Amazon GuardDuty ユーザーガイド

Amazon GuardDuty

Amazon GuardDuty: Amazon GuardDuty ユーザーガイド

Table of Contents

Amazon とは GuardDuty

Amazon GuardDuty は、 AWS 環境内の特定の AWS データソースとログを継続的にモニタリング、分析、処理する脅威検出サービスです。 GuardDuty は、悪意のある IP アドレスやドメインのリスト、機械学習 (ML) モデルなどの脅威インテリジェンスフィードを使用して、 AWS 環境内の予期しない、潜在的に不正なアクティビティを特定します。これには、次の問題が含まれます。

- 特権のエスカレーション、公開された認証情報の使用、悪意のある IP アドレスやドメインとの通信。
- Amazon EC2 インスタンスとコンテナワークロードにマルウェアが存在し、Amazon S3 バケットに新しくアップロードされたファイルがある。
- データベースでのログインイベントの異常なパターンの検出。

例えば、マルウェアやマイニングビットコインを処理する、侵害された可能性のある EC2 インスタンスとコンテナワークロードを検出 GuardDuty できます。また、不正なインフラストラクチャのデプロイなどの潜在的な侵害の兆候がないか、 AWS アカウントのアクセス動作をモニタリングします。例えば、以前に使用したことがないリージョンにデプロイされたインスタンスや、パスワード強度を低下させるためにパスワードポリシーの変更を提案する異常な API コールなどです。

内容

の機能 GuardDuty

ここでは、Amazon が AWS 環境内の潜在的な脅威のモニタリング、検出、管理 GuardDuty に役立つ主な方法をいくつか紹介します。

特定のデータソースとイベントログを継続的にモニタリングする

- 基盤データソースを自動的にモニタリングする – GuardDuty で を有効にすると AWS アカウント、 はそのアカウントに関連付けられた基盤データソースの取り込み GuardDuty を自動的に開始します。これらのデータソースには、 AWS CloudTrail 管理イベント、 AWS CloudTrail イ

ベントログ、VPC フローログ (Amazon EC2 インスタンスから)、DNS ログが含まれます。がこれらのデータソースの分析と処理を開始 GuardDuty して関連するセキュリティ検出結果を生成するために、他のものを有効にする必要はありません。詳細については、「基礎データソース」を参照してください。

- オプションの GuardDuty 保護プランを有効にする – AWS 環境のセキュリティ体制をより詳細に可視化するために、 GuardDuty では、有効にすることを選択できるさまざまな保護プランを提供しています。保護プランは、他の AWS サービスのログとイベントをモニタリングするのに役立ちます。これらのソースには、EKS 監査ログ、RDS ログインアクティビティ、S3 ログ、EBS ボリューム、ランタイムモニタリング、Lambda ネットワークアクティビティログが含まれます。 GuardDuty は、これらのログソースとイベントソースを - 機能 という用語で統合します。サポートされている で 1 つ以上のオプションの保護プランを AWS リージョン いつでも有効にできます。 GuardDuty は、有効にした保護プランに基づいて、アクティビティのモニタリング、処理、分析を開始します。各保護プランとその仕組みの詳細については、対応する保護プランドキュメントを参照してください。

> **Note**
>
> GuardDuty は、Amazon GuardDuty サービスを有効にすることなく、Malware Protection for S3 を個別に使用できる柔軟性を提供します。Malware Protection for S3 の使用を開始する方法の詳細については、「」を参照してくださいGuardDuty S3 のマルウェア保護。他のすべての保護プランを使用するには、 GuardDuty サービスを有効にする必要があります。

マルウェアの存在を検出し、セキュリティ検出結果を生成します。

がリソースに関連する潜在的なセキュリティ脅威 GuardDuty を検出すると AWS 、侵害された可能性のあるリソースに関する情報を提供するセキュリティ検出結果の生成が開始されます。関連する の生成サンプルの検出結果と表示について調べることができます検出結果の詳細。で識別される各リソースタイプに対して生成される可能性のあるセキュリティ検出結果の完全なリストについては GuardDuty、「」を参照してください検出結果タイプ。

生成されたセキュリティ検出結果を管理する

が検出結果を生成したときに GuardDuty通知を受信する EventBridge ように Amazon を設定したり、推奨ステップを使用して検出結果を修正したり、生成された検出結果をフィルタリングして傾向を特定したり、検出結果を S3 バケットにエクスポートしたりできます。詳細については、「 GuardDuty 結果の管理」を参照してください。

関連する AWS セキュリティサービスとの統合

環境のセキュリティ傾向の分析と調査をさらに支援するには、以下の AWS セキュリティ関連サービスを と組み合わせて使用することを検討してください AWS GuardDuty。

- Amazon Detective — このサービスは、セキュリティ検出結果や疑わしいアクティビティの根本原因の分析、調査、および迅速な特定に役立ちます。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 の事前構築されたデータ集約、概要、コンテキストは、潜在的なセキュリティ問題の性質と範囲の分析と判断に役立ちます。

  GuardDuty と Detective を一緒に使用する方法については、「」を参照してくださいAmazon Detective GuardDuty との統合。Detective の詳細については、「Amazon Detective ユーザーガイド」を参照してください。

- AWS Security Hub – このサービスでは、 リソースのセキュリティ状態を包括的に把握し、セキュリティ業界標準およびベストプラクティスに照らして AWS 環境をチェックできます AWS 。これは、複数の AWS サービス (Amazon Macie を含む) およびサポートされているパートナーネットワーク (APN) 製品からセキュリティ検出結果を消費、集約、整理、優先順位付けすることによって部分的に行われます。 AWS 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。

  GuardDuty と Security Hub を一緒に使用する方法については、「」を参照してください GuardDuty との統合 AWS Security Hub。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。

マルチアカウント環境を管理する

マルチアカウント AWS 環境を管理するには、 AWS Organizations （ 推奨) または招待の方法を使用します。詳細については、「複数のアカウントの管理」を参照してください。

PCI DSS コンプライアンス

GuardDuty は、マーチャントまたはサービスプロバイダーによるクレジットカードデータの処理、保存、および送信をサポートし、Payment Card Industry (PCI) Data Security Standard (DSS) に準拠していることが確認されています。PCI コンプライアンスパッケージのコピーをリクエストする方法など、 AWS PCI DSS の詳細については、「PCI DSS レベル 1」を参照してください。

の料金 GuardDuty

AWS 無料利用枠 は、各サービスで指定された制限まで AWS のサービス 無料で探索して試すのに役立ちます。12 か月間の無料トライアル、常に無料トライアル、短期無料トライアルの 3 つのカテゴリがあります。Amazon は短期無料トライアルカテゴリに GuardDuty 属し、30 日間の無料トライアルを提供しています。 GuardDuty この無料トライアル終了後も を引き続き使用すると、このサービスの使用方法に基づいてコストが発生します。

オンデマンドのマルウェアスキャン (EC2 の Malware Protection) と S3 の Malware Protection は、GuardDuty 30 日間の短期無料トライアルカテゴリには含まれません。Malware Protection for S3 は の 12 か月間の無料カテゴリに分類され AWS 無料利用枠 ますが、オンデマンドのマルウェアスキャンは pay-as-you-use コストモデルに従います。オンデマンドのマルウェアスキャンでは、30 日間の無料トライアルや 12 か月間の無料利用枠のコストモデルはありません。詳細については、「 のGuardDuty 料金」を参照してください。

GuardDuty 30 日間の無料トライアルの使用

GuardDuty を で初めて使用する場合 AWS リージョン、 AWS アカウント は、そのリージョンで 30 日間の無料トライアルに自動的に登録されます。一部の保護プランも自動的に有効になり、30 日間の無料トライアルに含まれます。 GuardDuty はリージョンサービスであるため、別のリージョンで初めて有効にすると、アカウントは の 30 日間の無料トライアル GuardDuty と、そのリージョンでサポートされている一部の保護プランを受け取ります。

次の表は、 GuardDuty を初めて有効にしたときに自動的に有効になる保護プランを示しています。

保護プラン	GuardDuty 30 日間の無料トライアルに含まれる	独自の 30 日間の無料トライアルがある[1]	
GuardDuty EKS 保護	はい	はい	
GuardDuty Lambda 保護	はい	はい	
GuardDuty EC2 のマルウェア保護 – GuardDutyが開始するマルウェアスキャン	はい	はい	

保護プラン	GuardDuty 30 日間の無料トライアルに含まれる	独自の 30 日間の無料トライアルがある[1]	
GuardDuty EC2 のマルウェア保護 – オンデマンドのマルウェアスキャン	いいえ	いいえ	
GuardDuty S3 のマルウェア保護	いいえ	いいえ	
GuardDuty RDS Protection	はい	はい	
GuardDuty ランタイムモニタリング	いいえ	はい	
GuardDuty S3 保護	はい	あり	

[1]一般的に、保護プランには独自の 30 日間の無料トライアルがあります。例えば、アカウントの GuardDuty 30 日間の無料トライアルの有効期限が切れた後に一般利用可能になる保護プランを有効にすると、この保護プランの 30 日間の無料トライアルを使用できます。保護プランの無料トライアルの詳細については、各保護プランに関連するドキュメントを参照してください。

無料トライアル中の推定使用コストを表示する – の 30 日間の無料トライアル中、 GuardDuty および保護プランの可能性がある場合、 はアカウントの推定使用コスト GuardDuty を提供します。委任された GuardDuty 管理者アカウントの場合、 を有効にしたすべてのメンバーアカウントの推定使用コストとアカウントレベルの内訳の合計を表示できます GuardDuty。詳細については、「GuardDuty コストの見積もり」を参照してください。

無料トライアル終了後の使用コスト – 無料トライアル終了後も GuardDuty またはその保護プランを引き続き使用すると、関連する使用コストが発生します。請求書を表示するには、https://console.aws.amazon.com/billing/ コンソールで Cost Explorer に移動します。 AWS アカウントの請求の詳細については、AWS Billing 「 ユーザーガイド」を参照してください。

12 か月間の無料利用枠での S3 の Malware Protection の使用

Malware Protection for S3 は、新規、継続的な無料利用枠、または 12 か月間の無料利用枠の有効期限が切れ AWS アカウント た に関連付けられた無料利用枠プランを使用します。詳細については、「Malware Protection for S3 の料金」を参照してください。

アクセス GuardDuty

GuardDuty は、次のいずれかの方法で使用できます。

GuardDuty コンソール

https://console.aws.amazon.com/guardduty/

コンソールは、 にアクセスして使用するブラウザベースのインターフェイスです GuardDuty。GuardDuty コンソールでは、 GuardDuty アカウント、データ、リソースにアクセスできます。

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、GuardDuty タスクと AWS タスクを実行できます。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。

のインストールと使用の詳細については AWS CLI、「AWS Command Line Interface ユーザーガイド」を参照してください。で使用可能な AWS CLI コマンドを表示するには GuardDuty、「CLI コマンドリファレンス」を参照してください。

GuardDuty HTTPS API

GuardDuty HTTPS API を使用して GuardDuty および に AWS プログラムでアクセスできます。これにより、HTTPS リクエストを サービスに直接発行できます。詳細については、GuardDuty「API リファレンス」を参照してください。

AWS SDKs

AWS は、さまざまなプログラミング言語とプラットフォーム (Java、Python、Ruby、.NET、iOS、Android など) 用のライブラリとサンプルコードで構成されるソフトウェア開発キット (SDKs) を提供します。SDKs、 へのプログラムによるアクセスを簡単に作成できます GuardDuty。ダウンロードやインストールなどの方法を含む AWS SDK の詳細については、「Tools for Amazon Web Services」(Amazon Web Services 用のツール) を参照してください。

の開始方法 GuardDuty

このチュートリアルでは、 の実践的な概要を説明します GuardDuty。をスタンドアロンアカウント GuardDuty として、または の GuardDuty 管理者として有効にするための最小要件 AWS Organizations については、ステップ 1 で説明します。ステップ 2～5 では、 が推奨する追加機能を使用して検出 GuardDuty 結果を最大限に活用します。

トピック

開始する前に

GuardDuty は、 AWS CloudTrail イベントログ、 AWS CloudTrail 管理イベント、Amazon VPC フローログ、DNS ログ基礎データソースなどの をモニタリングする脅威検出サービスです。GuardDuty は、保護タイプに関連付けられた機能を個別に有効にする場合にのみ分析します。機能には、Kubernetes 監査ログ、RDS ログインアクティビティ、S3 ログ、EBS ボリューム、ランタイムモニタリング、Lambda ネットワークアクティビティログが含まれます。これらのデータソースと機能 (有効になっている場合) を使用して、アカウントのセキュリティ検出結果 GuardDuty を生成します。

を有効にすると GuardDuty、環境のモニタリングが開始されます。どのリージョンのどのアカウント GuardDuty でも、いつでも を無効にできます。これにより、基盤データソースと個別に有効化された機能は処理され GuardDuty なくなります。

基礎データソース のいずれかを明示的に有効にする必要はありません。Amazon は、これらのサービスから直接独立したデータストリーム GuardDuty を取得します。新しい GuardDuty アカウントでは、 で AWS リージョン サポートされているすべての利用可能な保護タイプが有効になり、デフォルトで 30 日間の無料トライアル期間に含まれます。それらのいずれか、またはすべての設定をオプトアウトできます。既存の GuardDuty お客様は、 で利用可能な保護プランのいずれかまたはすべて

を有効にすることができます AWS リージョン。詳細については、「 の各保護タイプに関連付けられた機能」を参照してください GuardDuty。

を有効にするときは GuardDuty、次の項目を考慮してください。

- GuardDuty はリージョンサービスです。つまり、このページで実行する設定手順は、 でモニタリングする各リージョンで繰り返す必要があります GuardDuty。

  サポートされているすべての AWS リージョン GuardDuty で を有効にすることを強くお勧めします。これにより、アクティブ GuardDuty に使用されていないリージョンでも、不正または異常なアクティビティに関する検出結果を生成できます。これにより、 GuardDuty は IAM などのグローバル AWS サービスの AWS CloudTrail イベントをモニタリングすることもできます。サポートされているすべてのリージョンで が有効になってい GuardDuty ない場合、グローバルサービスを含むアクティビティを検出する機能は低下します。 GuardDuty が利用可能なリージョンの完全なリストについては、「」を参照してくださいリージョンとエンドポイント。
- AWS アカウントで管理者権限を持つユーザーは、 を有効にできます GuardDutyが、最小特権のセキュリティのベストプラクティスに従って、 GuardDuty 特に を管理する IAM ロール、ユーザー、またはグループを作成することをお勧めします。を有効にするために必要なアクセス許可の詳細については、 GuardDuty 「」を参照してください GuardDuty の有効化に必要なアクセス許可。
- 任意の で GuardDuty 初めて を有効にすると AWS リージョン、デフォルトでは、EC2 の Malware Protection など、そのリージョンでサポートされているすべての利用可能な保護タイプも有効になります。 は、 という名前のサービスにリンクされたロールをアカウントに GuardDuty 作成しますAWSServiceRoleForAmazonGuardDuty。このロールには、 が から直接イベント GuardDuty を消費および分析基礎データソースしてセキュリティ検出結果を生成できるようにするアクセス許可と信頼ポリシーが含まれます。Malware Protection for EC2 は、 というサービスにリンクされたロールをアカウントに作成しますAWSServiceRoleForAmazonGuardDutyMalwareProtection。このロールには、Malware Protection for EC2 がエージェントレススキャンを実行して GuardDuty アカウントのマルウェアを検出できるようにするアクセス許可と信頼ポリシーが含まれます。これにより GuardDuty 、 アカウントで EBS ボリュームスナップショットを作成し、そのスナップショットを GuardDuty サービスアカウントと共有できます。詳細については、「のサービスにリンクされたロールのアクセス許可 GuardDuty」を参照してください。サービスにリンクされたロールの詳細については、「サービスリンクロールの使用」を参照してください。
- 任意のリージョンで GuardDuty を初めて有効にすると、そのリージョンの 30 日間の GuardDuty 無料トライアルに AWS アカウントが自動的に登録されます。

ステップ 1: Amazon を有効にする GuardDuty

を使用する最初のステップ GuardDuty は、アカウントで有効にすることです。有効にすると、GuardDuty は直ちに現在のリージョンのセキュリティ脅威のモニタリングを開始します。

組織内の他のアカウント GuardDuty の結果を GuardDuty 管理者として管理する場合は、メンバーアカウントを追加して も有効にする必要があります GuardDuty 。

> **Note**
>
> を有効にせずに GuardDuty Malware Protection for S3 を有効にする場合は GuardDuty、「」を参照してくださいGuardDuty S3 のマルウェア保護。

Standalone account environment

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. Amazon GuardDuty - すべての機能 オプションを選択します。
3. [開始する] を選択します。
4. 「ようこそ GuardDuty」ページで、サービス条件を表示します。を有効にする を選択します GuardDuty。

Multi-account environment

> **Important**
>
> このプロセスの前提条件として、組織 GuardDuty 内の管理者を委任するには、管理するすべてのアカウントと同じ組織に所属し、 AWS Organizations 管理アカウントへのアクセス権を持っている必要があります。管理者の委任には追加の許可が必要になる場合があります。詳細については、「委任された GuardDuty 管理者アカウントを指定するために必要なアクセス許可」を参照してください。

委任 GuardDuty 管理者アカウントを指定するには

1. 管理アカウントを使用して、https://console.aws.amazon.com/organizations/ で AWS Organizations コンソールを開きます。

2. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   アカウントで GuardDuty 既に有効になっていますか？

   - がまだ有効 GuardDuty になっていない場合は、開始方法を選択し、「ようこそ GuardDuty」ページで GuardDuty 委任管理者を指定できます。
   - GuardDuty が有効になっている場合は、設定ページで GuardDuty 委任管理者を指定できます。

3. 組織の GuardDuty 委任管理者として指定する AWS アカウントの 12 桁のアカウント ID を入力し、 の委任を選択します。

> **Note**
>
> がまだ有効 GuardDuty になっていない場合、委任管理者を指定すると、現在のリージョンでそのアカウント GuardDuty に対して が有効になります。

メンバーアカウントを追加するには

この手順では、 を通じて GuardDuty 委任管理者アカウントにメンバーアカウントを追加する方法について説明します AWS Organizations。招待でメンバーを追加するオプションもあります。でメンバーを関連付けるための両方の方法の詳細については GuardDuty、「」を参照してくださいAmazon での複数のアカウントの管理 GuardDuty。

1. 委任された管理者のアカウントにログイン
2. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
3. ナビゲーションパネルで [設定] を選択してから、[アカウント] を選択します。

   アカウントの一覧に組織内のすべてのアカウントが表示されます。

4. アカウント ID の横にあるチェックボックスを選択し、メンバーとして追加したいアカウントを選択します。その後、[アクション] メニューから、[メンバーの追加] を選びます。

> **Tip**
>
> 新しいアカウントをメンバーとして追加するには、[Auto-enable] (自動有効化) の機能をオンにします。ただし、この機能は、機能を有効にした後に組織に参加したアカウントにのみ適用されます。

ステップ 2: サンプル検出結果を生成し、ベーシックなオペレーションの詳細を確認する

がセキュリティ問題 GuardDuty を検出すると、検出結果が生成されます。 GuardDuty 検出結果は、その固有のセキュリティ問題に関する詳細を含むデータセットです。検出結果の詳細を使用して、問題の調査に役立てることができます。

GuardDuty では、プレースホルダー値を含むサンプル検出結果の生成がサポートされています。プレースホルダー値を使用すると、 によって検出された実際のセキュリティ問題に対応する前に、GuardDuty 機能をテストし、検出結果に慣れることができます GuardDuty。以下のガイドに従って、 で利用可能な各検出結果タイプのサンプル検出結果を生成します。アカウント内でシミュレートされたセキュリティイベントを生成するなど、サンプル検出結果を生成する GuardDutyその他の方法については、「」を参照してくださいサンプルの検出結果。

サンプル検出結果を作成して調査するには

1. ナビゲーションペインで [設定] を選択します。
2. [設定] ページの [結果のサンプル] で、[結果サンプルの生成] を選択します。
3. ナビゲーションペインで、概要 を選択して、 AWS 環境で生成された結果に関するインサイトを表示します。概要ダッシュボードのコンポーネントの詳細については、「[要約] ダッシュボード」を参照してください。
4. ナビゲーションペインで [結果] を選択します。[Current findings] (最近の結果) ページに [SAMPLE] とプレフィックスされたサンプル検出結果が表示されます。
5. リストから検出結果を選択して、検出結果の詳細を表示します。

    - 検出結果の詳細ペインで使用可能なさまざまな情報フィールドを確認できます。検出結果のタイプが異なると、フィールドが異なる場合があります。すべての検出結果タイプで使用可能なフィールドの詳細については、「検出結果の詳細」を参照してください。詳細ペインから、次のアクションを実行できます。

        - ペインの一番上の [結果 ID] を選択し、検出結果のための完全な JSON 詳細を開きます。完全な JSON ファイルは、このパネルからダウンロードすることもできます。JSON には、コンソールビューに含まれない追加情報が含まれており、他のツールやサービスで取り込むことができる形式です。
        - [影響を受けるリソース] セクションを表示します。実際の検出結果では、ここに記載されている情報は、調査すべきアカウント内のリソースを特定するのに役立ち、実用的なリソース AWS Management Console に適した へのリンクが含まれます。

- 「+」または「-」の虫眼鏡アイコンを選択して、その詳細の包括的または排他的なフィルターを作成します。検出結果フィルターの詳細については、「検出結果のフィルタリング」を参照してください。

6. サンプル検出結果をすべてアーカイブする

   a. リストの上部にあるチェックボックスを選んで、すべての検出結果を選択します。

   b. 保持したい検出結果を選択解除します。

   c. [アクション] メニューを選択し、[アーカイブ] をクリックして、サンプルの検出結果を非表示にします。

> **Note**
>
> Actions メニューを見るために、[最新] を選択し、検出結果ビューを切り替えるために [アーカイブ] を選択してください。

ステップ 3: Amazon S3 バケットへの GuardDuty 結果のエクスポートを設定する

GuardDuty では、 GuardDuty 90 日間の保持期間を超えて無期限に保存するために、検出結果を S3 バケットにエクスポートできるので、検出結果をエクスポートするように設定することをお勧めします。これにより、検出結果の記録を保持したり、 AWS 環境内の問題を経時的に追跡したりできます。ここで概説するプロセスでは、新しい S3 バケットをセットアップし、コンソール内から検出結果を暗号化するための新しい KMS キーを作成する手順を説明します。独自の既存のバケットや別のアカウントのバケットを使用する方法などの詳細については、「検出結果のエクスポート」を参照してください。

