPC 所有者を Detective グラフのメンバーとして追加する必要があります。

での Amazon Detective API 呼び出しの口ギング AWS CloudTrail

Detective は AWS CloudTrail、Detective 内のユーザー、ロール、 AWS またはサービスが実行したアクションの記録を提供するサービスと統合されています。 CloudTrail 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。

- 証跡を作成すると、Detective CloudTrail のイベントを含むイベントを Amazon S3 バケットに継続的に配信できるようになります。
- トレイルを設定しなくても、 CloudTrailコンソールの [イベント履歴] で最新のイベントを確認できます。

によって収集された情報を使用して CloudTrail、次のことを判断できます。

- 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

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

のDetective 情報 CloudTrail

CloudTrail アカウントを作成すると、 AWS その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、 CloudTrail AWS そのアクティビティは他のサービスイベントとともにイベント履歴に記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「 CloudTrail イベント履歴によるイベントの表示」を参照してください。

Detective のイベントなど、 AWS アカウント内のイベントを継続的に記録するには、トレイルを作成してください。トレイルを使用すると CloudTrail 、Amazon S3 バケットにログファイルを配信できます。

デフォルトでは、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。トレイルは、 AWS パーティション内のすべてのリージョンからのイベントを記録し、指定した Amazon S3 バケットにログファイルを配信します。また、 AWS CloudTrail ログに収集されたイベントデータをさらに分析して処理するように他のサービスを設定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:

- 証跡の作成のための概要
- CloudTrail サポート対象のサービスとインテグレーション
- の Amazon SNS 通知の設定 CloudTrail
- CloudTrail 複数のリージョンからのログファイルの受信、 CloudTrail 複数のアカウントからのログファイルの受信

CloudTrail Detective API リファレンスに記載されているすべての検出操作を記録します。

たとえば、、`DeleteMembers`オペレーションを呼び出す
と`CreateMembersAcceptInvitation`、ログファイルにエントリが生成されます。 CloudTrail

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

- リクエストが root ユーザー認証情報または AWS Identity and Access Management (IAM) ユーザー認証情報のどちらで行われたか

- 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
- AWS リクエストが別のサービスによって行われたかどうか

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

Detective のログファイルエントリの理解

トレイルは、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。

イベント は、任意の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 呼び出しの順序付けられたスタックトレースではないため、エントリが特定の順序で表示されることはありません。

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


```
      {
            "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": []
        },
```

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 AWS リージョン を利用できる場所のリストについては、「Detective サービスのエンドポイント」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 9 TB	動作グラフのデータ量が 1 日あたり 9 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 10 TB	動作グラフのデータ量が 1 日あたり 10 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 15 TB	動作グラフのデータ量が 1 日あたり 15 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 15 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。

リソース	クォータ	コメント
		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。

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” 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。たとえば、セキュリティに関連するコストを追跡するために、Detective の行動グラフ、 AWS Security Hub ハブリソース、Amazon GuardDuty ディテクターに同じタグを割り当てることができます。で AWS Cost Explorer、そのタグを検索すると、それらのリソース全体のコストがまとめて表示されます。

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. https://console.aws.amazon.com/detective/ で Amazon 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 またはを使用して、 AWS Command Line Interface 行動グラフのタグのリストを取得できます。

挙動グラフ (Detective API) のタグのリストを取得するには AWS CLI

- Detective API: `ListTagsForResource` オペレーションを使用します。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。

行動グラフへのタグの追加 (Detective API、 AWS CLI)

Detective API またはを使用して、 AWS CLI 行動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: `TagResource` オペレーションを使用します。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 またはを使用して、 AWS CLI 行動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: `UntagResource` オペレーションを使用します。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。

コンテンツ

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。

Amazon ディDetective を無効にするには (コンソール)