S3 エクスポート検出結果を設定するには

1. 検出結果を暗号化するには、 がそのキー GuardDuty を暗号化に使用できるようにするポリシーを持つ KMS キーが必要です。次の手順は、新しい KMS キーの作成に役立ちます。別のアカウントの KMS キーを使用している場合は、キーを所有 AWS アカウント する にログインしてキーポリシーを適用する必要があります。KMS キーのリージョンおよび S3 バケットは同じである必要があります。ただし、検出結果をエクスポートするリージョンごとに、これと同じバケットとキーのペアを使用できます。

   a. https://console.aws.amazon.com/kms で AWS KMS コンソールを開きます。

b. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。

c. ナビゲーションペインで、[カスタマーマネージドキー] を選択します。

d. [Create key] (キーの作成) を選択します。

e. [キーのタイプ] の [対称] を選択してから、[次へ] を選択します。

> **Note**
>
> 詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

f. キーの [エイリアス] を指定し、[次へ] を選択します。

g. [次へ] を選択し、再度 [次へ] を選択して、デフォルトの管理許可と使用許可を承諾します。

h. 設定を [確認] した後、[完了] を選択してキーを作成します。

i. [顧客管理キー] ページで、キーエイリアスを選択します。

j. [キーポリシー] セクションで、[ポリシービューへの切り替え] を選択します。

k. 編集 を選択し、次のキーポリシーを KMS キーに追加して、キー GuardDuty へのアクセスを許可します。このステートメントでは GuardDuty 、このポリシーを追加するキーのみを使用できます。キーポリシーを編集するときは、JSON 構文が有効であることを確認してください。最後のステートメントの前にステートメントを追加する場合は、閉じ括弧の後にカンマを追加する必要があります。

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
```

```
}
```

Region1 を、ご使用の KMS キーのリージョンに置き換えます。*444455556666* を KMS キーを所有 AWS アカウント する に置き換えます。*KMSKeyId* を、暗号化用に選択した KMS キーのキー ID に置き換えます。リージョン AWS アカウント、およびキー ID のこれらの値をすべて識別するには、KMS キーの ARN を表示します。キー ARN を見つけるには、「キー ID と ARN を検索する」を参照してください。

同様に、*111122223333* を GuardDuty アカウントの AWS アカウント に置き換えます。*Region2* を GuardDuty アカウントのリージョンに置き換えます。*SourceDetectorID* を Region*Region2* の GuardDuty アカウントのディテクター ID に置き換えます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

l. [保存] を選択します。

2. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
3. ナビゲーションペインで [設定] を選択します。
4. [Findings export options] (結果のエクスポートオプション) の下で、[Configure now] (今すぐ設定) を選択します。
5. [新規バケット] を選択します。S3 バケットの一意の名前を入力します。
6. (オプション) サンプル検出結果を生成して、新しいエクスポート設定をテストできます。ナビゲーションペインで [設定] を選択します。
7. [サンプル検出結果] で、[サンプル調査結果を生成] を選択します。新しいサンプル検出結果は、最大 5 分 GuardDuty で によって作成された S3 バケットにエントリとして表示されます。

ステップ 4: SNS 経由で GuardDuty 結果アラートを設定する

GuardDuty は Amazon と統合されており EventBridge、これを使用して検出結果データを他のアプリケーションやサービスに送信して処理できます。 EventBridge を使用すると、 GuardDuty 検出結果イベントを AWS Lambda 関数、Amazon EC2 Systems Manager オートメーション、Amazon Simple Notification Service (SNS) などのターゲットに接続することで、検出結果への自動応答を開始できます。

この例では、 EventBridge ルールのターゲットとなる SNS トピックを作成し、 EventBridge を使用して から検出結果データをキャプチャするルールを作成します GuardDuty。結果として得られるルールは、検出結果の詳細をメールアドレスに転送します。検出結果を Slack または Amazon Chime に送信する方法、および送信される検出結果のアラートタイプを変更する方法については、「Amazon SNS トピックおよびエンドポイントの設定」を参照してください。

検出結果アラートの SNS トピックを作成するには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. ナビゲーションペインで、[トピック] を選択します。
3. [トピックの作成] を選択します。
4. [Type] (タイプ) に、[Standard] (標準) を選択します。
5. [名前] に **`GuardDuty`** と入力します。
6. [トピックの作成] を選択します。新しいトピックのトピック詳細が開きます。
7. [サブスクリプション] セクションで、[サブスクリプションの作成] を選択します。
8. [プロトコル] で [E メール] を選択します。
9. [Endpoint] (エンドポイント) に、通知を送信する先の E メールアドレスを入力します。
10. [Create subscription] (サブスクリプションの作成) を選択します。

    サブスクリプションを作成した後に、E メールを通してサブスクリプションを確認する必要があります。
11. サブスクリプションメッセージを確認するには、E メールの受信ボックスに移動して、サブスクリプションメッセージで [Confirm subscription] (サブスクリプションの確認) を選択します。

> **Note**
>
> メール確認のステータスを確認するには、SNS コンソールに移動して [Subscriptions] (サブスクリプション) を選択します。

GuardDuty 検出結果をキャプチャしてフォーマットする EventBridge ルールを作成するには

1. https://console.aws.amazon.com/events/ で EventBridge コンソールを開きます。
2. ナビゲーションペインで ルール] を選択します。
3. ルールの作成 を選択します。
4. ルールの名前と説明を入力します。

ルールには、同じリージョン内および同じイベントバス上の別のルールと同じ名前を付けることはできません。

5. [イベントバス] として、[デフォルト] を選択します。
6. [ルールタイプ] では、[イベントパターンを持つルール] を選択します。
7. [Next] (次へ) を選択します。
8. [Event source] (イベントソース) で、[AWS events] (イベント) を選択します。
9. [イベントパターン] で、[イベントパターンフォーム] を選択します。
10. [イベントパターンフォーム] では、AWS [サービス] を選択します。
11. [AWS のサービス] で、[GuardDuty] を選択します。
12. イベントタイプ で、GuardDuty検出結果 を選択します。
13. [Next] (次へ) を選択します。
14. [ターゲットタイプ] では、AWS [サービス] を選択します。
15. [Select a target] (ターゲットの選択) では、[SNS topic] (SNS トピック) を選択し、[Topic] (トピック) では、以前に作成した SNS トピックの名前を選択します。
16. [Additional settings] (追加設定) セクションの [Configure target input] (ターゲット入力の設定) では、[Input transformer] (入力トランスフォーマー) を選択します。

    入力トランスフォーマーを追加すると、 から送信された JSON 検出結果データが人間が読めるメッセージ GuardDuty にフォーマットされます。
17. [Configure input transformer] (入力トランスフォーマーの設定) を選択します。
18. [Target input transformer] (ターゲット入力トランスフォーマー) セクションで、[Input path] (入力パス) に以下のコードを貼り付けます。

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. E メールをフォーマットするには、テンプレート で次のコードを貼り付け、赤のテキストをリージョンに適した値に置き換えてください。

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. [確認] を選択します。
21. [次へ] をクリックします。
22. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、「Amazon ユーザーガイド」の「Amazon EventBridge タグ」を参照してください。 EventBridge
23. [次へ] をクリックします。
24. ルールの詳細を確認し、[ルールの作成] を選択します。
25. (オプション) ステップ 2 のプロセスでサンプル検出結果を生成して、新しいルールをテストします。生成されたサンプル検出結果ごとにメールが届きます。

次のステップ

を引き続き使用すると GuardDuty、環境に関連する検出結果のタイプを理解できるようになります。新しい検出結果を受け取ったときはいつでも、検出結果の詳細ペイン中の検出結果の記述から [詳細はこちら] を選択することにより、あるいは 検出結果タイプ の検出結果名を探すことにより、その検出結果に関する修復に関するレコメンデーションを含む情報を検索できます。

以下の機能は、 AWS 環境に最も関連性の高い結果を提供 GuardDuty できるように調整するのに役立ちます。

- インスタンス ID、アカウント ID、S3 バケット名など、特定の基準に基づいて結果を簡単にソートするには、 内でフィルターを作成して保存できます GuardDuty。詳細については、「検出結果のフィルタリング」を参照してください。
- 環境内で予想される動作に関する検出結果を受け取っている場合は、[suppression rules] (抑制ルール) で定義した基準に基づいて検出結果を自動的にアーカイブできます。
- 信頼された IPs のサブセットから検出結果が生成されないようにしたり、通常の GuardDuty モニタリング範囲外の IPs を でモニタリングしたりするには、信頼された IP と脅威リスト を設定できます。

概念と用語

Amazon の使用を開始すると GuardDuty、その主要な概念について学ぶことでメリットが得られます。

アカウント

AWS リソースを含む標準の Amazon Web Services (AWS) アカウント。アカウント AWS で にサインインし、 を有効にできます GuardDuty。

他のアカウントを招待して、 で AWS アカウントを有効に GuardDuty して関連付けることもできます GuardDuty。招待が承諾されると、アカウントが管理者アカウント GuardDuty として指定され、追加されたアカウントがメンバーアカウントになります。その後、それらのアカウントの結果を代理 GuardDuty で表示および管理できます。

管理者アカウントのユーザーは、自分のアカウントと GuardDutyすべてのメンバーアカウントの結果を設定 GuardDuty および表示および管理できます。には、最大 10,000 個のメンバーアカウントを設定できます GuardDuty。

メンバーアカウントのユーザーは、自分のアカウントで (GuardDuty マネジメントコンソールまたは GuardDuty API を介して) GuardDuty 結果を設定したり GuardDuty 、表示および管理したりできます。メンバーアカウントのユーザーは、他のメンバーアカウントの検出結果を表示または管理することはできません。

は、 GuardDuty 管理者アカウントとメンバーアカウントを同時に AWS アカウント 使用することはできません。は、メンバーシップの招待を 1 つだけ受け入れ AWS アカウント ることができます。メンバーシップの招待の承諾はオプションです。

詳細については、「Amazon での複数のアカウントの管理 GuardDuty」を参照してください。

ディテクター

Amazon GuardDuty はリージョンレベルのサービスです。特定の GuardDuty で を有効にすると AWS リージョン、 AWS アカウント はディテクター ID に関連付けられます。この 32 文字の英数字 ID は、そのリージョンのアカウントに固有です。例えば、別のリージョンで同じアカウント GuardDuty に対して を有効にすると、アカウントは別のディテクター ID に関連付けられます。detectorId の形式は `12abc34d567e8fa901bc2d34e56789f0` です。

GuardDuty 検出結果とサービスの管理に関するすべての検出結果、アカウント、およびアクションは、 GuardDutyディテクター ID を使用して API オペレーションを実行します。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

> **Note**
>
> 複数アカウント環境では、メンバーアカウントのすべての検出結果が管理者アカウントのディテクターに関連付けられます。

CloudWatch イベント通知頻度の設定や、 が処理 GuardDuty するオプションの保護プランの有効化または無効化など、一部の GuardDuty 機能はディテクターを介して設定されます。

内で S3 の Malware Protection を使用する GuardDuty

が有効になっているアカウントで Malware Protection for S3 GuardDuty を有効にすると、保護されたリソースの有効化、編集、無効化などの Malware Protection for S3 アクションはディテクター ID に関連付けられません。

脅威検出オプション Malware Protection for S3 を有効にして GuardDuty 選択しない場合、アカウント用に作成されるディテクター ID はありません。

基礎データソース

データのセットのオリジンまたは場所です。 AWS 環境内の不正または予期しないアクティビティを検出するには、 は AWS CloudTrail イベントログ、 AWS CloudTrail 管理イベント、S3 AWS CloudTrail のデータイベント、VPC フローログ、DNS ログからのデータを GuardDuty 分析して処理します。「」を参照してください基礎データソース。

機能

GuardDuty 保護プラン用に設定された特徴量オブジェクトは、 AWS 環境内の不正または予期しないアクティビティを検出するのに役立ちます。各 GuardDuty 保護プランは、データを分析および処理するための対応する機能オブジェクトを設定します。一部の機能オブジェクトには、EKS 監査ログ、RDS ログインアクティビティモニタリング、Lambda ネットワークアクティビティログ、EBS ボリュームが含まれます。詳細については、「での機能のアクティベーション GuardDuty」を参照してください。

結果

GuardDuty によって発見された潜在的なセキュリティの問題。詳細については、「Amazon GuardDuty の検出結果について」を参照してください。

結果は GuardDuty コンソールに表示され、セキュリティ問題の詳細な説明が含まれています。GetFindings および ListFindings API オペレーションを呼び出すことで、生成された結果を取得することもできます。

また、Amazon CloudWatch イベントを通じて GuardDuty 検出結果を確認することもできます。は、検出結果を HTTPS プロトコル CloudWatch 経由で Amazon GuardDuty に送信します。詳細については、「Amazon CloudWatch Events を使用した GuardDuty 結果へのカスタムレスポンスの作成」を参照してください。

IAM PassRole

これは、S3 オブジェクトをスキャンするために必要なアクセス許可を持つ IAM ロールです。スキャンされたオブジェクトのタグ付けが有効になっている場合、IAM アクセス PassRole 許可はスキャンされたオブジェクトにタグ GuardDuty を追加するのに役立ちます。

Malware Protection プランリソース

バケットの S3 の Malware Protection を有効にすると、 は EC2 プランリソースの Malware Protection GuardDuty を作成します。このリソースは、保護されたバケットの一意の識別子である EC2 プラン ID の Malware Protection に関連付けられています。Malware Protection プランリソースを使用して、保護されたリソースに対して API オペレーションを実行します。

保護されたバケット (保護されたリソース)

Amazon S3 バケットは、このバケットで Malware Protection for S3 を有効にし、その保護ステータスがアクティブ に変わると、保護されていると見なされます。

GuardDuty は、保護されたリソースとして S3 バケットのみをサポートします。

保護ステータス

Malware Protection プランリソースに関連付けられているステータス。バケットの Malware Protection for S3 を有効にすると、このステータスはバケットが正しく設定されているかどうかを表します。

S3 オブジェクトプレフィックス

Amazon Simple Storage Service (Amazon S3) バケットでは、プレフィックスを使用してストレージを整理できます。プレフィックスは、S3 バケット内のオブジェクトの論理グループです。詳細については、「Amazon S3 ユーザーガイド」の「オブジェクトの整理と一覧表示」を参照してください。 Amazon S3

スキャンオプション

GuardDuty Malware Protection for EC2 が有効になっている場合、スキャンまたはスキップする Amazon EC2 インスタンスと Amazon Elastic Block Store (EBS) ボリュームを指定できます。この機能を使用すると、EC2 インスタンスおよび EBS ボリュームに関連付けられている既存のタグを、包含タグリストまたは除外タグリストのいずれかに追加できます。包含タグリストに追加するタグに関連付けられているリソースは、マルウェアのスキャンが行われ、除外タグリストに追加されたリソースはスキャンされません。詳細については、「ユーザー定義タグ付きのスキャンオプション」を参照してください。

スナップショットの保持

GuardDuty Malware Protection for EC2 を有効にすると、EBS ボリュームのスナップショットを AWS アカウント内に保持するオプションが提供されます。 は、EBS ボリュームのスナップショットに基づいてレプリカ EBS ボリューム GuardDuty を生成します。EBS ボリュームのスナップショットは、Malware Protection for EC2 スキャンがレプリカ EBS ボリューム内のマルウェアを検出した場合にのみ保持できます。レプリカ EBS ボリュームでマルウェアが検出されない場合、 は、スナップショットの保持設定に関係なく、EBS ボリュームのスナップショット GuardDuty を自動的に削除します。詳細については、「スナップショットの保持」を参照してください。

抑制ルール

抑制ルールを使用すると、特定の属性の組み合わせを作成して検出結果数を抑えることができます。例えば、 GuardDuty フィルターを使用してルールを定義し、特定の VPC、特定の AMI の実行、または特定の EC2 タグを持つインスタンスのみ`Recon:EC2/Portscan`から自動アーカイブできます。このルールにより、ポートスキャンの検出結果は、条件を満たすインスタンスから自動的にアーカイブされます。ただし、 が暗号通貨マイニングなどの他の悪意のあるアクティビティを行っているインスタンス GuardDuty を検出した場合、アラートは引き続き許可されます。

GuardDuty 管理者アカウントで定義された抑制ルールは、 GuardDuty メンバーアカウントに適用されます。 GuardDuty メンバーアカウントは抑制ルールを変更できません。

抑制ルールを使用すると、 GuardDuty Seltitle はすべての検出結果を生成します。抑制ルールは、すべてのアクティビティの完全で不変な履歴を維持しながら、検出結果の数を抑えます。

通常、抑制ルールの使用目的は、環境に対して誤検知と判断した検出結果を非表示にし、重要度の低い検出結果からのノイズを減らして、より大きな脅威に集中できるようにすることです。詳細については、「抑制ルール」を参照してください。

信頼できる IP リスト

環境との AWS 非常に安全な通信のための信頼された IP アドレスのリスト。 は、信頼された IP GuardDuty リストに基づいて検出結果を生成しません。詳細については、「信頼できる IP リストと 脅威リストの使用」を参照してください。

脅威 IP リスト

悪意のある既知の IP アドレスのリスト は、疑わしい可能性のあるアクティビティが原因で検出結果を生成するだけでなく、これらの脅威リストに基づいて検出結果 GuardDuty も生成します。詳細については、「信頼できる IP リストと 脅威リストの使用」を参照してください。

での機能のアクティベーション GuardDuty

Amazon を初めて有効にするか、 内で保護タイプを有効にすると GuardDuty、 は AWS 環境基礎データソース内の対応する の処理 GuardDuty を開始します。 GuardDuty はこれらのデータソースを使用して、 GuardDuty VPC フローログ、DNS ログ、イベントログ、管理ログなどの AWS CloudTrail イベントのストリームを処理します。次に、これらのイベントを分析して潜在的なセキュリティ脅威を特定し、アカウントに関する検出結果を生成します。

は、ログデータソースに加えて、 AWS 環境内の他の AWS のサービスからの追加のデータを使用して、潜在的なセキュリティ脅威をモニタリングおよび分析 GuardDuty できます。

機能の有効化

S3 Protection GuardDuty 、Runtime Monitoring、EKS Protection などの保護を追加すると、保護タイプに対応する GuardDuty 機能を設定できます。これまで、 GuardDuty 保護は APIsdataSourcesで呼び出されていました。ただし、2023 年 3 月以降、新しい GuardDuty 保護タイプは として設定featuresされ、 として設定されなくなりましたdataSources。 GuardDuty は、 API dataSourcesを通じて 2023 年 3 月より前に起動された保護タイプの設定をサポートしていますが、新しい保護タイプは としてのみ使用できますfeatures。

コンソールを使用して GuardDuty 設定と保護タイプを管理する場合、この変更の直接的な影響を受けず、アクションを実行する必要はありません。機能のアクティベーションは、 内で GuardDuty または 保護タイプを有効にするために呼び出される APIs の動作に影響します GuardDuty。詳細については、「GuardDuty API の変更」を参照してください。

GuardDuty 2023 年 3 月の API の変更点

GuardDuty APIs、 のリストに属さない保護機能を設定します基礎データソース。機能オブジェクトには、機能名やステータスなどの機能の詳細が含まれ、一部の機能の追加設定が含まれる場合があります。この移行は、「Amazon APIs」の以下の API に影響します。 GuardDuty

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors

- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

データソースと比較した機能のアクティベーション

歴史的に、すべての GuardDuty 機能は API の dataSources オブジェクトを通過していました。2023 年 3 月以降、 は API の features オブジェクトではなく dataSources オブジェクトを GuardDuty 優先します。以前のデータソースにはすべて対応する機能がありますが、新しい機能には対応するデータソースがない場合があります。

次のリストは、API を介して渡されたときの dataSources および features オブジェクトとの比較を示しています。

- dataSources オブジェクトには、各保護タイプとそのステータスのオブジェクトが含まれています。features オブジェクトは、 内の各保護タイプに対応する利用可能な機能のリストです GuardDuty。

  2023 年 3 月以降、 環境で新機能を設定する唯一の方法は GuardDuty 機能の AWS アクティベーションです。
- API リクエストまたはレスポンスのdataSourcesスキーマは、 が利用可能な各 AWS リージョン で同じ GuardDuty です。ただし、すべての機能が各リージョンで利用できるわけではありません。そのため、利用可能な機能名は地域によって異なる場合があります。

機能アクティベーションの仕組みを理解する

GuardDuty APIs はdataSources引き続きオブジェクトを必要に応じて返し、同じ情報を含むfeaturesオブジェクトを別の形式で返します。2023 年 3 月より前に起動された GuardDuty 機能はdataSources、オブジェクトとfeaturesオブジェクトを通じて使用できます。2023 年 3 月以降に GuardDuty 起動された機能は、featuresオブジェクトを通じてのみ使用できます。同じ API リクエストでディテクターを作成または更新したり、dataSources および features オブジェクトの両方を表記して AWS Organizations を記述したりすることはできません。保護タイプを有効にする GuardDuty には、featuresオブジェクトを含む同じ APIs を使用して、既存のデータソースを features オブジェクトに移行する必要があります。

> **Note**
>
> GuardDuty は、この変更後に新しいデータソースを追加しません。

GuardDuty はデータソースの使用を廃止しました。ただし、まだ 基礎データソース をサポートしています。ベストプラクティスでは GuardDuty 、アカウントで既に有効になっている保護タイプに機能のアクティベーションを使用することをお勧めします。また、ベストプラクティスとしては、アカウントで新しい保護のタイプを有効にするときに機能を有効にすることも必要です。

機能の有効化に関する変更の組み込み

- APIs 、 SDKs、または AWS CloudFormation テンプレートを使用して GuardDuty 設定を管理し、潜在的な新機能を有効にする場合は GuardDuty 、それぞれコードとテンプレートを変更する必要があります。詳細については、「Amazon APIs」の「更新された API」を参照してください。GuardDuty
- このアップグレードの前に設定された GuardDuty 機能については、APIs、 SDKs、または AWS CloudFormation テンプレートを引き続き使用できます。ただし、`feature` オブジェクトの使用に切り替えることをお勧めします。

  すべてのデータソースには同等の機能オブジェクトがあります。詳細については、「dataSources を features へマッピング」を参照してください。
- 現在、`features` オブジェクトの `additionalConfiguration` は特定の保護タイプでのみ利用できます。
  - このような保護タイプでは、機能の `AdditionalConfigurationstatus`が に設定`ENABLED`されていても、機能の設定`status`が に設定されていない場合`ENABLED`、 はこの場合何も実行 GuardDuty しません。
  - 次の API はこの影響を受けます。
    - UpdateDetector
    - UpdateMemberDetectors
    - UpdateOrganizationConfiguration

dataSources を features へマッピング

次の表に、保護タイプである `dataSources` および `features` のマッピングを示します。

GuardDuty 保護タイプ	データソース名 *	機能名
VPC Flow Logs	flowLogs (読み込み専用、変更不可)	FLOW_LOGS (読み込み専用、変更不可)
DNS ログ	dnsLogs (読み込み専用、変更不可)	DNS_LOGS (読み込み専用、変更不可)
CloudTrail イベント	cloudTrail (読み込み専用、変更不可)	CLOUD_TRAIL (読み込み専用、変更不可)
S3	s3Logs	S3_DATA_EVENTS
EKS 監査ログのモニタリング	kubernetes.auditlogs	EKS_AUDIT_LOGS
EC2 のマルウェア保護	malwareProtection.scanEc2InstanceWithFindings.ebsVolumes	EBS_MALWARE_PROTECTION
RDS ログインイベント	GuardDuty は、これらの保護タイプに対して機能アクティベーションサポートのみを提供します。	RDS_LOGIN_EVENTS
EKS Runtime Monitoring		EKS_RUNTIME_MONITORING
Runtime Monitoring		RUNTIME_MONITORING
GuardDuty Amazon EKS クラスター用の セキュリティエージェント		EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT

GuardDuty 保護タイプ	データソース名 *	機能名
		RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
GuardDuty Amazon ECS-Fargate クラスターのセキュリティエージェント		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT
GuardDuty Amazon EC2 インスタンスのセキュリティエージェント		RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT
Lambda Protection		LAMBDA_NETWORK_LOGS

*GetUsageStatistics は独自の dataSource 名前を使用します。詳細については、GuardDuty コストの見積もりまたはGetUsageStatisticsを参照してください。

基礎データソース

GuardDuty は、基本的なデータソースを使用して、既知の悪意のあるドメインや IP アドレスとの通信を検出し、潜在的に異常な動作や不正なアクティビティを特定します。これらのソースから への転送中に GuardDuty、すべてのログデータが暗号化されます。 GuardDuty は、プロファイリングと異常検出のためにこれらのログソースからさまざまなフィールドを抽出し、これらのログを破棄します。

リージョンで GuardDuty 初めて を有効にすると、すべての基本的なデータソースの脅威検出を含む 30 日間の無料トライアルがあります。この無料トライアル中およびそれ以降は、 GuardDuty コンソールの使用状況ページで、推定月間使用量をデータソース別に分類してモニタリングできます。委任された GuardDuty 管理者アカウントとして、 を有効にした組織のメンバーアカウント別に分類された推定月額使用コストを表示できます GuardDuty。

GuardDuty で を有効にすると AWS アカウント、次のセクションで説明するログソースのモニタリングが自動的に開始されます。がこれらのデータソースの分析と処理を開始 GuardDuty して関連するセキュリティ検出結果を生成するために、他のものを有効にする必要はありません。

トピック

- AWS CloudTrail イベントログ
- AWS CloudTrail 管理イベント
- VPC Flow Logs
- DNS ログ

AWS CloudTrail イベントログ

AWS CloudTrail は AWS Management Console、、 SDK、コマンドラインツール、特定の AWS サービスを使用して行われた AWS API コールなど、 アカウントの API コールの履歴を提供します。 CloudTrail また、 は、 をサポートするサービスの AWS APIs を呼び出したユーザーとアカウント CloudTrail、呼び出し元の IP アドレス、呼び出しが呼び出された時刻を特定するのにも役立ちます。 AWS SDKs 詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrailとは」を参照してください。

GuardDuty は CloudTrail 管理イベントもモニタリングします。を有効にすると GuardDuty、イベントの独立した重複ストリーム CloudTrail を介して から直接 CloudTrail 管理イベントの使用が開始さ

れ、 CloudTrail イベントログが分析されます。が に記録されたイベント GuardDuty にアクセスする場合、追加料金は発生しません CloudTrail。

GuardDuty は CloudTrail イベントを管理したり、既存の CloudTrail 設定に影響を与えたりしません。同様に、 CloudTrail 設定は がイベントログを GuardDuty 消費して処理する方法には影響しません。 CloudTrail イベントへのアクセスと保持を管理するには、 CloudTrail サービスコンソールまたは API を使用します。詳細については、「 AWS CloudTrail ユーザーガイド」の「イベント履歴を含む CloudTrail イベントの表示」を参照してください。

が AWS CloudTrail グローバルイベント GuardDuty を処理する方法

ほとんどの AWS サービスでは、 CloudTrail イベントは作成された AWS リージョン に記録されます。 AWS Identity and Access Management (IAM) AWS Security Token Service 、 (AWS STS) 、Amazon Simple Storage Service (Amazon S3) CloudFront、Amazon 、Amazon Route 53 (Route 53) などのグローバルサービスでは、イベントは発生したリージョンでのみ生成されますが、グローバルに重要です。

は、ネットワーク設定やユーザーアクセス許可などのセキュリティ値を持つ CloudTrail グローバルサービスイベントを GuardDuty 消費し、それらのイベントをレプリケートして、 を有効にした各リージョンで処理します GuardDuty。この動作は、各リージョンのユーザープロファイルとロールプロファイル GuardDuty を維持するのに役立ちます。これは、異常なイベントを検出するのに不可欠です。

で有効 AWS リージョン になっているすべての GuardDuty で を有効にすることを強くお勧めします AWS アカウント。これにより、アクティブに使用していない可能性のあるリージョンでも、不正または異常なアクティビティに関する検出結果 GuardDuty が生成されます。

AWS CloudTrail 管理イベント

管理イベントは、コントロールプレーンイベントとも呼ばれます。これらのイベントは、 AWS アカウントのリソースで実行される管理オペレーションに関するインサイトを提供します。

以下は、 がモニタリングする CloudTrail GuardDuty管理イベントの例です。

- セキュリティの設定 (IAM `AttachRolePolicy` API オペレーション)
- データをルーティングするルールの設定 (Amazon EC2 `CreateSubnet` API オペレーション)
- ログ記録の設定 (AWS CloudTrail `CreateTrail` API オペレーション)

VPC Flow Logs

Amazon VPC の VPC フローログ機能は、 AWS 環境内の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされたネットワークインターフェイスとの間で送受信される IP トラフィックに関する情報をキャプチャします。

を有効にすると GuardDuty、アカウント内の Amazon EC2 インスタンスから VPC フローログの分析がすぐに開始されます。GuardDuty は、フローログの単独ストリームおよび重複ストリームを通じて、VPC フローログ機能から直接、VPC フローログイベントを消費します。このプロセスによる既存のフローログ設定への影響はありません。

GuardDuty Lambda 保護

Lambda Protection は、Amazon に対するオプションの強化です GuardDuty。現在、Lambda Network Activity Monitoring には、VPC ネットワークを使用しないログも含め、アカウントのすべての Lambda 関数からの Amazon VPC フローログが含まれています。Lambda 関数を潜在的なセキュリティ脅威から保護するには、 GuardDuty アカウントで Lambda Protection を設定する必要があります。詳細については、「GuardDuty Lambda 保護」を参照してください。

でのランタイムモニタリング GuardDuty

EC2 インスタンスの EKS Runtime Monitoring または Runtime Monitoring でセキュリティエージェントを (手動または を介して GuardDuty) 管理し、現在 Amazon EC2 インスタンスにデプロイされ、このインスタンス収集されたランタイムイベントタイプから を受け取った場合、GuardDuty はこの Amazon EC2 インスタンスからの VPC フローログの分析 AWS アカウント に対して に課金 GuardDuty しません。これにより、アカウントの 2 倍の使用コスト GuardDuty を回避できます。

GuardDuty は、フローログを管理したり、アカウントでアクセスできるようにしたりしません。フローログのアクセスと保持期間を管理するには、VPC フローログ機能を設定する必要があります。

DNS ログ

Amazon EC2 インスタンスに AWS DNS リゾルバーを使用する場合 (デフォルト設定) 、GuardDuty は内部 DNS リゾルバーを介してリクエストとレスポンスの AWS DNS ログにアクセスして処理できます。OpenDNS や GoogleDNS などの別の OpenDNS リゾルバーを使用する場合、または独自の DNS リゾルバーを設定した場合、 はこのデータソースのデータにアクセスして処理 GuardDuty することはできません。 GoogleDNS

を有効にすると GuardDuty、すぐに独立したデータストリームから DNS ログの分析が開始されます。このデータストリームは、Route 53 リゾルバークエリログ記録機能を通じて提供されるデータとは別のものです。この機能の設定は分析には影響 GuardDutyしません。

> **Note**
>
> GuardDuty は、 で起動された Amazon EC2 インスタンスの DNS ログのモニタリングをサポートしていません。これは、 Amazon Route 53 Resolver クエリログ記録機能がその環境で使用できない AWS Outposts ためです。

Amazon での EKS Protection GuardDuty

EKS 監査ログのモニタリングは、Amazon Elastic Kubernetes Service (Amazon EKS) 内の EKS クラスターの疑わしいアクティビティの可能性を検出するのに役立ちます。EKS Audit Log Monitoring は、EKS 監査ログを使用して、ユーザー、Kubernetes API を使用するアプリケーション、およびコントロールプレーンからの時系列アクティビティをキャプチャします。詳細については、「EKS 監査ログのモニタリング」を参照してください。

> **Note**
>
> EKS Runtime Monitoring は Runtime Monitoring の一部として管理されます。詳細については、「でのランタイムモニタリング GuardDuty」を参照してください。

EKS Protection の機能

EKS 監査ログのモニタリング

EKS 監査ログは、ユーザー、Kubernetes API を使用するアプリケーション、コントロールプレーンからのアクティビティなど、Amazon EKS クラスター内のシーケンシャルアクションをキャプチャします。監査ログは、すべての Kubernetes クラスターのコンポーネントです。

詳細については、Kubernetes ドキュメントの「監査」を参照してください。

Amazon EKS では、EKS コントロールプレーンのログ記録機能を使用して EKS 監査ログを Amazon CloudWatch Logs として取り込むことができます。Amazon EKS コントロールプレーンのログ記録を管理 GuardDuty したり、Amazon EKS に対して EKS 監査ログを有効にしていない場合は、アカウントで EKS 監査ログにアクセスしたりすることはできません。EKS 監査ログへのアクセスと保持を管理するには、Amazon EKS コントロールプレーンのログ記録機能を設定する必要があります。詳細については、「Amazon EKS ユーザーガイド」の「コントロールプレーンログの有効化と無効化」を参照してください。

EKS 監査ログのモニタリングの設定については、「EKS 監査ログのモニタリング」を参照してください。

EKS 監査ログのモニタリング

EKS 監査ログのモニタリングは、Amazon Elastic Kubernetes Service 内の EKS クラスターで疑わしいと思われるアクティビティを検出するのに役立ちます。EKS 監査ログのモニタリングを有効にすると、 GuardDuty はすぐに Amazon EKS クラスターEKS 監査ログのモニタリングからのモニタリングを開始し、悪意のあるアクティビティや疑わしいアクティビティがないか分析します。Kubernetes 監査ログイベントは、監査ログの独立した重複ストリームを介して、Amazon EKS コントロールプレーンのログ記録機能から直接消費されます。このプロセスでは、追加の設定は不要で、既存の Amazon EKS コントロールプレーンのログ設定 (存在する場合) に影響はありません。

EKS 監査ログのモニタリングを無効にすると、 は Amazon EKS リソースの EKS 監査ログのモニタリングと分析を GuardDuty 直ちに停止します。

EKS 監査ログのモニタリング GuardDuty は、 AWS リージョン が利用可能なすべての で利用できるとは限りません。詳細については、「リージョン固有機能の可用性」を参照してください。

30 日間の無料トライアル期間が GuardDuty アカウントに与える影響

- GuardDuty を初めて有効にすると、EKS 監査ログのモニタリングは既に 30 日間の無料トライアル期間に含まれています。
- 30 日間の無料トライアルが終了した既存の GuardDuty アカウントは、30 日間の無料トライアル期間で初めて EKS 監査ログのモニタリングを有効にできます。

スタンドアロンアカウントの EKS 監査ログのモニタリングの設定

任意のアクセス方法を選択して、スタンドアロンアカウントのために EKS 監査ログモニタリングを有効または無効にします。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[EKS Protection] を選択します。
3. [設定] タブでは、EKS 監査ログのモニタリングの現在の設定ステータスを確認できます。[EKS 監査ログモニタリング] セクションで、[有効にする] を選択して EKS 監査ログモニタリング機能を有効にするか、または [無効にする] を選択して無効にします。
4. [保存] を選択します。

API/CLI

- 委任された GuardDuty 管理者アカウントのリージョンレベルのディテクター ID を使用して updateDetector API オペレーションを実行し、`features`オブジェクト名を として`EKS_AUDIT_LOGS`、ステータスを `ENABLED`または として渡します`DISABLED`。

  または、 AWS CLI コマンドを実行する EKS 監査ログのモニタリングを有効または無効にすることもできます。次のサンプルコードは、 GuardDuty EKS 監査ログのモニタリングを有効にします。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
  ```

マルチアカウント環境での EKS 監査ログのモニタリングの設定

マルチアカウント環境では、委任された GuardDuty 管理者アカウントのみが、組織内のメンバーアカウントの EKS 監査ログのモニタリング機能を有効または無効にすることができます。GuardDuty メンバーアカウントは、自分のアカウントからこの設定を変更することはできません。委任 GuardDuty 管理者アカウントは、 を使用してメンバーアカウントを管理します AWS Organizations。この委任された GuardDuty 管理者アカウントは、組織に参加するすべての新しいアカウントの EKS 監査ログのモニタリングを自動有効化することを選択できます。マルチアカウント環境の詳細については、「Amazon での複数のアカウントの管理 GuardDuty」を参照してください。

委任された GuardDuty 管理者アカウントの EKS 監査ログのモニタリングの設定

任意のアクセス方法を選択して、委任された GuardDuty 管理者アカウントの EKS 監査ログのモニタリングを設定します。

Console

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

   必ず管理アカウントの認証情報を使用してください。
2. ナビゲーションペインで、[EKS Protection] を選択します。

3. [設定] タブでは、各セクションにおける EKS 監査ログのモニタリングの現在の設定ステータスを確認できます。委任された GuardDuty 管理者アカウントの設定を更新するには、EKS 監査ログのモニタリングペインで編集を選択します。
4. 次のいずれかを行います。

   [すべてのアカウントについて有効にする] の使用

   - [すべてのアカウントについて有効にする] を選択します。これにより、 AWS 組織に参加する新しい GuardDuty アカウントを含め、組織内のすべてのアクティブなアカウントに対して保護プランが有効になります。
   - [保存] を選択します。

   [アカウントを手動で設定] の使用

   - 委任された GuardDuty 管理者アカウントアカウントに対してのみ保護プランを有効にするには、アカウントを手動で設定を選択します。
   - 委任された GuardDuty 管理者アカウント (このアカウント) セクションで 有効化 を選択します。
   - [保存] を選択します。

API/CLI

ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト `name` を `EKS_AUDIT_LOGS` として、`status` を `ENABLED` または `DISABLED` として渡して、updateDetector API オペレーションを実行します。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

次の AWS CLI コマンドを実行すると、EKS 監査ログのモニタリングを有効または無効にできます。委任 GuardDuty 管理者アカウントの有効な`###### ID` を使用してください。

> **Note**
>
> 次のサンプルコードは EKS 監査ログのモニタリングを有効にします。`12abc34d567e8fa901bc2d34e56789f0` `detector-id`を委任 GuardDuty 管理者

アカウントの に、*555555555555* を AWS アカウント 委任 GuardDuty 管理者アカウントの に置き換えてください。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 555555555555 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

EKS 監査ログモニタリングを無効にするには、ENABLED を DISABLED に置き換えます。

すべてのメンバーアカウントの EKS 監査ログのモニタリングを自動で有効にする

任意のアクセス方法を選択して、組織内の既存のメンバーアカウントの EKS 監査ログのモニタリングを有効にします。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。
2. 次のいずれかを行います。

   [EKS Protection] ページの使用

   1. ナビゲーションペインで、[EKS Protection] を選択します。
   2. [設定] タブでは、組織内のアクティブなメンバーアカウントの EKS 監査ログのモニタリングの現在のステータスを確認できます。

      EKS 監査ログモニタリング設定を更新するには、[編集] を選択します。
   3. [すべてのアカウントについて有効にする] を選択します。このアクションにより、組織内の既存のアカウントと新しいアカウントの両方について EKS 監査ログモニタリングが自動的に有効になります。
   4. [保存] を選択します。

> **Note**
>
> メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

[アカウント] ページの使用

1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
2. [アカウント] ページで、[招待によるアカウントの追加] の前に [自動有効化] の詳細設定を選択します。
3. [自動有効化の詳細設定を管理] ウィンドウで、[EKS 監査ログモニタリング] の下の [すべてのアカウントについて有効にする] を選択します。
4. [保存] を選択します。

[すべてのアカウントについて有効にする] オプションを使用できず、組織内の特定のアカウントのために EKS 監査ログモニタリング設定をカスタマイズする場合は、「メンバーアカウントの EKS 監査ログのモニタリングを選択的に有効または無効にする」を参照してください。

API/CLI

- メンバーアカウントの EKS 監査ログのモニタリングを選択的に有効または無効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを呼び出します。
- 次の例では、単一のメンバーアカウントで EKS 監査ログのモニタリングを有効にする方法を示しています。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

すべての既存のアクティブなメンバーアカウントのために EKS 監査ログモニタリングを有効にする

任意のアクセス方法を選択して、組織内のすべての既存のアクティブなメンバーアカウントの EKS 監査ログのモニタリングを有効にします。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任 GuardDuty 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[EKS Protection] を選択します。
3. EKS Protection ページで、 GuardDuty実行型マルウェアスキャン設定の現在のステータスを表示できます。[アクティブなメンバーアカウント] セクションで、[アクション] を選択します。
4. [アクション] ドロップダウンメニューから、[すべての既存のアクティブなメンバーアカウントについて有効にする] を選択します。
5. [保存] を選択します。

API/CLI

- メンバーアカウントの EKS 監査ログのモニタリングを選択的に有効または無効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを呼び出します。
- 次の例では、単一のメンバーアカウントで EKS 監査ログのモニタリングを有効にする方法を示しています。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

新しいメンバーアカウントの EKS 監査ログのモニタリングを自動で有効にする

新しく追加されたメンバーアカウントは、 GuardDuty実行型マルウェアスキャンの設定を選択する前に を有効にする GuardDuty 必要があります。招待によって管理されるメンバーアカウントは、アカウントに対して GuardDuty実行型マルウェアスキャンを手動で設定できます。詳細については、「Step 3 - Accept an invitation」を参照してください。

任意のアクセス方法を選択して、組織に参加する新規アカウントの EKS 監査ログのモニタリングを有効にします。

Console

委任された GuardDuty 管理者アカウントは、EKS 監査ログのモニタリングページまたはアカウントページを使用して、組織内の新しいメンバーアカウントの EKS 監査ログのモニタリングを有効にできます。

新しいメンバーアカウントの EKS 監査ログのモニタリングを自動で有効にするには

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。

2. 次のいずれかを行います。

- [EKS Protection] ページを使用する場合:

  1. ナビゲーションペインで、[EKS Protection] を選択します。
  2. [EKS Protection] ページで、[EKS 監査ログモニタリング] の [編集] を選択します。
  3. [アカウントを手動で設定] を選択します。
  4. [新しいメンバーアカウントについて自動的に有効にする] を選択します。このステップにより、新しいアカウントが組織に参加するたびに、そのアカウントのために EKS 監査ログモニタリングが自動的に有効になります。この設定を変更できるのは、組織の委任 GuardDuty 管理者アカウントのみです。
  5. [保存] を選択します。

- [Accounts] (アカウント) ページを使用する場合:

  1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
  2. [アカウント] ページで、[自動有効化] 設定を選択します。
  3. [自動有効化の詳細設定を管理] ウィンドウで、[EKS 監査ログモニタリング] の下の [新しいアカウントについて有効にする] を選択します。
  4. [保存] を選択します。

API/CLI

- 新しいアカウントの EKS 監査ログのモニタリングを選択的に有効または無効にするには、自分の`###### ID` を使用し、UpdateOrganizationConfiguration API オペレーションを実行します。
- 次の例では、組織に参加する新規メンバーの EKS 監査ログのモニタリングを有効にする方法を示しています。スペースで区切られたアカウント ID のリストを渡すこともできます。

  アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

メンバーアカウントの EKS 監査ログのモニタリングを選択的に有効または無効にする

任意のアクセス方法を選択して、組織内の選択的メンバーアカウントの EKS 監査ログのモニタリングを有効または無効にします。

Console

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。
2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

   [アカウント] ページで、[EKS 監査ログのモニタリング] 列でメンバーアカウントのステータスを確認します。
3. EKS 監査ログのモニタリングを有効または無効にするには

   EKS 監査ログのモニタリング用に設定するアカウントを選択します。一度に複数のアカウントを選択できます。[保護プランの編集] ドロップダウンで [EKS 監査ログのモニタリング] を選択し、適切なオプションを選択します。

API/CLI

メンバーアカウントの EKS 監査ログのモニタリングを選択的に有効または無効にするには、自身の*###### ID* を使用し、updateMemberDetectors API オペレーションを呼び出します。

次の例では、単一のメンバーアカウントで EKS 監査ログのモニタリングを有効にする方法を示しています。無効にするには、`ENABLED` を `DISABLED` に置き換えます。スペースで区切られたアカウント ID のリストを渡すこともできます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Amazon での Lambda Protection GuardDuty