1. https://console.aws.amazon.com/detective/ で Amazon 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、[設定] の [全般] を選択します。
3. 「一般」ページの「Amazon Detective を無効にする」で、「Amazon Detective を無効にする」を選択します。
4. 確認を求められたら、**`disable`** と入力します。
5. 「Amazon Detective を無効にする」を選択します。

ディDetective を無効にする (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` オペレーションを使用します。

Detective (Detective API) を無効にするには、 AWS CLI

- Detective API: `DeleteGraph` オペレーションを使用します。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
```

リージョン間でのディDetective の無効化 (Python スクリプトオン) GitHub

Detective GitHub が提供しているオープンソーススクリプトを使用すると、指定したリージョンのリストで管理者アカウントの Detective を無効にできます。

GitHub スクリプトの設定方法および使用方法については、を参照してください。the section called “Amazon Detective の Python スクリプト”

Detective ユーザーガイドのドキュメント履歴

次の表に、Detective の前回のリリース以後に行われた、ドキュメントの重要な変更を示します。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

- ドキュメントの最終更新日： 2024 年 5 月 15 日

変更	説明	日付
新しい Security Lake ソースバージョン	ソースバージョン 1 (OCSF 1.0.0-rc.2) に加えて、Detective はソースバージョン 2 (OCSF 1.1.0) から、Detective でサポートされている Security Lake ソースのデータを取り込むようになりました。	2024 年 5 月 15 日
新しい Security Lake ログソース	Detective と Security Lake の統合を使用して、Amazon EKS 監査ログ からログとイベントを収集できます。	2024 年 5 月 15 日
ドキュメントの更新	Amazon Detective 管理ガイドのコンテンツが Amazon Detective ユーザーガイドに統合されました。Amazon Detective 管理ガイドは、2024 年 5 月 8 日に標準サポートを終了します。	2024 年 4 月 15 日
Amazon の検出結果のサポートを追加 GuardDuty	Detective では、次の GuardDuty Runtime Monitoring の検出結果タイプがサポートされるようになりました。 `Execution:Runtime/Malicious`	2024 年 4 月 5 日

	FileExecuted Execution:Runtime/SuspiciousTool DefenseEvasion:Runtime/PtraceAntiDebugging Execution:Runtime/SuspiciousCommand DefenseEvasion:Runtime/SuspiciousCommand	
Amazon GuardDuty メンバーシップ要件を削除しました	Amazon Detective を有効にするために GuardDuty 、顧客になる必要がなくなりました。Detective GuardDuty を有効にする前に、アカウントで を 48 時間有効にする要件は削除されました。	2024 年 2 月 21 日
Amazon の検出 GuardDuty 結果のサポートを追加	Detective は、GuardDuty EC2 Runtime Monitoring の検出結果タイプのサポートを ECS および EC2 リソースに拡張します。	2024 年 1 月 30 日

更新された機能	調査する特定のリソースについて、調査ページから Detective 調査を実行できるようになりました。Detective では、検出結果と検出結果グループでのアクティビティに基づいてリソースを推奨します。Detective Investigations を使用すると、侵害の指標を含む IAM ユーザーと IAM ロールを調査できます。これにより、リソースがセキュリティインシデントに関与しているかどうかを判断できます。	2024 年 1 月 16 日
更新された機能	推奨リソースの調査ページから Detective 調査を実行できるようになりました。Detective では、検出結果と検出結果グループでのアクティビティに基づいてリソースを推奨します。Detective Investigations を使用すると、侵害の指標を含む IAM ユーザーと IAM ロールを調査できます。これにより、リソースがセキュリティインシデントに関与しているかどうかを判断できます。	2023 年 12 月 26 日