Lambda Protection は、 AWS 環境内で AWS Lambda 関数が呼び出されたときに潜在的なセキュリティ脅威を特定するのに役立ちます。Lambda Protection を有効にすると、 は、VPC ネットワークを使用しないログを含むアカウントのすべての Lambda 関数VPC Flow Logsから開始して、Lambda 関数が呼び出されたときに生成される Lambda ネットワークアクティビティログのモニタリング GuardDuty を開始します。が Lambda 関数に悪意のある可能性のあるコードが存在することを示す疑わしいネットワークトラフィック GuardDuty を識別すると、 GuardDuty は検出結果を生成します。

> **Note**
>
> Lambda Network Activity Monitoring には Lambda@Edge 関数のログは含まれません。

Lambda Protection は AWS リージョン、任意のアカウントまたは利用可能な に対していつでも設定できます。デフォルトでは、既存の GuardDuty アカウントは 30 日間のトライアル期間で Lambda Protection を有効にできます。新しい GuardDuty アカウントの場合、Lambda Protection は既に有効になっており、30 日間のトライアル期間に含まれています。使用情報の詳細については、「コストの見積もり」を参照してください。

GuardDuty は、Lambda 関数を呼び出すことによって生成されたネットワークアクティビティログをモニタリングします。現在、Lambda Network Activity Monitoring には、VPC ネットワークを使用しないログを含め、アカウントのすべての Lambda 関数からの Amazon VPC フローログが含まれており、Lambda 関数を呼び出すことによって生成される DNS クエリデータなどの他のネットワークアクティビティへの拡張など、変更される可能性があります。他の形式のネットワークアクティビティモニタリングへの拡張により、Lambda Protection で処理されるデータ量が増え GuardDuty ます。これは Lambda Protection の使用コストに直接影響します。が追加のネットワークアクティビティログのモニタリング GuardDuty を開始するたびに、リリースの少なくとも 30 日前に Lambda Protection を有効にしたアカウントに通知が送信されます。

Lambda Protection の機能

Lambda Network Activity Monitoring

Lambda Protection を有効にすると、アカウントに関連付けられた Lambda 関数が呼び出されたときに生成された Lambda ネットワークアクティビティログが によって GuardDuty モニタリングさ

れます。これにより、Lambda 関数に対する潜在的なセキュリティ脅威を検出できます。 は、VPC ネットワークを使用しない関数を含め、すべての Lambda 関数からの VPC フローログ GuardDuty を監視します。VPC ネットワークを使用するように設定された Lambda 関数の場合、Lambda for によって作成された Elastic Network Interface (ENI) の VPC フローログを有効にする必要はありません GuardDuty。 GuardDuty は、検出結果を生成するために処理された Lambda ネットワークアクティビティログデータの量 (GB 単位) に対してのみ課金します。スマートフィルターを適用し、脅威検出に関連する Lambda ネットワークアクティビティログのサブセットを分析することでコスト GuardDuty を最適化します。料金の詳細については、「Amazon の GuardDuty 料金」を参照してください。

GuardDuty は、Lambda ネットワークアクティビティログ (VPC および VPC 以外のフローログを含む) を管理したり、アカウントでアクセスできるようにしたりしません。

Lambda Protection の設定

スタンドアロンアカウントの Lambda Protection の設定

に関連付けられているアカウントの場合 AWS Organizations、次のセクションで説明するように、コンソールまたは API の手順を使用して GuardDutyこのプロセスを自動化できます。

任意のアクセス方法を選択して、スタンドアロンアカウントの Lambda Protection を有効または無効にします。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインの [設定] で、[Lambda Protection] を選択します。
3. [Lambda Protection] ページにアカウントの現在のステータスが表示されます。[Enable] (有効化) または [Disable] (無効化) を選択することで、いつでもこの機能を有効または無効にできます。
4. [保存] を選択します。

API/CLI

ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト `name` を `LAMBDA_NETWORK_LOGS` として、`status` を `ENABLED` または `DISABLED` として渡して、updateDetector API オペレーションを実行します。

次の AWS CLI コマンドを実行して、Lambda Network Activity Monitoring を有効または無効にすることもできます。必ずご自身の有効な *###### ID* を使用してください。

> **Note**
>
> 次のサンプルコードは Lambda Network Activity Monitoring を有効にします。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]'
```

マルチアカウント環境での Lambda Protection の設定

マルチアカウント環境では、委任された GuardDuty 管理者アカウントのみが、組織内のメンバーアカウントの Lambda Protection を有効または無効にすることができます。 GuardDuty メンバーアカウントは、自分のアカウントからこの設定を変更することはできません。委任 GuardDuty 管理者アカウントは、 を使用してメンバーアカウントを管理します AWS Organizations。委任された GuardDuty 管理者アカウントは、組織に参加するすべての新しいアカウントに対して Lambda Network Activity Monitoring を自動有効化することを選択できます。マルチアカウント環境の詳細については、「Amazon での複数のアカウントの管理」を参照してください GuardDuty。

委任 GuardDuty 管理者アカウントの Lambda Protection の設定

任意のアクセス方法を選択して、委任された GuardDuty 管理者アカウントの Lambda Network Activity Monitoring を有効または無効にします。

Console

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

   必ず管理アカウントの認証情報を使用してください。
2. ナビゲーションペインの [設定] で、[Lambda Protection] を選択します。
3. [Lambda Protection] ページで、[編集] を選択します。

4. 次のいずれかを行います。

   [すべてのアカウントについて有効にする] の使用

   - [すべてのアカウントについて有効にする] を選択します。これにより、 AWS 組織に参加する新しい GuardDuty アカウントを含め、組織内のすべてのアクティブなアカウントに対して保護プランが有効になります。
   - [保存] を選択します。

   [アカウントを手動で設定] の使用

   - 委任された GuardDuty 管理者アカウントアカウントに対してのみ保護プランを有効にするには、アカウントを手動で設定を選択します。
   - 委任された GuardDuty 管理者アカウント (このアカウント) セクションで 有効化 を選択します。
   - [保存] を選択します。

API/CLI

ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト `name` を `LAMBDA_NETWORK_LOGS` として、`status` を `ENABLED` または `DISABLED` として渡して、updateDetector API オペレーションを実行します。

次の AWS CLI コマンドを実行すると、Lambda Network Activity Monitoring を有効または無効にできます。委任 GuardDuty 管理者アカウントの有効な`###### ID` を使用してください。

> **Note**
>
> 次のサンプルコードは Lambda Network Activity Monitoring を有効にします。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 555555555555 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Lambda Network Activity Monitoring をすべてのメンバーアカウントで Lambda Network Activity Monitoring を自動で有効にする

任意のアクセス方法を選択して、すべてのメンバーアカウントのために Lambda ネットワークアクティビティモニタリング機能を有効にします。これには、既存のメンバーアカウントと、組織に参加する新しいアカウントが含まれます。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。

2. 次のいずれかを行います。

   [Lambda Protection] ページの使用

   1. ナビゲーションペインで、[Lambda Protection] を選択します。
   2. [すべてのアカウントについて有効にする] を選択します。このアクションにより、組織内の既存のアカウントと新しいアカウントの両方について Lambda ネットワークアクティビティモニタリングが自動的に有効になります。
   3. [保存] を選択します。

      > **Note**
      >
      > メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

   [アカウント] ページの使用

   1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
   2. [アカウント] ページで、[招待によるアカウントの追加] の前に [自動有効化] の詳細設定を選択します。

3. [自動有効化の詳細設定を管理] ウィンドウで、[Lambda ネットワークアクティビティモニタリング] の下の [すべてのアカウントについて有効にする] を選択します。

> **Note**
>
> デフォルトでは、このアクションは新しいメンバーアカウント GuardDuty の自動有効化オプションを自動的にオンにします。

4. [保存] を選択します。

[すべてのアカウントについて有効にする] オプションを使用できない場合は、「メンバーアカウントで Lambda Network Activity Monitoring を選択的に有効または無効にする」を参照してください。

API/CLI

- メンバーアカウントの Lambda Network Activity Monitoring を選択的に有効または無効にするには、独自の`###### ID` を使用して updateMemberDetectors API オペレーションを呼び出します。
- 次の例では、単一のメンバーアカウントで Lambda Network Activity Monitoring を有効にする方法を示します。メンバーアカウントを無効にするには、`DISABLED` を `ENABLED` に置き換えてください。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  スペースで区切られたアカウント ID のリストを渡すこともできます。
- コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

すべての既存のアクティブなメンバーアカウントのために Lambda ネットワークアクティビティモニタリングを有効にする

任意のアクセス方法を選択して、組織内のすべての既存のアクティブなメンバーアカウントの Lambda Network Activity Monitoring を有効にします。

Console

すべての既存のアクティブなメンバーアカウントのために Lambda ネットワークアクティビティモニタリングを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任 GuardDuty 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[Lambda Protection] を選択します。
3. [Lambda Protection] ページでは、設定の現在のステータスを表示できます。[アクティブなメンバーアカウント] セクションで、[アクション] を選択します。
4. [アクション] ドロップダウンメニューから、[すべての既存のアクティブなメンバーアカウントについて有効にする] を選択します。
5. [確認] を選択します。

API/CLI

- メンバーアカウントの Lambda Network Activity Monitoring を選択的に有効または無効にするには、独自の`###### ID` を使用して updateMemberDetectors API オペレーションを呼び出します。
- 次の例では、単一のメンバーアカウントで Lambda Network Activity Monitoring を有効にする方法を示します。メンバーアカウントを無効にするには、`DISABLED` を `ENABLED` に置き換えてください。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

Lambda Network Activity Monitoring を新しいメンバーアカウントで Lambda Network Activity Monitoring を自動で有効にする

任意のアクセス方法を選択して、組織に参加する新しいアカウントの Lambda Network Activity Monitoring を有効にします。

Console

委任 GuardDuty 管理者アカウントは、Lambda Protection ページまたは Accounts ページを使用して、組織内の新しいメンバーアカウントの Lambda Network Activity Monitoring を有効にできます。

Lambda Network Activity Monitoring を新しいメンバーアカウントで Lambda Network Activity Monitoring を自動で有効にするには

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。
2. 次のいずれかを行います。
   - [Lambda Protection] ページの使用:

     1. ナビゲーションペインで、[Lambda Protection] を選択します。
     2. [Lambda Protection] ページで、[編集] を選択します。
     3. [アカウントを手動で設定] を選択します。
     4. [新しいメンバーアカウントについて自動的に有効にする] を選択します。このステップにより、新しいアカウントが組織に参加するたびに、そのアカウントのために Lambda Protection が自動的に有効になります。この設定を変更できるのは、組織の委任 GuardDuty 管理者アカウントのみです。
     5. [保存] を選択します。
   - [Accounts] (アカウント) ページを使用する場合:

     1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

2. [アカウント] ページで、[自動有効化] 設定を選択します。
3. [自動有効化の詳細設定を管理] ウィンドウで、[Lambda ネットワークアクティビティモニタリング] の下の [新しいアカウントについて有効にする] を選択します。
4. [保存] を選択します。

API/CLI

- 新しいメンバーアカウントの Lambda Network Activity Monitoring を有効または無効にするには、独自の`###### ID` を使用して UpdateOrganizationConfiguration API オペレーションを呼び出します。
- 次の例では、単一のメンバーアカウントで Lambda Network Activity Monitoring を有効にする方法を示します。無効にするには、「メンバーアカウントで Lambda Network Activity Monitoring を選択的に有効または無効にする」を参照してください。組織に参加する新規アカウントすべてに対して有効にしたくない場合は、`AutoEnable` を `NONE` に設定します。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

  スペースで区切られたアカウント ID のリストを渡すこともできます。
- コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

メンバーアカウントで Lambda Network Activity Monitoring を選択的に有効または無効にする

任意のアクセス方法を選択して、メンバーアカウントの Lambda Network Activity Monitoring を選択的に有効または無効にします。

Console

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

委任された GuardDuty 管理者アカウントの認証情報を使用してください。

2. ナビゲーションペインで 設定の アカウントを選択します。

   [アカウント] ページで、[Lambda Network Activity Monitoring] 列を確認します。Lambda Network Activity Monitoring が有効になっているかどうかを示します。

3. Lambda Protection を設定するアカウントを選択します。一度に複数のアカウントを選択できます。
4. [保護プランの編集] ドロップダウンメニューから [Lambda Network Activity Monitoring] を選択し、適切なアクションを選択します。

API/CLI

独自の*###### ID* を使用して updateMemberDetectors API を呼び出します。

次の例では、単一のメンバーアカウントで Lambda Network Activity Monitoring を有効にする方法を示します。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

スペースで区切られたアカウント ID のリストを渡すこともできます。

コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

Amazon での EC2 のマルウェア保護 GuardDuty

Malware Protection for EC2 は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスとコンテナワークロードにアタッチされている Amazon Elastic Block Store (Amazon EBS) ボリュームをスキャンして、マルウェアの潜在的な存在を検出するのに役立ちます。Amazon EC2 Malware Protection for EC2 には、スキャン時に特定の Amazon EC2 インスタンスとコンテナワークロードを含めるか除外するかを決定できるスキャンオプションが用意されています。また、Amazon EC2 インスタンスまたはコンテナワークロードにアタッチされた Amazon EBS ボリュームのスナップショットを GuardDuty アカウント内に保持するオプションも提供します。スナップショットは、マルウェアが発見され、Malware Protection for EC2 の検出結果が生成された場合にのみ保持されます。

Malware Protection for EC2 には、Amazon EC2 インスタンスとコンテナワークロードでの潜在的に悪意のあるアクティビティを検出するための 2 種類のスキャンが用意されています。開始されたマルウェアスキャンとオンデマンドのマルウェアスキャンです。 GuardDuty次の表は、両方のスキャンタイプの比較を示しています。

Factor	GuardDutyが開始するマルウェアスキャン	オンデマンドのマルウェアスキャン
スキャンの起動方法	GuardDuty実行型マルウェアスキャンを有効にすると、 が Amazon EC2 インスタンスまたはコンテナワークロードにマルウェアが存在する可能性を示す検出結果 GuardDuty を生成するたびに、 は、影響を受ける可能性のあるリソースにアタッチされた Amazon EBS ボリュームに対してエージェントレスマルウェアスキャン GuardDuty を自動的に開始します。詳細については、「GuardDutyが開始するマルウェアスキャン」を参照してください。	Amazon EC2 インスタンスまたはコンテナワークロードに関連付けされた Amazon リソースネーム (ARN) を指定することで、オンデマンドのマルウェアスキャンを開始できます。リソースの結果 GuardDuty が生成されない場合でも、オンデマンドのマルウェアスキャンを開始できます。詳細については、「オンデマンドのマルウェアスキャン」を参照してください。

Factor	GuardDutyが開始するマルウェアスキャン	オンデマンドのマルウェアスキャン
設定が必要です	GuardDuty実行型マルウェアスキャンを使用するには、アカウントで有効にする必要があります。詳細については、「GuardDutyが開始するマルウェアスキャンの設定」を参照してください。	アカウントで GuardDuty が有効になっている必要があります。オンデマンドのマルウェアスキャンを使用するには、機能レベルで設定は必要ありません。
新しいスキャンを開始するまでの待ち時間	が 1 つ GuardDuty を生成するたびに GuardDuty実行型マルウェアスキャンを呼び出す検出結果、マルウェアスキャンは 24 時間に 1 回のみ自動的に開始されます。	オンデマンドマルウェアスキャンは、前回のスキャンの開始時刻から 1 時間後にいつでも同じリソースで開始できます。
30 日間の無料トライアル期間の利用可能性	アカウントで初めて GuardDuty実行型マルウェアスキャンを有効にすると、30 日間の無料トライアル期間* を使用できます。 GuardDuty実行型マルウェアスキャンの詳細については、「」を参照してください30 日間の無料トライアル。	新規または既存の GuardDuty アカウントのオンデマンドマルウェアスキャンには、無料トライアル期間* はありません。

Factor	GuardDutyが開始するマルウェアスキャン	オンデマンドのマルウェアスキャン
スキャンオプション	GuardDuty実行型マルウェアスキャンを設定した後、Malware Protection for EC2 はスキャンまたはスキップするリソースを選択するのにも役立ちます。Malware Protection for EC2 は、スキャンから除外するリソースに対して自動スキャンを開始しません。	オンデマンドのマルウェアスキャンは、 グローバルタグ をサポートしますGuardDuty Excluded 。リソース ARN を手動で指定するため、ユーザー定義タグ付きのスキャンオプションはオンデマンドのマルウェアスキャンには適用されません。

*EBS ボリュームスナップショットの作成およびスナップショットの保持には使用料が発生します。スナップショットを保持するようにアカウントを設定する方法の詳細については、「」を参照してくださいスナップショットの保持。

EC2 の Malware Protection は に対するオプションの強化であり GuardDuty、リソースのパフォーマンスに影響を与えないように設計されています。Malware Protection for EC2 が 内でどのように機能するかについては GuardDuty、「」を参照してくださいMalware Protection for EC2 の機能。さまざまな での Malware Protection for EC2 の可用性については AWS リージョン、「」を参照してくださいリージョンとエンドポイント。

> **Note**
>
> GuardDuty EC2 の Malware Protection は、Amazon EKS または Amazon ECS のいずれかで Fargate をサポートしていません。

Malware Protection for EC2 の機能

Elastic Block Storage (EBS) ボリューム

このセクションでは、 GuardDuty実行型マルウェアスキャンとオンデマンドマルウェアスキャンの両方を含む EC2 の Malware Protection が、Amazon EC2 インスタンスとコンテナワークロードに関

連付けられた Amazon EBS ボリュームをスキャンする方法について説明します。先に進む前に、次のカスタマイズを検討してください。

- スキャンオプション – Malware Protection for EC2 には、Amazon EC2 インスタンスと Amazon EBS ボリュームをスキャンプロセスに含めるか除外するかのいずれかのタグを指定する機能があります。 GuardDuty開始のマルウェアスキャンのみが、ユーザー定義タグを含むスキャンオプションをサポートします。 GuardDuty実行型マルウェアスキャンとオンデマンドマルウェアスキャンの両方が グローバル`GuardDutyExcluded`タグをサポートします。詳細については、「ユーザー定義タグ付きのスキャンオプション」を参照してください。
- スナップショットの保持 — Malware Protection for EC2 には、Amazon EBS ボリュームのスナップショットを AWS アカウント内に保持するオプションが用意されています。デフォルトでは、このオプションは無効になっています。 GuardDuty 開始されたマルウェアスキャンとオンデマンドのマルウェアスキャンの両方で、スナップショットの保持をオプトインできます。詳細については、「スナップショットの保持」を参照してください。

Amazon EC2 インスタンスまたはコンテナワークロードにマルウェアが存在する可能性を示す検出結果 GuardDuty を生成し、Malware Protection for EC2 内で GuardDuty 開始されたスキャンタイプを有効にした場合、スキャンオプションに基づいて GuardDuty実行されたマルウェアスキャンが呼び出される可能性があります。

Amazon EC2 インスタンスに関連付けされた Amazon EBS ボリュームにオンデマンドのマルウェアスキャンを開始するには、Amazon EC2 インスタンスの Amazon リソースネーム (ARN) を指定します。

オンデマンドのマルウェアスキャン、または自動的に呼び出される GuardDuty実行型マルウェアスキャンへの応答として、 GuardDuty は、影響を受ける可能性のあるリソースにアタッチされた関連する EBS ボリュームのスナップショットを作成し、 と共有しますGuardDuty サービスアカウント。これらのスナップショットから、 はサービスアカウントに暗号化されたレプリカ EBS ボリューム GuardDuty を作成します。

スキャンが完了すると、 は暗号化されたレプリカ EBS ボリュームと EBS ボリュームのスナップショット GuardDuty を削除します。マルウェアが発見され、スナップショットの保持設定をオンにした場合、EBS ボリュームのスナップショットは削除されず、自動的に AWS アカウントに保持されます。マルウェアが見つからないとき、スナップショットの保持設定とは関係なく、EBS ボリュームのスナップショットは保持されません。デフォルトでは、スナップショットの保持設定はオフになっています。スナップショットとその保持にかかるコストについては、「Amazon EBS の料金」を参照してください。

GuardDuty は、各レプリカ EBS ボリュームをサービスアカウントに最大 55 時間保持します。サービスが停止した場合、またはレプリカ EBS ボリュームとそのマルウェアスキャンで障害が発生した場合、 はそのような EBS ボリュームを 7 日以内に保持 GuardDuty します。ボリュームの保持期間の延長は、停止または障害をトリアージして対処することです。EC2 の GuardDuty マルウェア保護は、停止または障害に対処した後、または保持期間の延長が経過すると、サービスアカウントからレプリカ EBS ボリュームを削除します。

マルウェアスキャンでサポートされている Amazon EBS ボリューム

AWS リージョン が Malware Protection for EC2 機能 GuardDuty をサポートしているすべての で、暗号化されていない、または暗号化されていない Amazon EBS ボリュームをスキャンできます。AWS マネージドキー または カスタマーマネージドキー のいずれかで暗号化された Amazon EBS ボリュームを持つことができます。現在、 の一部は Amazon EBS ボリュームを暗号化する方法の両方 AWS リージョン をサポートしており、その他はカスタマーマネージドキーのみをサポートしています。

この機能がまだサポートされていない場合の詳細については、「」を参照してください。 China Regions

次のリストでは、Amazon EBS ボリュームが暗号化されているかどうかにかかわらず、 GuardDuty が使用するキーについて説明します。

- 暗号化されていないか、 で暗号化されている Amazon EBS ボリューム AWS マネージドキーは、独自のキー GuardDuty を使用してレプリカ Amazon EBS ボリュームを暗号化します。

  アカウント AWS リージョン が、EBS のデフォルト で暗号化された Amazon EBS ボリュームのスキャンをサポートしていない に属している場合は、 AWS マネージドキー「」を参照してくださいAmazon EBS ボリュームのデフォルト AWS KMS キー ID の変更。
- カスタマーマネージドキーで暗号化された Amazon EBS ボリューム – GuardDuty 同じキーを使用してレプリカ EBS ボリュームを暗号化します。

Malware Protection for EC2 は、 を `productCode`として持つ Amazon EC2 インスタンスのスキャンをサポートしていませんmarketplace。そのような Amazon EC2 インスタンスに対してマルウェアスキャンが開始された場合、スキャンはスキップされます。詳細については、「マルウェアスキャン中にリソースをスキップする理由」の UNSUPPORTED_PRODUCT_CODE_TYPE を参照してください。

Amazon EBS ボリュームのデフォルト AWS KMS キー ID の変更

デフォルトでは、暗号化を に設定し、KMS キー ID を指定しない CreateVolume API を呼び出すtrueと、 は EBS 暗号化のデフォルト AWS KMS キー で暗号化される Amazon EBS ボリュームを作成します。ただし、暗号化キーが明示的に指定されていない場合は、ModifyEbsDefaultKmsKeyIdAPI を呼び出すか、対応する AWS CLI コマンドを使用してデフォルトキーを変更できます。

EBS デフォルトキー ID を変更するには、次の必要な許可を IAM ポリシーに追加します - `ec2:modifyEbsDefaultKmsKeyId`。新しく作成された Amazon EBS ボリュームは、暗号化するように選択したが、関連付けられた KMS キー ID を指定しない場合、デフォルトのキー ID が使用されます。EBS のデフォルトキー ID を更新するには、次のいずれかの方法を使用します。

Amazon EBS ボリュームのデフォルト KMS キー ID を変更するには

次のいずれかを行います。

- API の使用 – ModifyEbsDefaultKmsKeyId API を使用できます。ボリュームの暗号化ステータスを表示する方法については、「Amazon EBS ボリュームの作成」を参照してください。
- AWS CLI コマンドの使用 – 次の例では、KMS キー ID を指定しない場合に Amazon EBS ボリュームを暗号化するデフォルトの KMS キー ID を変更します。リージョンを KM キー ID AWS リージョン の に置き換えてください。

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
id AKIAIOSFODNN7EXAMPLE
```

上記のコマンドは、次の出力と同様な出力を生成します。

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

詳細については、modify-ebs-default-kms「-key-id」を参照してください。

Malware Protection for EC2 のカスタマイズ

このセクションでは、マルウェアスキャンがオンデマンドで開始されたとき、または を介して呼び出されたときに、Amazon EC2 インスタンスまたはコンテナワークロードのスキャンオプションをカスタマイズする方法について説明します GuardDuty。

全般設定

スナップショットの保持

GuardDuty には、EBS ボリュームのスナップショットをアカウント AWS 内に保持するオプションが用意されています。デフォルトでは、スナップショットの保持設定はオフになっています。スナップショットは、スキャン開始前にこの設定をオンにしている場合にのみ保持されます。

スキャンが開始されると、 は EBS ボリュームのスナップショットに基づいてレプリカ EBS ボリューム GuardDuty を生成します。スキャンが完了して、アカウントのスナップショットの保持設定が既にオンになっている場合、マルウェアが見つかって EC2 検出結果タイプの Malware Protection が生成された場合に限り、EBS ボリュームのスナップショットが保持されます。スナップショットの保持設定をオンにしているかどうかにかかわらず、マルウェアが検出されない場合、は EBS ボリュームのスナップショット GuardDuty を自動的に削除します。

スナップショットの使用コスト

マルウェアスキャン中、 は Amazon EBS ボリュームのスナップショット GuardDuty を作成するため、このステップには使用コストがかかります。アカウントのスナップショット保持設定を有効にした場合、マルウェアが検出されてスナップショットが保持されたとき、同様な内容で使用コストが発生します。スナップショットおよびその保持にかかるコストについては、「Amazon EBS 料金」を参照してください。

任意のアクセス方法を選択して、スナップショットの保存設定を有効にします。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインの保護プラン で、EC2 の Malware Protection EC2を選択します。
3. コンソールの下部のセクションで [General settings] (一般設定) を選択します。スナップショットを保持するには、[Snapshots retention] (スナップショットの保持) をオンにします。

API/CLI

1. UpdateMalwareScanSettings を実行して、スナップショット保持設定の現在の設定を更新します。
2. または、次の AWS CLI コマンドを実行して、 GuardDuty Malware Protection for EC2 が検出結果を生成するときにスナップショットを自動的に保持することもできます。

   必ず *detector-id* をご自身の有効な detectorId に置き換えてください。
3. アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

4. スナップショットの保持を無効にしたい場合は、RETENTION_WITH_FINDING を NO_RETENTION に置き換えます。

ユーザー定義タグ付きのスキャンオプション

GuardDuty実行型マルウェアスキャンを使用すると、Amazon EC2 インスタンスと Amazon EBS ボリュームをスキャンおよび脅威検出プロセスに含めたり除外したりするためのタグを指定することもできます。が GuardDuty開始するマルウェアスキャンは、包含タグリストまたは除外タグリストのいずれかでタグを編集することでカスタマイズできます。各リストには、最大 50 個のタグを含めることができます。

EC2 リソースに関連付けられたユーザー定義タグがまだない場合は、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付ける」または「Amazon EC2Amazon EC2 ユーザーガイド」のAmazon EC2 リソースにタグを付ける」を参照してください。 Amazon EC2

> **Note**
>
> オンデマンドのマルウェアスキャンは、ユーザー定義タグ付けされたスキャンオプションをサポートしません。グローバル GuardDutyExcluded タグ をサポートします。

EC2 インスタンスをマルウェアウェアスキャンから除外する方法

スキャンプロセス中に Amazon EC2 インスタンスまたは Amazon EBS ボリューム を除外する場合は、任意の Amazon EC2 インスタンスまたは Amazon EBS ボリューム`true`の `GuardDutyExcluded` タグを に設定でき、 GuardDuty はそれをスキャンしません。`GuardDutyExcluded` タグの詳細については、「Malware Protection for EC2 のサービスにリンクされたロールのアクセス許可」を参照してください。Amazon EC2 インスタンスタグを除外リストに追加することもできます。複数のタグを除外タグリストに追加する場合、これらのタグを少なくとも 1 つ含む Amazon EC2 インスタンスがマルウェアスキャンのプロセスから除外されます。

任意のアクセス方法を選択して、Amazon EC2 インスタンスに関連付けされたタグを除外リストに追加します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインの保護プラン で、EC2 の Malware Protection EC2を選択します。
3. [包含/除外タグ] セクションを展開します。[Add tags (タグの追加)] を選択します。
4. [除外タグ] を選択したら [確認] を選択します。
5. 除外するタグの **`Key`** および **`Value`** ペアを指定します。**`Value`** を指定するかどうかは任意です。すべてのタグを追加したら、[保存] を選択します。

   > **Important**
   >
   > タグのキーと値は大文字と小文字が区別されます。詳細については、Amazon EC2 ユーザーガイド」の「タグの制限」または「Amazon EC2 ユーザーガイド」の「タグの制限」を参照してください。 Amazon EC2

   キーの値が指定されておらず、EC2 インスタンスに指定されたキーがタグ付けされている場合、この EC2 インスタンスは、タグに割り当てられた値に関係なく、 GuardDuty実行型マルウェアスキャンプロセスから除外されます。

API/CLI

- EC2 インスタンスまたはコンテナワークロードをスキャンプロセスから除外することによって、マルウェアスキャン設定を更新します。

次のコマンド AWS CLI 例では、除外タグリストに新しいタグを追加します。必ず *detector-id* の例を、ご自身の有効な detectorId に置き換えてください。

MapEquals は Key/Value ペアの一覧です。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> タグのキーと値は大文字と小文字が区別されます。詳細については、Amazon EC2 ユーザーガイド」の「タグ制限」または「Amazon EC2 ユーザーガイド」の「タグ制限」を参照してください。 Amazon EC2

EC2 インスタンスをマルウェアスキャンに含めるには

EC2 インスタンスをスキャンする場合は、そのタグを包含リストに追加します。包含タグのリストにタグを追加すると、追加されたタグを含まない EC2 インスタンスは、マルウェアスキャン時にスキップされます。複数のタグを包含タグのリストに追加した場合、これらのタグを 1 つでも含む EC2 インスタンスには、マルウェアスキャンが実施されます。場合によっては、スキャンプロセス中に EC2 インスタンスがスキップされることがあります。詳細については、「マルウェアスキャン中にリソースをスキップする理由」を参照してください。

任意のアクセス方法を選択して、EC2 インスタンスに関連付けられているタグを包含リストに追加します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインの保護プラン で、EC2 の Malware Protection EC2を選択します。

3. [包含/除外タグ] セクションを展開します。[Add tags (タグの追加)] を選択します。
4. [包含タグ] を選択したら [確認] を選択します。
5. [Add new inclusion tag] (新しい包含タグを追加) を選択し、除外するタグの **Key** と **Value** ペアを指定します。**Value** を指定するかどうかは任意です。

   すべての包含タグを追加したら、[保存] を選択します。

   キーの値が指定されていない場合、EC2 インスタンスに指定されたキーがタグ付けされ、タグに割り当てられた値に関係なく、EC2 インスタンスは Malware Protection for EC2 スキャンプロセスに含まれます。

API/CLI

- マルウェアスキャン設定を更新して、スキャンプロセスに EC2 インスタンスまたはコンテナワークロードを含めます。

  次のコマンド AWS CLI 例では、包含タグリストに新しいタグを追加します。必ず *detector-id* の例をお使いの有効な `detectorId` に置き換えてください。例 *TestKey*とを、EC2 リソースに関連付けられたタグの `Key`と `Value`ペア*TestValue*に置き換えます。

  `MapEquals` は `Key/Value` ペアの一覧です。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> タグのキーと値は大文字と小文字が区別されます。詳細については、Amazon EC2 ユーザーガイド」の「タグ制限」または「Amazon EC2 ユーザーガイド」の「タグ制限」を参照してください。 Amazon EC2

> **Note**
>
> が新しいタグを検出する GuardDuty までに最大 5 分かかる場合があります。

ユーザーはいつでも [Inclusion tags] (包含タグ) または [Exclusion tags] (除外タグ) のどちらかを選択できますが、両方を選択することはできません。タグを切り替える場合、新しいタグを追加する際にドロップダウンメニューからそのタグを選択し、選択したものを [確認] します。このアクションにより、現在のタグがすべてクリアされます。

グローバル `GuardDutyExcluded` タグ

デフォルトでは、EBS ボリュームのスナップショットは `GuardDutyScanId` タグ付きで作成されます。このタグを削除しないでください。削除すると、 がスナップショットにアクセスできなくなります GuardDuty。Malware Protection for EC2 のどちらのスキャンタイプも、`GuardDutyExcluded` タグが に設定されている Amazon EC2 インスタンスまたは Amazon EBS ボリュームをスキャンしません`true`。このようなリソースで Malware Protection for EC2 スキャンを実行すると、スキャン ID が生成されますが、そのスキャンは`EXCLUDED_BY_SCAN_SETTINGS`理由とともにスキップされます。詳細については、「マルウェアスキャン中にリソースをスキップする理由」を参照してください。

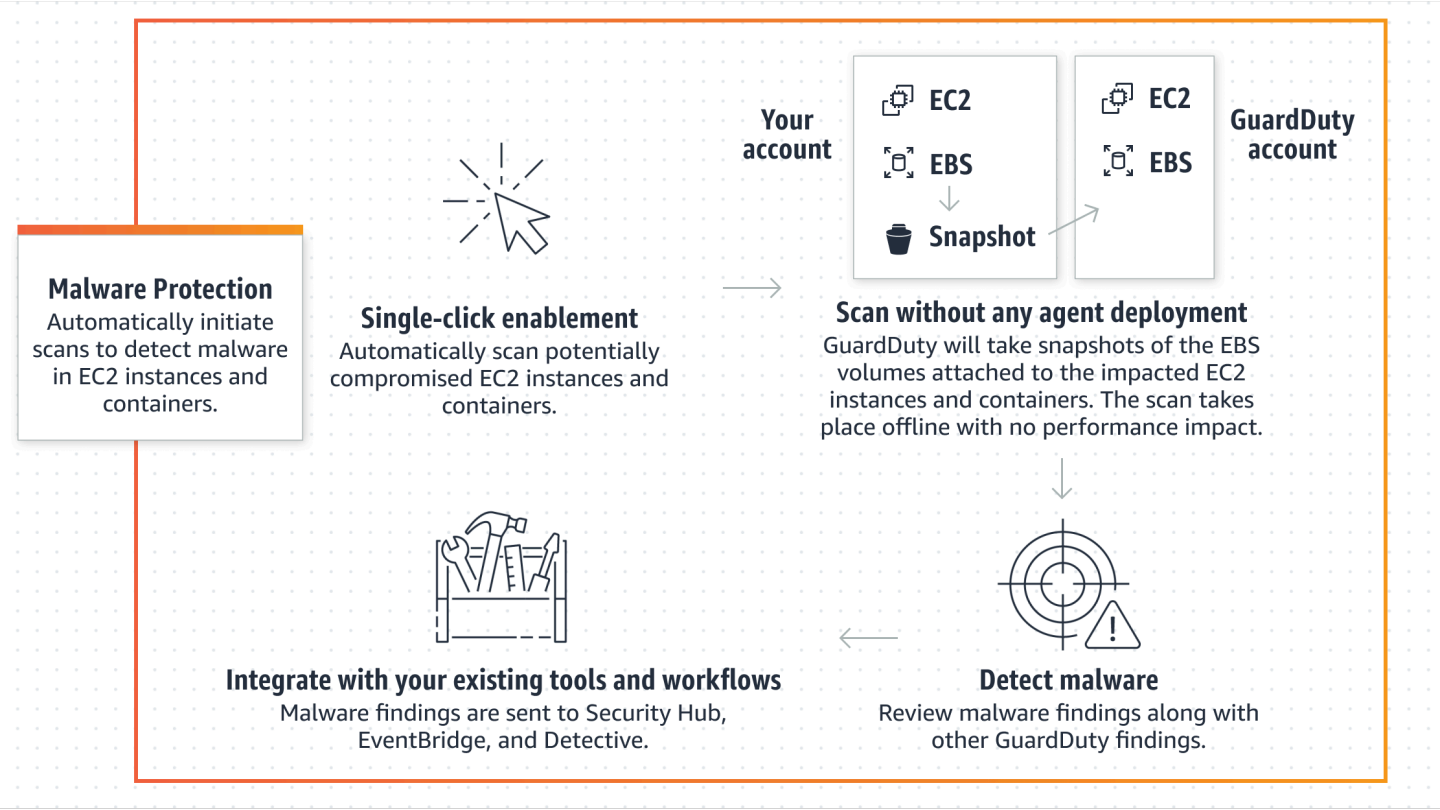
GuardDutyが開始するマルウェアスキャン

GuardDuty実行型マルウェアスキャンを有効にすると、 は Amazon EC2 インスタンスまたはコンテナワークロードにマルウェアが存在する可能性を示す悪意のあるアクティビティ GuardDuty を検出し、 GuardDuty を生成するたびに GuardDuty実行型マルウェアスキャンを呼び出す検出結果、影響を受ける可能性のある Amazon EC2 インスタンスまたはコンテナワークロードにアタッチされた Amazon Elastic Block Store (Amazon EBS) ボリュームでエージェントレススキャン GuardDuty を自動的に開始してマルウェアの存在を検出します。スキャンオプションを使用すると、スキャンするリソースに関連付けされた包含タグを追加したり、スキャンプロセスでスキップするリソースに関連付けされた除外タグを追加したりできます。自動スキャンの開始は、常にスキャンオプションに基づいて実行されます。また、Malware Protection for EC2 がマルウェアの存在を検出した場合にのみ、EBS ボリュームのスナップショットを保持するスナップショット保持設定をオンにすることもできます。詳細については、「Malware Protection for EC2 のカスタマイズ」を参照してください。

が検出結果 GuardDuty を生成する Amazon EC2 インスタンスとコンテナワークロードごとに、GuardDutyが開始するマルウェアの自動スキャンが 24 時間に 1 回呼び出されます。Amazon EC2 イ

ンスタンスまたはコンテナワークロードにアタッチされた Amazon EBS ボリュームのスキャン方法については、「Malware Protection for EC2 の機能」を参照してください。

次の画像は、 GuardDuty実行型マルウェアスキャンの仕組みを示しています。



マルウェアが見つかると、 は GuardDuty を生成しますEC2 検出結果タイプの Malware Protection。が同じリソースでマルウェアを示す検出結果を生成 GuardDuty しない場合、 GuardDuty実行型マルウェアスキャンは呼び出されません。同じリソースでオンデマンドのマルウェアスキャンを開始することもできます。詳細については、「オンデマンドのマルウェアスキャン」を参照してください。

30 日間の無料トライアル

でサポートされている AWS アカウント の GuardDuty実行型マルウェアスキャンを AWS リージョン いつでも有効または無効にすることができます。組織をお持ちの場合、各メンバーアカウントには独自の 30 日間の無料トライアルがあります。

30 日間の無料トライアルの仕組みを理解するには、次のシナリオを検討してください。

- GuardDuty を初めて (新しい GuardDuty アカウント) 有効にすると、 GuardDuty開始されたマルウェアスキャンも有効になり、 GuardDuty サービスに関連付けられた 30 日間の無料トライアルに含まれます。

- 既存の GuardDuty アカウントでは、30 日間の無料トライアルで、 GuardDuty実行型マルウェアスキャンを初めて有効にできます。別のリージョンでこの機能を初めて有効にすると、そのリージョンで 30 日間の無料トライアルが受けられます。
- オンデマンドのマルウェアスキャンが発表される前に Malware Protection for EC2 を使用している既存の GuardDuty アカウントがあり、この GuardDuty アカウントが既に の料金モデルを使用している場合は AWS リージョン、 GuardDuty実行型マルウェアスキャンを引き続き使用できます。

> **Note**
>
> 30 日間の無料トライアル期間中であっても、Amazon EBS ボリュームスナップショットの作成とその保持には標準使用コストが適用されます。詳細については、Amazon EBS の料金表を参照してください。

実行型マルウェアスキャンの有効化については、 GuardDuty「」を参照してください GuardDutyが開始するマルウェアスキャンの設定。

GuardDutyが開始するマルウェアスキャンの設定

スタンドアロンアカウントの GuardDuty実行型マルウェアスキャンの設定

に関連付けられているアカウントの場合 AWS Organizations、次のセクションで説明するように、コンソール設定を使用してこのプロセスを自動化できます。

GuardDuty実行型マルウェアスキャンを有効または無効にするには

任意のアクセス方法を選択して、スタンドアロンアカウントの GuardDuty実行型マルウェアスキャンを設定します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインの保護プラン で、EC2 の Malware Protection EC2を選択します。
3. Malware Protection for EC2 ペインには、アカウントの GuardDuty実行型マルウェアスキャンの現在のステータスが一覧表示されます。[有効にする] または [無効にする] をそれぞれ選択することで、いつでも有効または無効にすることができます。
4. [保存] を選択します。

API/CLI

- ユーザー独自のリージョンレベルのディテクター ID を使用し、`EbsVolumes` を `true` または `false` に設定した `dataSources` オブジェクトを渡して、updateDetector API オペレーションを実行します。

  次の AWS CLI コマンドを実行して、 AWS コマンドラインツールを使用して GuardDuty実行型マルウェアスキャンを有効または無効にすることもできます。必ずご自身の有効な *### ### ID* を使用してください。

  > **Note**
  >
  > 次のサンプルコードは、 GuardDuty実行型マルウェアスキャンを有効にします。無効にするには、`true` を `false` に置き換えます。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

マルチアカウント環境での GuardDuty実行型マルウェアスキャンの設定

マルチアカウント環境では、 GuardDuty 管理者アカウントアカウントのみが GuardDuty実行型マルウェアスキャンを設定できます。 GuardDuty 管理者アカウントは、メンバーアカウントに対して GuardDuty実行型マルウェアスキャンの使用を有効または無効にできます。管理者アカウントがメンバーアカウントの GuardDuty実行型マルウェアスキャンを設定すると、メンバーアカウントは管理者アカウントの設定に従い、コンソールからこれらの設定を変更できなくなります。 AWS Organizations サポート対象のメンバーアカウントを管理する GuardDuty 管理者アカウントは、組織内のすべての既存アカウントと新規アカウントで GuardDuty実行型マルウェアスキャンを自動的に有効にすることを選択できます。詳細については、「による GuardDuty アカウントの管理 AWS Organizations」を参照してください。

GuardDutyが開始するマルウェアスキャンを有効にするための信頼されたアクセスを確立する

GuardDuty 委任管理者アカウントが組織内の管理アカウントと同じでない場合、管理アカウントは組織に対して GuardDuty実行型マルウェアスキャンを有効にする必要があります。これにより、委任された管理者アカウントは、 を通じて管理されるMalware Protection for EC2 のサービスにリンクされたロールのアクセス許可メンバーアカウントに を作成できます AWS Organizations。

> **Note**
>
> 委任された GuardDuty 管理者アカウントを指定する前に、「」を参照してください考慮事項とレコメンデーション。

任意のアクセス方法を選択して、委任 GuardDuty 管理者アカウントが組織内のメンバーアカウントに対して GuardDuty実行型マルウェアスキャンを有効にできるようにします。

Console

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

   ログインするには、 AWS Organizations 組織の管理アカウントを使用します。

2. a. 委任 GuardDuty 管理者アカウントを指定していない場合は、次の操作を行います。

      設定ページの委任 GuardDuty 管理者アカウント に、組織内の GuardDuty ポリシーを管理するために**account ID**指定する 12 桁の を入力します。[委任] を選択します。

   b. i. 管理アカウントとは異なる委任 GuardDuty 管理者アカウントを既に指定している場合は、次の操作を行います。

         [Settings] (設定) ページの [Delegated Administrator] (委任された管理者) で、[Permissions] (許可) 設定をオンにします。このアクションにより、委任された GuardDuty 管理者アカウントは、関連するアクセス許可をメンバーアカウントにアタッチし、これらのメンバーアカウントで GuardDuty実行型マルウェアスキャンを有効にすることができます。

      ii. 管理アカウントと同じ委任 GuardDuty 管理者アカウントを既に指定している場合は、メンバーアカウントに対して GuardDuty実行型マルウェアスキャンを直接有効にできます。詳細については、「すべてのメンバーアカウントで GuardDuty実行型マルウェアスキャンを自動有効化する」を参照してください。

> **Tip**
>
> 委任された GuardDuty 管理者アカウントが管理アカウントと異なる場合は、委任された GuardDuty 管理者アカウントにアクセス許可を付与して、メンバーアカウントの GuardDuty実行型マルウェアスキャンを有効にする必要があります。

3. 委任された GuardDuty 管理者アカウントに、他のリージョンのメンバーアカウントに対して GuardDuty実行型マルウェアスキャンを有効にすることを許可する場合は、 を変更し AWS リージョン、上記の手順を繰り返します。