Detective が共有 VPC のフロートラフィックを読み取る方法の変更	共有 Amazon VPC を使用している場合、Detective によって監視されているトラフィックで変化が生じる場合があります。[全体的な VPC フロー量] のアクティビティの詳細の変化を確認してカバレッジへの潜在的な影響を把握し、Detective による予測コストの計算方法を確認して、そのサービスコストへの影響を把握することをお勧めします。	2023 年 12 月 20 日
リージョナルな可用性	Detective と Security Lake の統合が利用可能なリージョンのリストに、欧州 (ストックホルム)、欧州 (パリ)、カナダ (中部) AWS リージョンを追加しました。	2023 年 12 月 8 日
新機能	Detective の調査では、侵害のインジケータを使用して IAM ユーザーと IAM ロールを調査します。これは、リソースがセキュリティインシデントに関与しているかどうかを判断するのに役立ちます。	2023 年 11 月 26 日

新機能	デフォルトで、Detective は生成人工知能 (生成 AI) を活用して、検出結果グループの検出結果グループの概要を自動的に生成します。検出結果グループの概要では、検出結果と影響を受けるリソースとの関係が迅速に分析され、潜在的な脅威が自然言語で要約されています。	2023 年 11 月 26 日
新機能	Security Lake と Detective の統合により、Security Lake に保存されている未加工のログデータを検索して取得できます。この統合を使用すると、CloudTrail 管理イベントと Amazon Virtual Private Cloud (Amazon VPC) フローログからログとイベントを収集できます。	2023 年 11 月 26 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	Detective の調査と検出結果グループの概要アクションを `AmazonDetectiveInvestigatorAccess` ポリシーに追加しました。	2023 年 11 月 26 日
検出結果の概要の表示	検出結果がより大きなアクティビティに関連している場合、その検出結果グループに移動するように Detective から通知されるようになりました。	2023 年 9 月 18 日

Amazon Detective エンドポイントとクォータ	Detective がイスラエル (テルアビブ) リージョンで使用可能になりました。	2023 年 8 月 25 日
検出結果グループの視覚化が強化されました	Detective 検出結果グループの視覚化には、検出結果が集約された検出結果グループが含まれるようになったので、関連する証拠、エンティティ、および検出結果をより効率的に分析できるようになりました。	2023 年 8 月 8 日
検出結果グループ拡張済み	検出結果グループに、Amazon Inspector からの脆弱性検出結果が含まれるようになりました。	2023 年 6 月 13 日
Amazon GuardDuty Lambda Protection のサポートを追加	Detective が GuardDuty Lambda Protection のサポートを提供するようになりました。	2023 年 5 月 26 日
新しいオプションのデータソースパッケージとして AWS セキュリティ検出結果を追加しました。	Detective は、 AWS セキュリティ検出結果をオプションのデータソースパッケージとして提供するようになりました。このオプションのデータソースパッケージにより、Detective は Security Hub からデータを取り込み、そのデータを動作グラフに追加することができます。	2023 年 5 月 16 日

Amazon GuardDuty EKS Runtime Monitoring の検出結果タイプのサポートを追加	Detective で、 GuardDuty EKS Runtime Monitoring の検出結果タイプのサポートが提供されるようになりました。	2023 年 5 月 3 日
Amazon GuardDuty RDS Protection の検出結果タイプのサポートを追加	Detective で GuardDuty RDS Protection の検出結果タイプのサポートが提供されるようになりました。	2023 年 4 月 20 日
追加の Amazon GuardDuty 検出結果タイプのサポートを追加	Detective は、以下の追加の GuardDuty 検出結果タイプのプロファイルを提供するようになりました。 `DefenseEvasion: EC2UnusualDNSResolver` `DefenseEvasion: EvasionEC2UnusualDoHActivity` `DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity`	2023 年 4 月 12 日
Detective コンソールに新しいコンソールパネルが追加されて、ユーザーが特定のユースケースに適した AWS マネージドポリシーを選択できるようになりました。	Detective は安全なマネージドポリシーを提供します。必要なアクセス許可を選択してください。	2023 年 4 月 3 日
EKS クラスターの VPC フロートラフィックを表示する	Amazon Elastic Kubernetes Service (Amazon EKS) クラスターと Amazon Virtual Private Cloud (Amazon VPC) フロートラフィック用に新しいセクションを追加しました。	2023 年 3 月 2 日

検出結果グループで、Detective の動作グラフのダイナミックな視覚表現ができるようになりました	Detective 検出結果グループで、Detective の動作グラフのダイナミックな視覚表現ができるようになったので、検出結果グループ内のエンティティと検出結果との関係を強調表示できるようになりました。	2023 年 2 月 28 日
Detective の [概要] ページと検索結果ページからデータをエクスポートします。データは、カンマ区切り値 (CSV) 形式でエクスポートされます。	Detective に、Detective コンソールからブラウザにデータをエクスポートするオプションが追加されました。	2023 年 2 月 7 日
Amazon Elastic Kubernetes Service (Amazon EKS) ワークロードに全体的な VPC フロー量を追加しました	Detective は、Amazon Elastic Kubernetes Service (Amazon EKS) ワークロードに、Amazon 仮想プライベートクラウド(VPC) フローログに関する視覚的な概要と分析を追加するようになりました。	2023 年 1 月 19 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	Detective は、 AmazonDetectiveFullAccess ポリシーを通じて検出 GuardDuty 結果の取得アクションをサポートするようになりました。セキュリティの章では、Detective: AmazonDetectiveMemberAccess および の新しい管理ポリシーの詳細について説明します AmazonDetectiveInvestigatorAccess。	2023 年 1 月 17 日

データ保持期間が追加されました	Detective を使用すると、最長 1 年間の履歴イベントデータにアクセスできるようになりました。	2022 年 12 月 20 日
[概要] ページに、時間範囲を調整するオプションを追加しました。	Detective で時間範囲を調整して、過去 365 日間の任意の 24 時間枠のアクティビティを表示できるようになりました。	2022 年 10 月 5 日
検出結果またはエンティティの検索	Detective で、大文字と小文字を区別しない検索が可能になりました。	2022 年 10 月 3 日
時間範囲のタイムスタンプを設定する機能を追加しました。	Detective で、時間範囲のタイムスタンプ形式の詳細設定を設定できるようになりました。この詳細設定は Detective のすべてのタイムスタンプに適用されます。	2022 年 10 月 3 日
検出結果グループに関連する用語を追加しました	関連する検出結果を 1 つにまとめて表示する検出結果グループが Detective でサポートされるようになりました。これにより、環境内で発生する可能性のある悪意のあるアクティビティを調査しやすくなりました。検出結果グループプロファイルから、エンティティプロファイルと、そのグループに関連する検出結果の概要にピボットできるようになりました。	2022 年 8 月 3 日

Amazon EKS 監査ログに関連する新しいプロファイルを追加しました	Detective は、コンテナ関連のエンティティ (Amazon EKS クラスター、コンテナイメージ、Kubernetes ポッド、Kubernetes サブジェクト) に関連するアクティビティを調査できるプロファイルを提供するようになりました。	2022 年 7 月 26 日
新しいオプションのデータソースを追加しました	Detective が、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、この新しいデータソースを既存の動作グラフ用に有効にすることができます。この日付より後に作成したグラフでは、このデータソースがデフォルトで有効になります。管理者はこのデータソースをいつでも手動で無効にできます。	2022 年 7 月 26 日
Detective の新しいサービスリンクロールとマネージドポリシー	Detective に、サービスリンクロール `AWSServiceRoleForDetective` が追加されました。このサービスリンクロールは、ユーザーの代わりに Organizations データにアクセスするのに使用されます。このロールは新しいマネージドポリシー `AmazonDetectiveServiceLinkedRolePolicy` を使用します。	2021 年 12 月 16 日

との統合を追加 AWS Organizations	Detective が Organizations と統合されました。組織管理アカウントが組織の 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、組織動作グラフのメンバーアカウントとしてそれらのアカウントを有効にすることができます。	2021 年 12 月 16 日