API/CLI

1. 管理アカウントの認証情報を使用して、次のコマンドを実行します。

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (オプション) 委任された管理者アカウントではない管理アカウントに対して GuardDuty 実行型マルウェアスキャンを有効にするには、管理アカウントはまずそのアカウントにMalware Protection for EC2 のサービスにリンクされたロールのアクセス許可明示的に を作成し、次に他のメンバーアカウントと同様に、委任された管理者アカウントから GuardDuty実行型マルウェアスキャンを有効にします。

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. 現在選択されている で委任 GuardDuty 管理者アカウントを指定しました AWS リージョン。あるリージョンでアカウントを委任された GuardDuty 管理者アカウントとして指定している場合、そのアカウントは他のすべてのリージョンで委任された GuardDuty 管理者アカウントである必要があります。上記のステップを他のすべてのリージョンについて繰り返します。

委任された GuardDuty 管理者アカウントの GuardDuty実行型マルウェアスキャンの設定

任意のアクセス方法を選択して、委任された GuardDuty 管理者アカウントの GuardDuty実行型マルウェアスキャンを有効または無効にします。

Console

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

   必ず管理アカウントの認証情報を使用してください。

2. ナビゲーションペインで、EC2 の Malware Protection を選択します。
3. Malware Protection for EC2 ページで、 実行型マルウェアスキャン の横にある編集を選択します。 GuardDuty
4. 次のいずれかを行います。

   [すべてのアカウントについて有効にする] の使用

   - [すべてのアカウントについて有効にする] を選択します。これにより、 AWS 組織に参加する新しい GuardDuty アカウントを含め、組織内のすべてのアクティブなアカウントに対して保護プランが有効になります。
   - [保存] を選択します。

   [アカウントを手動で設定] の使用

   - 委任された GuardDuty 管理者アカウントアカウントに対してのみ保護プランを有効にするには、アカウントを手動で設定を選択します。
   - 委任された GuardDuty 管理者アカウント (このアカウント) セクションで 有効化 を選択します。
   - [保存] を選択します。

API/CLI

ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト `name` を `EBS_MALWARE_PROTECTION` として、`status` を `ENABLED` または `DISABLED` として渡して、updateDetector API オペレーションを実行します。

次の AWS CLI コマンドを実行すると、 GuardDuty実行型マルウェアスキャンを有効または無効にできます。委任 GuardDuty 管理者アカウントの有効な`###### ID` を使用してください。

> **Note**
>
> 次のサンプルコードは、 GuardDuty実行型マルウェアスキャンを有効にします。無効にするには、ENABLED を DISABLED に置き換えます。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

すべてのメンバーアカウントで GuardDuty実行型マルウェアスキャンを自動有効化する

任意のアクセス方法を選択して、すべてのメンバーアカウントに対して GuardDuty実行型マルウェアスキャン機能を有効にします。これには、既存のメンバーアカウントと、組織に参加する新しいアカウントが含まれます。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。
2. 次のいずれかを行います。

   Malware Protection for EC2 ページの使用

   1. ナビゲーションペインで、EC2 の Malware Protection を選択します。
   2. Malware Protection for EC2 ページで、 GuardDuty実行型マルウェアスキャンセクションで編集を選択します。
   3. [すべてのアカウントについて有効にする] を選択します。このアクションにより、組織内の既存アカウントと新規アカウントの両方に対して GuardDuty実行型マルウェアスキャンが自動的に有効になります。
   4. [保存] を選択します。

> **Note**
>
> メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

[アカウント] ページの使用

1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
2. [アカウント] ページで、[招待によるアカウントの追加] の前に [自動有効化] の詳細設定を選択します。
3. 自動有効化設定の管理ウィンドウで、 GuardDutyが開始したマルウェアスキャン のすべてのアカウントに対して有効化を選択します。
4. Malware Protection for EC2 ページで、 GuardDuty実行型マルウェアスキャンセクションで編集を選択します。
5. [すべてのアカウントについて有効にする] を選択します。このアクションにより、組織内の既存アカウントと新規アカウントの両方に対して GuardDuty実行型マルウェアスキャンが自動的に有効になります。
6. [保存] を選択します。

> **Note**
>
> メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

[アカウント] ページの使用

1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
2. [アカウント] ページで、[招待によるアカウントの追加] の前に [自動有効化] の詳細設定を選択します。
3. 自動有効化設定の管理ウィンドウで、 GuardDutyが開始したマルウェアスキャン のすべてのアカウントに対して有効化を選択します。
4. [保存] を選択します。

[すべてのアカウントについて有効にする] オプションを使用できない場合は、「メンバーアカウントの GuardDuty実行型マルウェアスキャンを選択的に有効または無効にする」を参照してください。

API/CLI

- メンバーアカウントの GuardDuty実行型マルウェアスキャンを選択的に有効または無効にするには、独自のディテクター ID を使用して updateMemberDetectors API オペレーションを呼び出します。
- 次の例は、単一のメンバーアカウントに対して GuardDuty実行型マルウェアスキャンを有効にする方法を示しています。メンバーアカウントを無効にするには、DISABLED を ENABLED に置き換えてください。

  アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

  スペースで区切られたアカウント ID のリストを渡すこともできます。
- コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

既存のすべてのアクティブなメンバーアカウントに対して GuardDuty実行型マルウェアスキャンを有効にする

任意のアクセス方法を選択して、組織内のすべての既存のアクティブなメンバーアカウントに対して GuardDuty実行型マルウェアスキャンを有効にします。

既存のアクティブなメンバーアカウントすべてに対して GuardDuty実行型マルウェアスキャンを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任 GuardDuty 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、EC2 の Malware Protection を選択します。
3. Malware Protection for EC2 では、 GuardDuty実行型マルウェアスキャン設定の現在のステータスを表示できます。[アクティブなメンバーアカウント] セクションで、[アクション] を選択します。
4. [アクション] ドロップダウンメニューから、[すべての既存のアクティブなメンバーアカウントについて有効にする] を選択します。
5. [保存] を選択します。

新しいメンバーアカウントの GuardDuty実行型マルウェアスキャンを自動で有効にする

新しく追加されたメンバーアカウントは、 GuardDuty実行型マルウェアスキャンの設定を選択する前に を有効にする GuardDuty 必要があります。招待によって管理されるメンバーアカウントは、アカウントに対して GuardDuty実行型マルウェアスキャンを手動で設定できます。詳細については、「Step 3 - Accept an invitation」を参照してください。

任意のアクセス方法を選択して、組織に参加する新しいアカウントの GuardDuty実行型マルウェアスキャンを有効にします。

Console

委任された GuardDuty 管理者アカウントは、EC2 の Malware Protection GuardDutyページまたは アカウントページを使用して、組織内の新しいメンバーアカウントの 実行型マルウェアスキャンを有効にできます。 EC2

新しいメンバーアカウントの GuardDuty実行型マルウェアスキャンを自動で有効にするには

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。
2. 次のいずれかを行います。
   - Malware Protection for EC2 ページの使用：

1. ナビゲーションペインで、EC2 の Malware Protection を選択します。
2. EC2 の Malware Protection ページで、 GuardDuty実行型マルウェアスキャン で 編集 を選択します。
3. [アカウントを手動で設定] を選択します。
4. [新しいメンバーアカウントについて自動的に有効にする] を選択します。このステップにより、新しいアカウントが組織に加わるたびに、 GuardDutyそのアカウントに対して開始されたマルウェアスキャンが自動的に有効になります。この設定を変更できるのは、組織の委任 GuardDuty 管理者アカウントのみです。
5. [保存] を選択します。

- [Accounts] (アカウント) ページを使用する場合:

1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
2. [アカウント] ページで、[自動有効化] 設定を選択します。
3. 自動有効化設定の管理ウィンドウで、 実行型マルウェアスキャン で新しいアカウントの有効化を選択します。 GuardDuty
4. [保存] を選択します。

API/CLI

- 新しいメンバーアカウントの GuardDuty実行型マルウェアスキャンを有効または無効にするには、独自のディテクター ID を使用して UpdateOrganizationConfiguration API オペレーションを呼び出します。
- 次の例は、単一のメンバーアカウントに対して GuardDuty実行型マルウェアスキャンを有効にする方法を示しています。無効にするには、「メンバーアカウントの GuardDuty実行型マルウェアスキャンを選択的に有効または無効にする」を参照してください。組織に参加する新規アカウントすべてに対して有効にしたくない場合は、`AutoEnable` を `NONE` に設定します。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
 "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

メンバーアカウントの GuardDuty実行型マルウェアスキャンを選択的に有効または無効にする

任意のアクセス方法を選択して、メンバーアカウントの GuardDuty実行型マルウェアスキャンを選択的に設定します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
3. アカウントページで、 GuardDutyが開始するマルウェアスキャン列でメンバーアカウントのステータスを確認します。
4. GuardDuty実行型マルウェアスキャンを設定するアカウントを選択します。一度に複数のアカウントを選択できます。
5. 保護プランの編集メニューから、 GuardDuty実行型マルウェアスキャン に適したオプションを選択します。

API/CLI

メンバーアカウントの GuardDuty実行型マルウェアスキャンを選択的に有効または無効にするには、独自のディテクター ID を使用して updateMemberDetectors API オペレーションを呼び出します。

次の例は、単一のメンバーアカウントに対して GuardDuty実行型マルウェアスキャンを有効にする方法を示しています。無効にするには、ENABLED を DISABLED に置き換えます。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

メンバーアカウントの GuardDuty実行型マルウェアスキャンを選択的に有効または無効にするには、独自のディテクター ID を使用して updateMemberDetectors API オペレーションを実行します。 次の例は、単一のメンバーアカウントに対して GuardDuty実行型マルウェアスキャンを有効にする方法を示しています。無効にするには、`true` を `false` に置き換えます。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

招待によって管理される Organization GuardDuty内の既存のアカウントに対して 実行型マルウェアスキャンを有効にする

GuardDuty Malware Protection for EC2 サービスにリンクされたロール (SLR) は、メンバーアカウントで作成する必要があります。管理者アカウントは、 によって管理されていないメンバーアカウントで GuardDuty実行型マルウェアスキャン機能を有効にすることはできません AWS Organizations。

現在、https://console.aws.amazon.com/guardduty/ の GuardDuty コンソールから次の手順を実行して、既存のメンバーアカウントの GuardDuty実行型マルウェアスキャンを有効にできます。

Console

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

   管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
3. GuardDuty実行型マルウェアスキャンを有効にするメンバーアカウントを選択します。一度に複数のアカウントを選択できます。
4. [アクション] を選択します。
5. [Disassociate member] (メンバーの関連付けを解除する) を選択します。
6. メンバーアカウントのナビゲーションペインで、[保護プラン] から [Malware Protection] を選択します。
7. GuardDuty開始されたマルウェアスキャンを有効にする を選択します。 GuardDuty はメンバーアカウントの SLR を作成します。SLR の詳細については、「Malware Protection for EC2 のサービスにリンクされたロールのアクセス許可」を参照してください。
8. 管理者アカウントで、ナビゲーションペインのアカウントを選択します。
9. 組織に追加し直す必要があるメンバーアカウントを選択します。
10. [Actions] (アクション)、[Add member] (メンバーの追加) の順に選択します。

API/CLI

1. 管理者アカウントアカウントを使用して、 GuardDuty実行型マルウェアスキャンを有効にするメンバーアカウントで DisassociateMembers API を実行します。
2. メンバーアカウントを使用して を呼び出しUpdateDetector、 GuardDuty実行型マルウェアスキャンを有効にします。

   アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. 管理者アカウントを使用して CreateMembers API を実行し、メンバーを組織に戻します。

GuardDuty実行型マルウェアスキャンを呼び出す検出結果

GuardDutyが開始したマルウェアスキャンは、 が Amazon EC2 インスタンスまたはコンテナワークロードでマルウェアを示す疑わしい動作 GuardDuty を検出すると呼び出されます。

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (アウトバウンドのみ)
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS

- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce (アウトバウンドのみ)
- UnauthorizedAccess:EC2/SSHBruteForce (アウトバウンドのみ)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint!DNS

- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

オンデマンドのマルウェアスキャン

オンデマンドのマルウェアスキャンは、Amazon EC2 インスタンスにアタッチされた Amazon Elastic Block Store (Amazon EBS) ボリュームでマルウェアの存在を検出するのに役立ちます。設定は不要で、スキャンする Amazon EC2 インスタンスの Amazon リソースネーム (ARN) を指定することで、オンデマンドのマルウェアスキャンを開始できます。オンデマンドのマルウェアスキャンは、 GuardDuty コンソールまたは API を使用して開始できます。オンデマンドのマルウェアスキャンを開始する前に、希望する スナップショットの保持 設定をセットできます。以下のシナリオは、 でオンデマンドのマルウェアスキャンタイプを使用するタイミングを特定するのに役立ちます GuardDuty。

- GuardDuty実行型マルウェアスキャンを有効にせずに、Amazon EC2 インスタンスにマルウェアが存在することを検出したい。
- GuardDuty実行型マルウェアスキャンを有効にし、スキャンが自動的に呼び出されました。生成された Malware Protection for EC2 の検出結果タイプに対して推奨される修復後、同じリソースでスキャンを開始する場合は、前回のスキャン開始時刻から 1 時間が経過した後にオンデマンドのマルウェアスキャンを開始できます。

  オンデマンドのマルウェアスキャンは、前回のマルウェアスキャンが開始された時刻から 24 時間経過する必要はありません。同じリソースでオンデマンドのマルウェアスキャンを開始する前に 1 時間経過している必要があります。同じ EC2 インスタンスでマルウェアスキャンの重複を避けるには、「同じ Amazon EC2 インスタンスの再スキャン」を参照してください。

> **Note**
>
> オンデマンドのマルウェアスキャンは、 の 30 日間の無料トライアル期間には含まれません GuardDuty。使用コストは、マルウェアスキャンごとにスキャンされた Amazon EBS ボリュームの合計に適用されます。詳細については、「Amazon GuardDuty の料金」を参照してください。Amazon EBS ボリュームのスナップショットおよびその保持にかかるコストについては、「Amazon EBS 料金設定」を参照してください。

オンデマンドのマルウェアスキャンの仕組み

オンデマンドのマルウェアスキャンでは、Amazon EC2 インスタンスが現在使用中であっても、そのインスタンスに対するマルウェアスキャンリクエストを開始できます。オンデマンドのマルウェアスキャンを開始すると、 はスキャン用に Amazon リソースネーム (ARN) が指定された Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームのスナップショット GuardDuty を作成します。次に、 GuardDuty はこれらのスナップショットを と共有しますGuardDuty サービスアカウント。 GuardDuty は、 GuardDuty サービスアカウントのスナップショットから暗号化されたレプリカ EBS ボリュームを作成します。Amazon EBS ボリュームがスキャンされる方法の詳細については、「Elastic Block Storage (EBS) ボリューム」を参照してください。

> **Note**
>
> GuardDuty は、オンデマンドのマルウェアスキャンを開始する point-in-time ときに、 で Amazon EBS ボリュームに既に書き込まれているデータのスナップショットを作成します。

マルウェアが見つかってスナップショットの保持設定を有効にしている場合、EBS ボリュームのスナップショットは自動的に AWS アカウントで保持されます。オンデマンドのマルウェアスキャンは EC2 検出結果タイプの Malware Protection を生成します。マルウェアが見つからなければ、スナップショットの保持設定とは関係なく、EBS ボリュームのスナップショットは削除されます。

デフォルトでは、EBS ボリュームのスナップショットは `GuardDutyScanId` タグ付きで作成されます。このタグを削除しないでください。削除すると、 がスナップショットにアクセスできなくなります GuardDuty。Malware Protection for EC2 のどちらのスキャンタイプも、`GuardDutyExcluded`タグが `true` に設定されている Amazon EC2 インスタンスまたは Amazon EBS ボリュームをスキャンしません。このようなリソースで Malware Protection for EC2 スキャンを実行すると、スキャン ID が生成されますが、そのスキャンは`EXCLUDED_BY_SCAN_SETTINGS`理由とともにスキップされます。詳細については、「マルウェアスキャン中にリソースをスキップする理由」を参照してください。

AWS Organizations サービスコントロールポリシー — アクセス拒否

でサービスコントロールポリシー (SCPs)を使用すると AWS Organizations、委任された GuardDuty 管理者アカウントはアクセス許可を制限し、アカウントが所有する Amazon EC2 インスタンスのオンデマンドマルウェアスキャンを開始するなどのアクションを拒否できます。

GuardDuty メンバーアカウントとして、Amazon EC2 インスタンスのオンデマンドのマルウェアスキャンを開始すると、エラーが表示されることがあります。管理アカウントに接続して、メンバーア

カウントに SCP がセットアップされた理由について説明します。詳細については、「許可に対する SCP の影響」を参照してください。

オンデマンドのマルウェアスキャンの開始方法

GuardDuty 管理者アカウントとして、アカウントで以下の前提条件が設定されているアクティブなメンバーアカウントに代わって、オンデマンドのマルウェアスキャンを開始できます。のスタンドアロンアカウントとアクティブなメンバーアカウント GuardDuty は、独自の Amazon EC2 インスタンスのオンデマンドのマルウェアスキャンを開始することもできます。

前提条件

- GuardDuty は、オンデマンドのマルウェアスキャン AWS リージョン を開始する で有効にする必要があります。
- AWS マネージドポリシー: AmazonGuardDutyFullAccess が IAM ユーザーまたは IAM ロールにアタッチされていることを確認します。IAM ユーザーまたは IAM ロールに関連付けされたアクセスキーおよびシークレットキーが必要になります。
- 委任された GuardDuty 管理者アカウントとして、アクティブなメンバーアカウントに代わってオンデマンドのマルウェアスキャンを開始するオプションがあります。
- を持っていないメンバーアカウントの場合Malware Protection for EC2 のサービスにリンクされたロールのアクセス許可、アカウントに属する Amazon EC2 インスタンスのオンデマンドのマルウェアスキャンを開始すると、 は EC2 の Malware Protection の SLR を自動的に作成します。

> **Important**
>
> Malware Protection for EC2 の SLR アクセス許可は、 GuardDuty開始かオンデマンドかにかかわらず、マルウェアスキャンがまだ進行中であるときに、誰も削除しないようにします。これを行うと、スキャンが正常に完了せず、明確なスキャン結果が得られません。

オンデマンドのマルウェアスキャンを開始する前、過去 1 時間以内に同じリソースにスキャンが開始されていないことを確認してください。そうしないと、重複除外されます。詳細については、「同じリソースの再スキャン」を参照してください。

オンデマンドのマルウェアスキャンの開始

任意のアクセス方法を選択して、オンデマンドのマルウェアスキャンを開始します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. 次のオプションのいずれかを使用してスキャンを開始します。

   a. Malware Protection for EC2 ページの使用：

      i. ナビゲーションペインの保護プラン で、EC2 の Malware Protection EC2を選択します。

      ii. Malware Protection for EC2 ページで、スキャンを開始する Amazon EC2 インスタンス ARN [1] を指定します。

   b. [マルウェアスキャン] ページの使用:

      i. ナビゲーションペインで、[マルウェアスキャン] を選択します。

      ii. [オンデマンドスキャンの開始] を選択し、スキャンを開始する [Amazon EC2 インスタンス ARN][1] を指定します。

      iii. 再スキャンの場合、[マルウェアスキャン] ページで [Amazon EC2] インスタンス ID を選択します。

      [オンデマンドスキャンの開始] ドロップダウンを展開し、[選択したインスタンスを再スキャン] を選択します。

3. いずれかの方法でスキャンを正常に開始すると、スキャン ID が生成されます。このスキャン ID を使用して、スキャンの進行状況を追跡できます。詳細については、「スキャンステータスと結果の監視」を参照してください。

API/CLI

オンデマンドのマルウェアスキャンを開始する Amazon EC2 インスタンス [1] `resourceArn`の StartMalwareScanを受け入れる を呼び出します。

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

スキャンを正常に開始すると、`StartMalwareScan` は `scanId` を返します。Invoke は、開始されたスキャンの進行状況をDescribeMalwareScansモニタリングします。

[1]Amazon EC2 インスタンス ARN の形式については、「Amazon リソースネーム (ARN)」を参照してください。Amazon EC2 インスタンスの場合、パーティション、リージョン、 AWS アカウント ID、Amazon EC2 インスタンス ID の値を置き換えることで、次の ARN 形式の例を使用できます。インスタンス ID の長さについては、「リソース ID」を参照してください。

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

同じ Amazon EC2 インスタンスの再スキャン

スキャンが GuardDuty開始かオンデマンドかにかかわらず、前回のマルウェアスキャンの開始時刻から 1 時間後に、同じ EC2 インスタンスで新しいオンデマンドマルウェアスキャンを開始できます。前回のマルウェアスキャンの開始から 1 時間以内に新しいマルウェアスキャンが開始された場合、リクエストの結果として次のエラーが発生し、このリクエストのスキャン ID は生成されません。

```
A scan was initiated on this resource recently. You can request a scan on
the same resource one hour after the previous scan start time.
```

同じリソースに新しいスキャンを開始する方法については、「オンデマンドのマルウェアスキャンの開始」を参照してください。

マルウェアスキャンのステータスを追跡するには、「スキャンステータスと結果のモニタリングにより、 GuardDuty Malware Protection for EC2 が実行されます。」を参照してください。

スキャンステータスと結果のモニタリングにより、 GuardDuty Malware Protection for EC2 が実行されます。

各 GuardDuty Malware Protection for EC2 スキャンのスキャンステータスをモニタリングできます。想定されるスキャンの [Status] (ステータス) の値は、`Completed`、`Running`、`Skipped`、および `Failed` です。

スキャンが完了すると、[Status] (ステータス) が `Completed` のスキャンに [Scan result] (スキャン結果) が入力されます。[Scan result] (スキャン結果) で可能な値は、`Clean` と `Infected` です。[スキャンタイプ] を使用すると、マルウェアスキャンが `GuardDuty initiated` なのか `On demand` なのか特定できます。

マルウェアスキャンの各検索結果の保持期間は 90 日です。任意のアクセス方法を選択して、マルウェアスキャンのステータスを追跡します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで [Malware scans] (マルウェアウェアのスキャン) を選択します。
3. [filter criteria] (フィルター条件) で利用可能な次の [Properties] (プロパティ) によってマルウェアスキャンをフィルターできます。

   - [Scan ID] (スキャン ID)
   - アカウント ID
   - [EC2 instance ARN] (EC2 インスタンス ARN)
   - [スキャンタイプ]
   - [Scan status] (スキャンステータス)