検出結果プロファイルを検出結果の概要に置き換えました	検出結果プロファイルには、関連するリソースのアクティビティの分析結果であるビジュアライゼーションが含まれていました。新しい検出結果の概要には、 から取り込まれた検出結果の詳細と GuardDuty、関係するエンティティのリストが含まれています。検出結果の概要から、関連するエンティティのプロファイルにピボットできます。	2021 年 9 月 20 日
サポートされている GuardDuty 検出結果タイプの制限を削除しました	Detective は、選択した GuardDuty 検出結果タイプのセットに制限されなくなりました。Detective は、すべての検出結果タイプの検出結果の詳細を自動的に収集し、関連するエンティティのためにエンティティプロファイルへのアクセスを提供します。	2021 年 9 月 20 日

関連する検出結果プロファイルパネルの検出結果の詳細へのリンク	エンティティプロファイルで、関連する検出結果リストで検出結果を選択すると、右側のパネルに検出結果の詳細が表示されます。スコープ時間は、検出結果の時間枠に設定されます。	2021 年 9 月 20 日
Detective で利用可能なエンティティタイプに S3 バケットを追加しました	Detective は、S3 バケットのプロファイルの提供を開始しました。S3 バケットプロファイルは、S3 バケットとインタラクションしたプリンシパルとそれらが S3 バケットで実行した API 操作に関する詳細を提供します。	2021 年 9 月 20 日
Splunk で Detective URL を生成する新しいオプション	Splunk Trumpet プロジェクトでは、 AWS コンテンツを Splunk に送信できます。プロジェクトでは、検出URLs を追加できるようになりました GuardDuty 。	2021 年 9 月 8 日

アカウントとロールのアクティビティの詳細で AKID を置き換えました	アカウントプロファイルで、[全体的な API コール量] のアクティビティの詳細に、アクセスキー識別子 (AKID) ではなくユーザーまたはロールが表示されるようになりました。ロールプロファイルで、[全体的な API コール量] のアクティビティの詳細に、AKID ではなくロールセッションが表示されるようになりました。この変更の前に発生したアクティビティについては、発信者は [Unknown resource] (不明なリソース) としてリストされます。	2021 年 7 月 14 日
API コールに関する情報に対するコールサービスを追加しました	Detective コンソールで、API コールに関する情報に、コールを発行したサービスが含まれるようになりました。[全体的な API コール量]、[新しく観察された API コール]、および [量が増加した API コール] のリストに [サービス] 列を追加しました。[全体的な API コール量] と [新しく観測されたジオロケーション] のアクティビティの詳細では、API メソッドはそれらを発行したサービスの下にグループ化されます。この変更の前に発生したアクティビティについては、API メソッドは [Unknown service] (不明なサービス) の下にグループ化されます。	2021 年 7 月 14 日

ユーザー、ロール、およびロールセッション用の [リソースのインタラクション] タブを追加しました	ユーザー、ロール、およびロールセッションの [Resource interaction] (リソースインタラクション) タブには、これらのエンティティが関与したロール引き受けアクティビティに関する情報が含まれています。ロールセッションについては、これは新しいタブです。ユーザーとロールについては、これは新しいコンテンツを含む既存のタブです。	2021 年 6 月 29 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追加することができなくなります。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。	2021 年 6 月 10 日
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、許可された総量の割合として量が表示されていました。	2021 年 4 月 29 日

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

追加の Amazon GuardDuty 検出結果タイプのサポートを追加	Detective は、、CredentialAccess:IAMUser/AnomalousBehavior 、DefenseEvasion:IAMUser/AnomalousBehavior 、、、Discovery:IAMUser/AnomalousBehavior 、、 という追加の GuardDuty 検出結果タイプのプロファイルを提供するようになりました。 Exfiltration:IAMUser/AnomalousBehavior Impact:IAMUser/AnomalousBehavior InitialAccess:IAMUser/AnomalousBehavior Persistence:IAMUser/AnomalousBehavior PrivilegeEscalation:IAMUser/AnomalousBehavior	2021 年 3 月 29 日