   フィルター条件に使用されるプロパティについては、「検出結果の詳細」を参照してください。

API/CLI

- マルウェアスキャンの結果が表示されると、`EC2_INSTANCE_ARN`、`SCAN_ID`、`ACCOUNT_ID`、`SCAN_TYPE`、`GUARDDUTY_FINDING_ID`、`SC` に基づいてマルウェアスキャンをフィルタリングできます。

  `GUARDDUTY_FINDING_ID` フィルター条件`SCAN_TYPE`は、 GuardDuty の開始時に使用できます。フィルター条件については、「検出結果の詳細」を参照してください。
- *`filter-criteria`* の例は、次のコマンドで変更できます。現在、1 つの `CriterionKey` を基準にフィルタリングできます。`CriterionKey` のオプションは、`EC2_INSTANCE_ARN`、`SCAN_ID`、`ACCOUNT_ID`、`SCAN_TYPE`、`GUARDDUTY_FINDING_ID`、`SC` です。

  以下のように同じ `CriterionKey` を使うなら、必ず `EqualsValue` の例を、ご自身の有効な AWS *`scan-id`* に置き換えてください。

  `detector-id` の値の例を有効な *`detector-id`* に置き換えます。*`max-results`* (最大 50) と *`sort-criteria`* を変更できます。`AttributeName` は必須であり、`scanStartTime` である必要があります。

```
aws guardduty describe-malware-scans --detector-
id 60b87779336485625554d637e0e4bb3b2 --max-results 1 --sort-criteria
 '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
{"EqualsValue":"123456789012"}}] }'
```

- このコマンドの応答には、最大 1 つの結果が表示され、(Infected の場合は) 影響を受けるリソースとマルウェアの検出結果に関する詳細が含まれます。

GuardDuty による サービスアカウント AWS リージョン

スナップショットが作成され、 GuardDuty サービスアカウントと共有されると、新しいイベントが CloudTrail ログに作成されます。このイベントは、対応する snapshotIdと userId (その GuardDuty のサービスアカウント) を指定します AWS リージョン。詳細については、「Malware Protection for EC2 の機能」を参照してください。

次の例は、リクエストのリクエストボディを示す CloudTrail イベントからのスニペットですModifySnapshotAttribute。

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

次の表は、各リージョン GuardDuty のサービスアカウントを示しています。userId は GuardDuty サービスアカウントであり、選択したリージョンによって異なります。

AWS リージョン	リージョンコード	GuardDuty サービスアカウント ID (**`userId`**)
米国東部 (バージニア北部)	us-east-1	652050842985
米国東部 (オハイオ)	us-east-2	178123968615
米国西部 (北カリフォルニア)	us-west-1	669213148797
米国西部 (オレゴン)	us-west-2	447226417196
アジアパシフィック (ムンバイ)	ap-south-1	913179291432
アジアパシフィック (大阪)	ap-northeast-3	089661699081
アジアパシフィック (ソウル)	ap-northeast-2	039163547507
アジアパシフィック (東京)	ap-northeast-1	874749492622
アジアパシフィック (シンガポール)	ap-southeast-1	247460962669
アジアパシフィック (シドニー)	ap-southeast-2	124839743349
カナダ (中部)	ca-central-1	175877067165
カナダ西部 (カルガリー)	ca-west-1	894794104037
欧州 (フランクフルト)	eu-central-1	002294850712
欧州 (アイルランド)	eu-west-1	283769539786
欧州 (ロンドン)	eu-west-2	310125036783

AWS リージョン	リージョンコード	GuardDuty サービスアカウント ID (**`userId`**)
欧州 (パリ)	eu-west-3	866607715269
欧州 (ストックホルム)	eu-north-1	693780578038
中国 (北京)	cn-north-1	448721096076
中国 (寧夏)	cn-northwest-1	480864352451
南米 (サンパウロ)	sa-east-1	546914126324
アジアパシフィック (ハイデラバード) (オプトイン)	ap-south-2	682251015962
アジアパシフィック (メルボルン) (オプトイン)	ap-southeast-4	353488359550
欧州 (スペイン) (オプトイン)	eu-south-2	936182149045
欧州 (チューリッヒ) (オプトイン)	eu-central-2	867642063380
イスラエル (テルアビブ) (オプトイン)	il-central-1	619233833001
欧州 (ミラノ) (オプトイン)	eu-south-1	977238331021
アジアパシフィック (香港) (オプトイン)	ap-east-1	249472122084
中東 (バーレーン) (オプトイン)	me-south-1	404001805210
アフリカ (ケープタウン) (オプトイン)	af-south-1	957664736811

AWS リージョン	リージョンコード	GuardDuty サービスアカウント ID (**`userId`**)
アジアパシフィック (ジャカルタ) (オプトイン)	ap-southeast-3	452118225523
中東 (アラブ首長国連邦) (オプトイン)	me-central-1	828603743433

EC2 クォータの Malware Protection

EC2 の Malware Protection には、この機能が使用するさまざまなリソースの以下のデフォルト可用性があります。

範囲	デフォルト値	コメント
圧縮ファイルまたはアーカイブファイル内のデータの抽出と分析	5	アーカイブファイルで許可されるネストレベルの最大数。
アーカイブされたファイル内のファイルの数	1,000	アーカイブ内でスキャンできるファイルの最大数。この数は、アーカイブから抽出されたファイルの数と、ネストされたすべてのアーカイブから抽出されたファイルの数の合計です。
脅威の数	32	検出結果パネルで表示できる脅威の最大数。EC2 の GuardDuty マルウェア保護では、より多くの脅威名が検出されている可能性があります。検出された脅威名の数がデフォルト値より大きい場合は、 GuardDuty コンソールの

範囲	デフォルト値	コメント
		詳細パネルの検出結果名で検出結果 ID を選択すると、JSON の詳細を表示できます。
検出された脅威ごとのファイル数	5	検出された脅威ごとに識別されるファイルの最大数。例えば、 が 1 つの脅威に関連付けられた 10 個のファイル GuardDuty を検出すると、脅威には最大 5 個のファイルが表示されます。
スキャン毎、インスタンス毎の EBS ボリューム	11	EC2 インスタンスごとにスキャン GuardDuty できる EBS ボリュームの最大数。スキャンする必要がある EBS ボリュームが 11 個を超える場合、EC2 の GuardDuty マルウェア保護は`deviceName` アルファベット順にソートし、最初の 11 個の EBS ボリュームを選択します。
EBS ボリュームサイズ	2048 GB	Amazon EC2 インスタンスおよびコンテナワークロードに関連付けられている GuardDuty EC2 のマルウェア保護は、最大 2048 GB のサイズの各 Amazon EBS ボリュームをスキャンできます。このクォータは、Malware Protection for EC2 のサポート AWS リージョン が利用可能な各 に適用されます。

範囲	デフォルト値	コメント
サポートされているファイルの種類	GuardDuty Malware Protection for EC2 では、次のファイルシステムタイプをスキャンできます。 • 新技術ファイルシステム (NTFS) • X ファイルシステム (XFS) • ext2 ファイルシステム • ext4 ファイルシステム • File Allocation Table (FAT) ファイルシステム • Virtual File Allocation Table (VFAT) ファイルシステム	該当なし
スキャンオプションタグ	50	マルウェアスキャンオプションの設定をカスタマイズするために追加できるリソースタグの最大数。詳細については、「ユーザー定義タグ付きのスキャンオプション」を参照してください。
保持期間の検索	90	が結果 GuardDuty を保持する最大日数。最新情報については、「Amazon GuardDuty クォータ」を参照してください。

範囲	デフォルト値	コメント
マルウェアウェアスキャンの保持期間	90	GuardDuty Malware Protection for EC2 がスキャンの履歴を保持する最大日数。最新のマルウェアスキャンを表示する方法については、「スキャンステータスと結果のモニタリングにより、 GuardDuty Malware Protection for EC2 が実行されます。」を参照してください。
オンデマンドのマルウェアスキャンの 1 秒当たりのトランザクション数 (TPS)	1	各リージョンで 1 秒ごとに開始可能なオンデマンドのマルウェアスキャンリクエスト数。
オンデマンドのマルウェアスキャンのバースト制限	1	各リージョンで 1 秒ごとに同時に開始可能なオンデマンドのマルウェアスキャンリクエスト数。

GuardDuty S3 のマルウェア保護

Malware Protection for S3 は、選択した Amazon Simple Storage Service (Amazon S3) バケットに新しくアップロードされたオブジェクトをスキャンして、マルウェアの潜在的な存在を検出するのに役立ちます。S3 オブジェクトまたは既存の S3 オブジェクトの新しいバージョンが選択したバケットにアップロードされると、 はマルウェアスキャン GuardDuty を自動的に開始します。

S3 の Malware Protection - 概要とデモ

Malware Protection for S3 を有効にする 2 つのアプローチ

がサービスを有効にし、全体的な GuardDuty エクスペリエンスの一部として S3 の Malware Protection を使用する場合、または AWS アカウント GuardDuty サービスを有効にせずに S3 の Malware Protection 機能を単独で使用する場合、S3 の Malware Protection を有効にできます GuardDuty 。S3 の Malware Protection を単独で有効にすると、 GuardDuty ドキュメントでは、S3 の Malware Protection を独立した機能として使用していると参照されます。

Malware Protection for S3 を個別に使用する際の考慮事項

- GuardDuty セキュリティ検出結果 – ディテクター ID は、リージョン内のアカウントに関連付けられている一意の識別子です。アカウントの 1 つ以上のリージョン GuardDuty で を有効にすると、 を有効にするリージョンごとに、このアカウントに対してディテクター ID が自動的に作成されます GuardDuty。詳細については、 概念と用語ドキュメントの「ディテクター」を参照してください。

  アカウントで S3 の Malware Protection を個別に有効にすると、そのアカウントには関連するディテクター ID がありません。これは、利用できる GuardDuty 機能に影響します。例えば、S3 マルウェアスキャンでマルウェアの存在が検出された場合、すべての GuardDuty GuardDuty検出結果がディテクター ID に関連付けられている AWS アカウント ため、 では検出結果は生成されません。
- スキャンされたオブジェクトが悪意のあるものであるかどうかを確認する – デフォルトでは、 はマルウェアスキャン結果をデフォルトの Amazon EventBridge イベントバスと Amazon CloudWatch 名前空間に GuardDuty 発行します。バケットの Malware Protection for S3 を有効にしたときにタグ付けを有効にすると、スキャンされた S3 オブジェクトはスキャン結果を示すタグを取得します。タグ付けの詳細については、「スキャン結果に基づくオブジェクトのオプションのタグ付け」を参照してください。

Malware Protection for S3 を有効にするための一般的な考慮事項

Malware Protection for S3 を個別に使用する場合も、 GuardDuty エクスペリエンスの一部として使用する場合も、次の一般的な考慮事項が適用されます。

- Malware Protection for S3 は、自分のアカウントに属する Amazon S3 バケットに対して有効にできます。委任 GuardDuty 管理者アカウントとして、メンバーアカウントに属する Amazon S3 バケットでこの機能を有効にすることはできません。
- 委任された GuardDuty 管理者アカウントは、メンバーアカウントが Amazon S3 バケットに対してこの機能を有効にするたびに Amazon EventBridge 通知を受け取ります。
- 現在、S3 検出結果タイプの Malware Protection は、 AWS Security Hub および Amazon Detective との統合をサポートしていません。これは、S3 の検出結果タイプに対する Malware Protection にのみ適用されます。

内容

Malware Protection for S3 の仕組み

このセクションでは、Malware Protection for S3 の仕組みを理解するのに役立つコンポーネントについて説明します。

概要

独自の に属する Amazon S3 バケットに対して Malware Protection for S3 を有効にできます AWS アカウント。 GuardDuty では、この機能をバケット全体で有効にしたり、マルウェアスキャンの範囲を、選択したプレフィックスのいずれかで始まるアップロードされた各オブジェクトを が GuardDuty スキャンする特定のオブジェクトプレフィックスに制限したりできます。 Amazon S3 最大 5 つのプレフィックスを追加できます。S3 バケットに対してこの機能を有効にすると、そのバケットは保護されたバケット と呼ばれます。

IAM アクセス PassRole 許可

Malware Protection for S3 は、 PassRole がユーザーに代わってマルウェアスキャンアクションを実行 GuardDuty することを許可する IAM を使用します。これらのアクションには、選択したバケットに新しくアップロードされたオブジェクトの通知、それらのオブジェクトのスキャン、およびオプションでスキャンされたオブジェクトへのタグの追加が含まれます。これは、この機能を使用して S3 バケットを設定する前提条件です。

既存の IAM ロールを更新するか、この目的のために新しいロールを作成するかを選択できます。複数のバケットに対して Malware Protection for S3 を有効にすると、必要に応じて既存の IAM ロールを更新して、他のバケット名を含めることができます。詳細については、「前提条件 - IAM PassRole ポリシーを作成または更新する」を参照してください。

スキャン結果に基づくオブジェクトのオプションのタグ付け

バケットで Malware Protection for S3 を有効にするときに、スキャンされた S3 オブジェクトのタグ付けを有効にするオプションステップがあります。IAM には、スキャン後にオブジェクトにタグを追加するアクセス許可が PassRole 既に含まれています。ただし、 GuardDuty は、セットアップ時にこのオプションを有効にした場合にのみタグを追加します。

オブジェクトをアップロードする前に、このオプションを有効にする必要があります。スキャンが終了すると、 は、次のキーと値のペアを使用して、スキャンされた S3 オブジェクトに事前定義されたタグ GuardDuty を追加します。

`GuardDutyMalwareScanStatus:`*`Potential scan result`*

潜在的なスキャン結果タグ値には`NO_THREATS_FOUND`、、`THREATS_FOUND`、`UNSUPPORTED`、`ACCESS_DENIED`、および が含まれます`FAILED`。これらの値の詳細については、S3 object potential scan result value を参照してください。

タグ付けを有効にすることは、S3 オブジェクトのスキャン結果を知る方法の 1 つです。これらのタグをさらに使用して、タグベースのアクセスコントロール (TBAC) S3 リソースポリシーを追加して、潜在的に悪意のあるオブジェクトに対してアクションを実行できます。詳細については、「S3 バケットリソースへの TBAC の追加」を参照してください。

バケットの Malware Protection for S3 を設定するときに、タグ付けを有効にすることをお勧めします。オブジェクトがアップロードされ、スキャンが開始された後にタグ付けを有効にすると、 はスキャンされたオブジェクトにタグを追加 GuardDuty できなくなります。関連する S3 オブジェクトのタグ付けコストについては、「」を参照してくださいMalware Protection for S3 の料金。

バケットの S3 の Malware Protection を有効にした後

Malware Protection for S3 を有効にすると、Malware Protection プランリソースは選択した S3 バケットに対してのみ作成されます。このリソースは、保護されたリソースの一意の識別子である Malware Protection プラン ID に関連付けられます。IAM アクセス許可のいずれかを使用することで、 は の名前で EventBridge マネージドルール GuardDuty を作成および管理しますDO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*。

データ保護のためのガードレール

Malware Protection for S3 は Amazon EventBridge 通知をリッスンします。オブジェクトが選択したバケットまたはプレフィックスのいずれかにアップロードされると、 を使用してそのオブジェクト GuardDuty をダウンロードAWS PrivateLinkし、同じリージョン内の隔離された環境でオブジェクトを読み取り、復号化、スキャンします。スキャン中は、 はダウンロードした S3 オブジェクトをスキャン環境に GuardDuty 一時的に保存します。マルウェアスキャンが完了すると、 はダウンロードしたオブジェクトのコピー GuardDuty を削除します。

S3 オブジェクトのスキャン結果を表示する

GuardDuty は、S3 オブジェクトスキャン結果イベントを Amazon の EventBridge デフォルトイベントバスに発行します。 GuardDuty は、スキャンされたオブジェクトの数やスキャンされたバイト数などのスキャンメトリクスも Amazon に送信します CloudWatch。タグ付けを有効にした場合、 GuardDuty は事前定義されたタグGuardDutyMalwareScanStatusと潜在的なスキャン結果をタグ値として追加します。

GuardDuty サービスが有効になっている場合の S3 の Malware Protection の使用 (ディテクター ID)

マルウェアスキャンで S3 オブジェクト内の潜在的に悪意のあるファイルが検出されると、GuardDuty は関連する検出結果を生成します。検出結果の詳細を表示し、推奨されるステップを使用して検出結果を修正できます。検出結果のエクスポート頻度 に基づいて、生成された検出結果は S3 バケットと EventBridge イベントバスにエクスポートされます。

Malware Protection for S3 を独立した機能として使用する (ディテクター ID なし)

GuardDuty に関連付けられたディテクター ID がないため、 は検出結果を生成できません。S3 オブジェクトのマルウェアスキャンステータスを知るには、 がデフォルトのイベントバス GuardDuty に自動的に発行するスキャン結果を表示できます。 CloudWatch メトリクスを表示して、スキャンを試み GuardDuty たオブジェクトとバイト数を評価することもできます。 CloudWatch アラームを設定して、スキャン結果に関する通知を受け取ることができます。S3 オブジェクトのタグ付けを有効にしている場合は、S3 オブジェクトで`GuardDutyMalwareScanStatus`タグキーとスキャン結果タグ値を確認することで、マルウェアスキャンのステータスを表示することもできます。

Malware Protection for S3 の機能

次のリストは、バケットで Malware Protection for S3 を有効にした後に期待または実行できることの概要を示しています。

- スキャン対象の選択 — 選択した S3 バケットに関連付けられているすべてのプレフィックスまたは特定のプレフィックス (最大 5 つ) にアップロードされたファイルをスキャンします。
- アップロードされたオブジェクトの自動スキャン – バケットに対して Malware Protection for S3 を有効にすると、 は自動的にスキャンを開始し、新しくアップロードされたオブジェクト内の潜在的なマルウェアを検出 GuardDuty します。
- コンソール、API/AWS CLI、または を使用して を有効にする AWS CloudFormation – Malware Protection for S3 を有効にする任意の方法を選択します。

  Terraform などの Infrastructure as Code (IaC) プラットフォームを使用して、S3 の Malware Protection を有効にできます。詳細については、「リソース：`aws_guardduty_malware_protection_plan`」を参照してください。
- スキャンされた S3 オブジェクトのタグ付けをサポート (オプション) — マルウェアスキャンのたびに、アップロードされた S3 オブジェクトのスキャンステータスを示すタグ GuardDuty が追加されます。このタグを使用して、S3 オブジェクトのタグベースのアクセスコントロール (TBAC) を設定できます。例えば、悪意のあることが判明し、タグ値が である S3 オブジェクトへのアクセスを制限できます`THREATS_FOUND`。
- Amazon EventBridge 通知 – EventBridge ルールを設定すると、S3 マルウェアスキャンのステータスに関する通知が送信されます。

  EventBridge メンバーアカウントが自分のアカウントに属する Amazon S3 バケットに対してこの保護を有効にすると、委任 GuardDuty 管理者アカウントに通知が送信されます。

- CloudWatch metrics – GuardDuty コンソールに埋め込まれたメトリクスを表示します。これらのメトリクスには、S3 オブジェクトに関する詳細が含まれます。

も有効にすると GuardDuty、S3 オブジェクトに悪意のある可能性のあるファイルが含まれていると識別されたときに、セキュリティ検出結果を受け取ります。生成された検出結果を修正するのに役立つ手順 GuardDuty を推奨します。

Malware Protection for S3 の料金

無料利用枠プラン (スキャンコスト)

各 には、各リージョンの 1 か月あたりの特定の制限までの使用量を含む 12 か月の無料利用枠 AWS アカウント が付与されます。使用量が指定された制限を超えた場合、超過した制限の使用コストが発生します。指定された制限と料金の例については、GuardDuty 「 保護プランの料金」を参照してください。

- 既存の AWS アカウント はすべて、2024 年 6 月 11 日から 2025 年 6 月 11 日まで、この機能に 12 か月間の無料利用枠を使用できます。アカウントのこの延長された 12 か月間の無料利用枠は、Malware Protection for S3 の使用に適用されます。他の機能 AWS のサービス や他の GuardDuty 機能はありません。

  2025 年 6 月 11 日以降、またはアカウントの 12 か月間の無料利用枠が終了した後に既存の が S3 の Malware Protection の使用 AWS アカウント を開始した場合、関連する使用コストが発生します。
- 新しい があり、Malware Protection for S3 AWS アカウント の一般提供 (2024 年 6 月 11 日) 後に 12 か月間の無料利用枠が開始された場合、この機能の 12 か月間の無料利用枠期間は、アカウントの 12 か月間の無料利用枠期間と同じになります。

Malware Protection for S3 を有効にした後の使用コストについては、「」を参照してくださいMalware Protection for S3 の使用状況とコストの表示。

S3 オブジェクトタグ付けの使用コスト

Malware Protection for S3 を有効にする場合、スキャンした S3 オブジェクトのタグ付けを有効にすることはオプションです。S3 オブジェクトタグ付けを有効にすることを選択した場合、関連する使用コストが発生します。コストの詳細については、Amazon S3 料金ページの「管理とインサイト」タブを参照してください。

S3 オブジェクトタグ付けの使用コストは、 無料利用枠プランには含まれていません。

Amazon S3 APIs- GETおよびPUT使用コスト

が IAM に基づいて Amazon S3 APIs GuardDuty を実行すると、使用コストが発生します PassRole。例えば、IAM を想定した後 PassRole、 GuardDuty は `PutObject` API を実行して、選択したバケットにテストオブジェクトを追加します。これにより、この機能の有効なステータスを評価するのに役立ちます GuardDuty。