AWS GovCloud (US) リージョンの違いを追加	Detective が AWS GovCloud (US) リージョンで利用可能になりました。 AWS GovCloud（米国東部) および AWS GovCloud（米国西部) では、Detective はメンバーアカウントに招待メールを送信しません。また、Detective は、AWSで終了するメンバーアカウントを自動的に削除することもありません。	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。ステータスが [承認済み (有効になっています)] のメンバーアカウントと、ステータスが [承認済み (有効になっています)] 以外のメンバーアカウントを含むすべてのメンバーアカウントを表示できます。	2021 年 3 月 16 日
追加の Amazon GuardDuty 検出結果タイプのサポートを追加	Detective は、、`Backdoor:EC2/C&CActivity.B` 、`Impact:EC2/PortSweep` `Impact:EC2/WinRMBruteForce` および のその他の GuardDuty 検出結果タイプのプロファイルを提供するようになりました。 `PrivilegeEscalation:IAMUser/AdministrativePermissions`	2021 年 3 月 4 日
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

「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	「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
「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	「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
検出結果の IP アドレスとの間における VPC フロー量のプロファイルパネルについて、アクティビティの詳細を追加しました	[VPC flow volume to and from the finding's IP address] (検出結果の IP アドレスとの間における VPC フロー量) のプロファイルパネルで、アクティビティの詳細を表示できるようになりました。アクティビティの詳細は、検出結果が単一の IP アドレスに関連付けられている場合にのみ使用できます。アクティビティの詳細には、ポート、プロトコル、および方向の各組み合わせの量が表示されます。	2021 年 2 月 25 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

IP アドレスプロファイルの [全体的な API コール量] プロファイルパネルに関する新しいアクティビティの詳細	[全体的な API コール量] プロファイルパネルから IP アドレスのアクティビティの詳細を表示できるようになりました。アクティビティの詳細には、IP アドレスからコールを発行した各リソースの成功したコールと失敗したコールの数が表示されます。	2021 年 2 月 23 日
IP アドレスプロファイルに関する新しい [Overall VPC flow volume] (全体的な VPC フローボリューム) プロファイルパネル	IP アドレスプロファイルに [Overall VPC flow volume] (全体的な VPC フローボリューム) プロファイルパネルが含まれるようになりました。プロファイルパネルには、IP アドレスとの間における VPC フロートラフィックの量が表示されます。アクティビティの詳細を表示して、IP アドレスが通信した各 EC2 インスタンスの量を表示できます。	2021 年 1 月 21 日
Detective の [Summary] (概要) ページを追加しました	Detective の [概要] ページには、位置情報、API コールの数、Amazon EC2 トラフィック量に基づいてアナリストを関心のあるエンティティにガイドするためのビジュアライゼーションが含まれています。	2021 年 1 月 21 日

Amazon から Detective にピボット GuardDuty するオプションを更新しました	では GuardDuty、Detective での調査オプションがアクションメニューから検出結果の詳細パネルに移動されます。関連エンティティのリストが表示されます。検出結果タイプがサポートされている場合、リストには検出結果も含まれます。その後、エンティティプロファイルまたは検出結果プロファイルのいずれかに移動することを選択できます。	2021 年 1 月 15 日
アクティビティの詳細のウィンドウをデフォルトのスコープ時間に設定するオプションを追加しました	[全体的な API コール量] と [全体的な VPC フロー量] についてのアクティビティの詳細で、アクティビティの詳細の時間枠をプロファイルのデフォルトのスコープ時間に設定できます。	2021 年 1 月 15 日
エンティティ向けに大量の時間間隔の処理を追加しました	エンティティに 1 つ以上の大量の時間間隔がある場合に注意喚起するための新しい通知を追加しました。新しい [High-volume entities] (大量のエンティティ) ページには、現在のスコープ時間のすべての大量の間隔が表示されます。	2020 年 12 月 18 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

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関する情報を更新し、特定のクォータ値を追加しました。	2020 年 12 月 11 日
Overall API call volume] (全体的な API コール量) プロファイルパネルで、アクティビティの詳細についての時間範囲の選択を追加しました	[Overall API flow volume] (全体的な VPC フロー量) パネルで、選択した時間範囲におけるアクティビティの詳細を表示できるようになりました。パネルには、スコープ時間のアクティビティの詳細を表示するオプションが最初に表示されます。	2020 年 9 月 29 日
Overall VPC flow volume] (全体的な VPC フロー量) プロファイルパネルで、アクティビティの詳細についての時間間隔の選択を追加しました	[Overall VPC flow volume] (全体的な VPC フロー量) パネルでは、チャートから単一の時間間隔についてのアクティビティの詳細を表示できます。時間間隔の詳細を表示するには、時間間隔を選択します。	2020 年 9 月 25 日
新しいロールセッションとフェデレーティッドユーザーエンティティ	Detective では、フェデレーション認証を詳しく調べたり、調査したりできるようになりました。各ロールを引き受けたリソースと、それらの認証が行われた時期を確認できます。	2020 年 9 月 17 日

スコープ時間管理に対する更新	スコープ時間をロックまたはロック解除するオプションを削除しました。常にロックされています。検出結果プロファイルでは、スコープ時間が検出結果の時間枠と異なる場合、警告が表示されます。	2020 年 9 月 4 日
プロファイルをスクロールしても、プロファイルヘッダーは表示されたままとなります	プロファイルでは、タブ上のプロファイルパネルをスクロールしても、タイプ、識別子、およびスコープ時間は表示されたままになります。タブが表示されない場合は、パンくずのタブドロップダウンリストを使用して、別のタブに移動できます。	2020 年 9 月 4 日
検索は常に検索結果を表示します	検索を実行すると、[Search] (検索) ページに結果が表示されるようになりました。結果から、検出結果またはエンティティプロファイルにピボットできます。	2020 年 8 月 27 日
検索の許可条件に追加しました	検索の許可条件が拡張されました。 AWS ユーザーと AWS ロールを名前で検索できます。ARN を使用して、検出結果、 AWS ロール、 AWS ユーザー、EC2 インスタンスを検索できます。	2020 年 8 月 27 日

プロファイルパネルから他のコンソールへのリンク	[EC2 instance details] (EC2 インスタンスの詳細) プロファイルパネルでは、EC2 インスタンス識別子が Amazon EC2 コンソールにリンクされています。[User details] (ユーザーの詳細) および [Role details] (ロールの詳細) のプロファイルパネルでは、ユーザー名とロール名が IAM コンソールにリンクされています。	2020 年 8 月 14 日
VPC フローデータのアクティビティの詳細	[Overall VPC flow volume] (全体的な VPC フロー量) プロファイルパネルで、アクティビティの詳細にアクセスできるようになりました。アクティビティの詳細には、選択した期間中の IP アドレスと EC2 インスタンス間のトラフィックフローが表示されます。	2020 年 7 月 23 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
の新しいオープンソース Python スクリプト GitHub	の新しいamazon-detective-multiaccount-scriptsリポジトリ GitHub には、リージョン間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 スクリプトが用意されています。Detective を有効にしたり、メンバーアカウントを追加したり、メンバーアカウントを削除したり、Detective を無効にしたりできます。	2020 年 1 月 21 日
Amazon Detective のご紹介	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。	2019 年 12 月 2 日

Detective 管理ガイドのコンテンツが Detective ユーザーガイドに統合されました。

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。