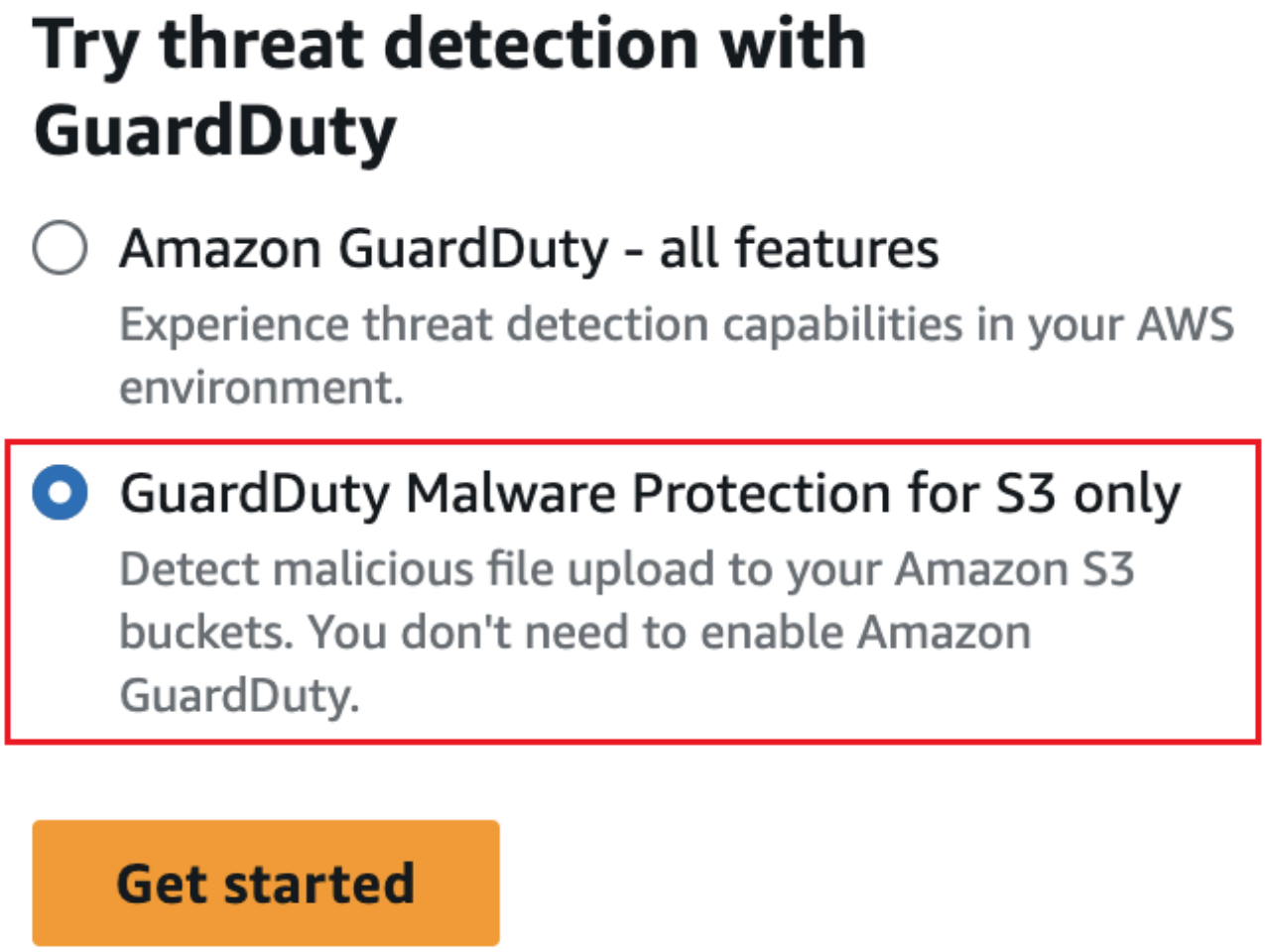
での S3 API コールの料金については AWS リージョン、Amazon S3 料金ページの「ストレージとリクエスト」タブの「リクエストとデータの取得」を参照してください。

(オプション) GuardDuty Malware Protection for S3 を個別に開始する (コンソールのみ)

このオプションのステップは、 GuardDuty のステータスに関係なく、S3 脅威検出用 Malware Protection オプションの使用を開始する場合に使用します AWS アカウント。アカウント GuardDuty で を既に有効にしている場合は、このステップをスキップして を続行できますバケットの S3 の Malware Protection の設定。

Malware Protection for S3 のみの脅威検出を開始する手順

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. GuardDuty S3 のみの Malware Protection を選択します。これにより、Amazon Simple Storage Service (Amazon S3) バケットに新しくアップロードされたファイルにマルウェアが含まれている可能性があるかどうかを検出できます。



3. [開始する] を選択します。これで、「」の手順に進むことができますバケットの S3 の Malware Protection の設定。

バケットの S3 の Malware Protection の設定

このセクションでは、前提条件を追加し、自分のアカウントに属する Amazon S3 バケットの S3 の Malware Protection を有効にする手順について説明します。 Amazon S3 以下のセクションの手順は、Malware Protection for S3 を個別に開始するか、 GuardDuty サービスの一部として有効にしても変わりません。

この脅威検出を S3 バケットに追加するたびに、次の手順を実行します。

1. 前提条件 - IAM PassRole ポリシーを作成または更新する
2. バケットの S3 の Malware Protection を有効にする

前提条件 - IAM PassRole ポリシーを作成または更新する

Malware Protection for S3 が S3 オブジェクトをスキャンして (オプションで) タグを追加するには、以下の必要なアクセス許可を含む IAM ロールを作成してアタッチする必要があります。

- Malware Protection for S3 が S3 S3 オブジェクト通知をリッスンできるように、Amazon EventBridge アクションが EventBridge マネージドルールを作成および管理できるようにします。

  詳細については、「Amazon ユーザーガイド」の「Amazon EventBridge マネージドルール」を参照してください。 EventBridge
- このバケット内のすべてのイベント EventBridge について、Amazon S3 および EventBridge アクションが に通知を送信することを許可する

  詳細については、「Amazon S3 EventBridgeAmazon S3の有効化」を参照してください。
- Amazon S3 アクションがアップロードされた S3 オブジェクトにアクセスし、スキャンされた S3 オブジェクト`GuardDutyMalwareScanStatus`に事前定義されたタグ を追加できるようにします。オブジェクトプレフィックスを使用する場合は、ターゲットプレフィックスにのみ`s3:prefix`条件を追加します。これにより、 はバケット内のすべての S3 オブジェクトにアクセスできなくなります GuardDuty。
- サポートされている DSSE-KMS および SSE-KMS 暗号化を使用して、スキャンしてテストオブジェクトをバケットに配置する前に、KMS キーアクションがオブジェクトにアクセスできるようにします。

> **Note**
>
> このステップは、アカウント内のバケットに対して Malware Protection for S3 を有効にするたびに必要です。既存の IAM がある場合は PassRole、そのポリシーを更新して、別の S3 バケットリソースの詳細を含めることができます。このIAM ポリシーのアクセス許可の追加トピックでは、これを行う方法の例を示します。

次のポリシーを使用して、IAM を作成または更新します PassRole。

ポリシー

- IAM ポリシーのアクセス許可の追加
- 信頼関係ポリシーの追加

IAM ポリシーのアクセス許可の追加

既存の IAM のインラインポリシーを更新するか PassRole、新しい IAM を作成するかを選択できます PassRole。ステップの詳細については、「IAM ユーザーガイド」の「IAM ロールの作成」または「ロールのアクセス許可ポリシーの変更」を参照してください。

次のアクセス許可テンプレートを優先 IAM ロールに追加します。次のプレースホルダー値を、アカウントに関連付けられた適切な値に置き換えます。

- *DOC-EXAMPLE-BUCKET* の場合は、 を Amazon S3 バケット名に置き換えます。

  複数の S3 バケットリソース PassRole に同じ IAM を使用するには、次の例に示すように既存のポリシーを更新します。

```
...
...
"Resource": [
    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
    "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
],
...
...
```

  S3 バケットに関連付けられた新しい ARN を追加する前に、必ずカンマ (,) を追加してください。これは、ポリシーテンプレートResourceで S3 バケットを参照する場所で行います。

- *111122223333* の場合は、 を AWS アカウント ID に置き換えます。
- *us-east-1* の場合は、 をお使いの に置き換えます AWS リージョン。
- *APKAEIBAERJR2EXAMPLE*の場合は、 をカスタマーマネージドキー ID に置き換えます。バケットが を使用して暗号化されている場合は AWS KMS key、次の例に示すように*、プレースホルダー値を に置き換えます。

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

IAM PassRole ポリシーテンプレート

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ],
            "Condition": {
                "StringLike": {
                    "events:ManagedBy": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
            "Effect": "Allow",
            "Action": [
                "events:DescribeRule",
                "events:ListTargetsByRule"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ]
        },
        {
            "Sid": "AllowPostScanTag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:GetObjectVersionTagging"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        },
        {
            "Sid": "AllowEnableS3EventBridgeEvents",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketNotification",
                "s3:GetBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
            ]
        },
        {
            "Sid": "AllowPutValidationObject",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/malware-protection-resource-
validation-object"
            ]
        },
        {
            "Sid": "AllowCheckBucketOwnership",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
            ]
        },
        {
           "Sid": "AllowMalwareScan",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        },
        {
            "Sid": "AllowDecryptForMalwareScan",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                }
            }
        }
    ]
}
```

信頼関係ポリシーの追加

次の信頼ポリシーを IAM ロールにアタッチします。ステップの詳細については、「ロールの信頼ポリシーの変更」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

バケットの S3 の Malware Protection を有効にする

このセクションでは、自分のアカウントで選択したバケットに対して Malware Protection for S3 を有効にする方法の詳細な手順について説明します。

バケットの S3 の Malware Protection を有効にする手順

- S3 バケットの詳細を入力する
- (オプション) スキャンされたオブジェクトにタグを付ける
- アクセス許可
- (オプション) Malware Protection プラン ID にタグを付ける
- Malware Protection for S3 を有効にした後のステップ

S3 バケットの詳細を入力する

Amazon S3 バケットの詳細を指定するには、次の手順に従います。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、Malware Protection for S3 を有効にするリージョンを選択します。
3. ナビゲーションペインで、Malware Protection for S3 を選択します。
4. 保護対象バケット セクションで、有効化 を選択して、独自の に属する S3 バケットの S3 の Malware Protection を有効にします AWS アカウント。
5. S3 バケットの詳細を入力」で、Amazon S3 バケット名を入力します。または、S3 を参照 を選択して S3 バケットを選択します。

   S3 バケット AWS リージョン の と、S3 の Malware Protection AWS アカウント を有効にするは同じである必要があります。例えば、アカウントが `us-east-1`リージョンに属している場合、Amazon S3 バケットリージョンも である必要がありま`us-east-1`す。
6. プレフィックス では、S3 バケット内のすべてのオブジェクト、または特定のプレフィックスで始まるオブジェクトを選択できます。

   - 選択したバケットに新しくアップロードされたすべてのオブジェクトをスキャンできるようにする場合は、S3 バケット内のすべてのオブジェクトを選択します。 GuardDuty
   - 特定のプレフィックスに属する新しくアップロードされたオブジェクトをスキャンする場合は、特定のプレフィックスで始まるオブジェクトを選択します。このオプションは、選択した

オブジェクトプレフィックスのみにマルウェアスキャンの範囲を絞り込むのに役立ちます。プレフィックスの使用の詳細については、Amazon S3 ユーザーガイド」の「フォルダを使用して Amazon S3 コンソールでオブジェクトを整理する」を参照してください。 Amazon S3

プレフィックスを追加 を選択し、プレフィックスを入力します。最大 5 つのプレフィックスを追加できます。

(オプション) スキャンされたオブジェクトにタグを付ける

これは任意の手順です。オブジェクトがバケットにアップロードされる前にタグ付けオプションを有効にするGuardDutyMalwareScanStatusと、スキャンが完了すると、 GuardDuty は、キーが 、値がスキャン結果として事前定義されたタグを追加します。Malware Protection for S3 を最適に使用するには、スキャン終了後に S3 オブジェクトにタグを追加するオプションを有効にすることをお勧めします。標準の S3 オブジェクトタグ付けコストが適用されます。詳細については、「Malware Protection for S3 の料金」を参照してください。

タグ付けを有効にする理由

- タグ付けを有効にすることは、マルウェアスキャン結果を知る方法の 1 つです。S3 マルウェアスキャンの結果については、「」を参照してくださいS3 オブジェクトスキャンステータスのモニタリング。
- 悪意のある可能性のあるオブジェクトを含む S3 バケットにタグベースのアクセスコントロール (TBAC) ポリシーを設定します。考慮事項とタグベースのアクセスコントロール (TBAC) の実装方法については、「」を参照してくださいMalware Protection for S3 でのタグベースのアクセスコントロール (TBAC) の使用。

が S3 オブジェクト GuardDuty にタグを追加する際の考慮事項：

- デフォルトでは、オブジェクトに最大 10 個のタグを関連付けることができます。詳細については、「Amazon S3 ユーザーガイド」の「タグを使用したストレージの分類」を参照してください。 Amazon S3

  すでに 10 個のタグがすべて使用されている GuardDuty 場合は、スキャンされたオブジェクトに事前定義されたタグを追加できません。 GuardDuty は、スキャン結果をデフォルトの EventBridge イベントバスに発行します。詳細については、「Amazon の使用 EventBridge」を参照してください。
- 選択した IAM ロールに の S3 オブジェクト GuardDuty へのタグ付けのアクセス許可が含まれていない場合、保護されたバケットに対してタグ付けが有効になっている場合でも、 GuardDuty はこ

のスキャンされた S3 オブジェクトにタグを追加できません。タグ付けに必要な IAM ロールのアクセス許可の詳細については、「」を参照してください前提条件 - IAM PassRole ポリシーを作成または更新する。

GuardDuty は、スキャン結果をデフォルトの EventBridge イベントバスに発行します。詳細については、「Amazon の使用 EventBridge」を参照してください。

スキャンされたオブジェクトのタグ付けでオプションを選択するには

- スキャンした S3 オブジェクトにタグを追加する場合は GuardDuty 、オブジェクトのタグ付け を選択します。
- スキャンした S3 オブジェクトにタグを追加しない場合は GuardDuty 、オブジェクトにタグを付けない を選択します。

アクセス許可

次の手順を使用して、ユーザーに代わってマルウェアスキャンアクションを実行するために必要なアクセス許可を持つ IAM ロールを選択します。これらのアクションには、新しくアップロードされた S3 オブジェクトのスキャンや、それらのオブジェクトへのタグの追加 (オプション) が含まれる場合があります。

IAM ロール名を選択するには

1. のステップをすでに実行している場合は前提条件 - IAM PassRole ポリシーを作成または更新する、次の手順を実行します。
   - 「アクセス許可」セクションの「IAM ロール名」で、必要なアクセス許可を含む IAM ロール名を選択します。
2. のステップをまだ実行していない場合は前提条件 - IAM PassRole ポリシーを作成または更新する、次の手順を実行します。
   a. アクセス許可の表示 を選択します。
   b. アクセス許可の詳細 で、ポリシー タブを選択します。これは、必要な IAM アクセス許可のテンプレートを示しています。

      このテンプレートをコピーし、アクセス許可の詳細ウィンドウの最後に閉じるを選択します。

c. 新しいタブで IAM コンソールを開くポリシーをアタッチを選択します。新しい IAM ロールを作成するか、コピーされたテンプレートからのアクセス許可を使用して既存の IAM ロールを更新するかを選択できます。

このテンプレートにはプレースホルダー値が含まれており、バケットと に関連付けられた適切な値に置き換える必要があります AWS アカウント。

d. GuardDuty コンソールでブラウザタブに戻ります。アクセス許可を再度表示を選択します。

e. アクセス許可の詳細 で、信頼関係タブを選択します。これは、IAM ロールの信頼関係ポリシーのテンプレートを示しています。

このテンプレートをコピーし、アクセス許可の詳細ウィンドウの最後に閉じるを選択します。

f. IAM コンソールが開いているブラウザタブに移動します。任意の IAM ロールに、この信頼関係ポリシーを追加します。

3. この保護されたリソース用に作成された Malware Protection プラン ID にタグを追加するには、次のセクションに進みます。それ以外の場合は、このページの最後にある有効化を選択して、保護されたリソースとして S3 バケットを追加します。

(オプション) Malware Protection プラン ID にタグを付ける

これは、S3 バケットリソース用に作成される Malware Protection プランリソースにタグを追加するのに役立つオプションのステップです。

各タグには、タグキーとオプションのタグ値の 2 つの部分があります。タグ付けとその利点の詳細については、「AWS リソースのタグ付け」を参照してください。

Malware Protection プランリソースにタグを追加するには

1. タグのキーとオプションの値を入力します。タグキーとタグ値の両方で大文字と小文字が区別されます。タグキーとタグ値の名前については、「タグの命名制限と要件」を参照してください。
2. Malware Protection プランリソースにタグを追加するには、新しいタグを追加を選択し、前のステップを繰り返します。 リソースごとに最大 50 個のタグを追加できます。
3. [Enable (有効化)] を選択します。

Malware Protection for S3 を有効にした後のステップ

バケット (または特定のオブジェクトプレフィックス) の Malware Protection for S3 を有効にしたら、リストされている順序で次の手順を実行します。

1. タグベースのアクセスコントロール (TBAC) リソースポリシーの追加 – タグ付けを有効にし、選択したバケットにオブジェクトをアップロードする前に、必ず TBAC ポリシーを S3 バケットリソースに追加してください。詳細については、「S3 バケットリソースへの TBAC の追加」を参照してください。
2. Malware Protection プランのステータスをモニタリングする – 保護された各バケットの Protection ステータス列をモニタリングします。潜在的なステータスとその意味については、「」を参照してくださいMalware Protection プランのリソースステータス。
3. オブジェクトをアップロードする：
    1. https://console.aws.amazon.com/s3/でAmazon S3 コンソールを開きます。
    2. この機能を有効にした S3 バケットまたはオブジェクトプレフィックスにファイルをアップロードします。ファイルをアップロードする手順については、「Amazon S3 ユーザーガイド」の「バケットにオブジェクトをアップロードする」を参照してください。 Amazon S3
4. S3 オブジェクトスキャンステータスのモニタリング – このステップには、S3 オブジェクトのマルウェアスキャンステータスを確認する方法に関する情報が含まれています。

S3 の GuardDuty と Malware Protection の両方を有効化	S3 でのみ Malware Protection を有効にしました
• GuardDuty を有効にすると、スキャンされた S3 オブジェクトにマルウェアが存在するS3 検出結果タイプの Malware Protectionことを示す が生成されます。 • S3 オブジェクトのスキャン結果は、 で 1 つ以上のオプションを使用して確認できますS3 オブジェクトスキャンステータスのモニタリング。これには、Amazon の使用 EventBridge、Malware Protection プランの CloudWatch メトリクス、スキャンされたオブジェクトのタグ付けが含まれます。	S3 オブジェクトのスキャン結果は、 で 1 つ以上のオプションを使用して確認できますS3 オブジェクトスキャンステータスのモニタリング。これには、Amazon の使用 EventBridge、Malware Protection プランの CloudWatch メトリクス、スキャンされたオブジェクトのタグ付けが含まれます。

Malware Protection プランのリソースステータス

このセクションでは、Malware Protection プランリソースに関連するさまざまな保護ステータス値について説明します。

ステータス	説明
[アクティブ]	S3 バケットが Malware Protection for S3 で正常に設定されました。
警告*	バケットは保護されていません。この S3 オブジェクトに関連付けられているマルウェアスキャンの一部が完了しない可能性があります。修正しないと、すべてのオブジェクトで重大な障害が発生する可能性があります。考えられる根本原因が 1 つ以上ある可能性があります。
エラー*	バケットは保護されていません。この S3 バケットに関連付けられているマルウェアスキャンは完了しません。考えられる根本原因が 1 つ以上ある可能性があります。

*潜在的な問題とその解決のための対応する手順については、「」を参照してくださいMalware Protection プランのステータス詳細のトラブルシューティング。

Malware Protection プランのステータス詳細のトラブルシューティング

保護されたバケットの場合、 はランク付けに基づいてステータス GuardDuty を表示します。例えば、保護されたバケットにエラーカテゴリと警告カテゴリの両方の問題がある場合、 GuardDuty はまずエラーステータスに関連付けられた問題を表示します。

次の表に、ステータスの詳細と、これらの問題を解決するための対応する手順を示します。

ステータス	問題	ステータスの詳細	トラブルシューティングの手順
警告	テストオブジェクトを	選択したバケットの設定を検証するために、	選択した IAM ロールに次のアクセス許可を追加して、 が GuardDuty選択した

ステータス	問題	ステータスの詳細	トラブルシューティングの手順
	配置できない	GuardDuty はテストオブジェクトをバケットに配置します。	リソースにテストオブジェクトを配置できるようにします。 `{ "Sid": "AllowPut ValidationObject", "Effect": "Allow", "Action": [ "s3:PutObject" ], "Resource": [ "arn:aws:s3::: DOC-EXAMPLE-BUCKET /malware-protection-resource-validation-object" ] }` *DOC-EXAMPLE-BUCKET* を Amazon S3 バケット名に置き換えます。IAM ロールのアクセス許可の詳細については、「」を参照してください前提条件 - IAM PassRole ポリシーを作成または更新する。 ステータス列の値がアクティブ に変わるまでに数分かかる場合があります。

ステータス	問題	ステータスの詳細	トラブルシューティングの手順

	S3 セットアップの Malware Protection をモニタリングできない	IAM ロールに、このバケットの Malware Protection for S3 設定をモニタリング GuardDuty するための のアクセス許可がありません。	IAM ロールに次のアクセス許可を追加します。
			
			{
			"Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
			"Effect": "Allow",
			"Action": [
			"events:PutRule",
			"events:DeleteRule",
			"events:PutTargets",
			"events:RemoveTargets"
			],
			"Resource": [
			"arn:aws:events: *us-east-1* :*111122223333* :rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
			],
			"Condition": {
			"StringEquals": {
			"events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
			}
			}
			},
			{
			"Sid": "AllowEnableS3EventBridgeEvents",
			"Effect": "Allow",
			"Action": [
			"s3:PutBucketNotification",
			"s3:GetBucketNotification"

ステータス	問題	ステータスの詳細	トラブルシューティングの手順

			<pre>],
			"Resource": [
			"arn:aws:s3::: *DOC-EXAMPLE-BUCKET* "
			]
			}</pre>
			ステータス列の値がアクティブ に変わるまでに数分かかる場合があります。

ステータス	問題	ステータスの詳細	トラブルシューティングの手順
エラー	EventBridge この S3 バケットの通知は無効になっています。	GuardDuty は EventBridge 、新しいオブジェクトがこの S3 バケットにアップロードされたときに通知を受け取るためにを使用します。このアクセス許可は IAM ロールにありません。	• オプション 1: IAM ロールに次のアクセス許可ステートメントを追加します。 `{ "Sid": "AllowEnableS3EventBridgeEvents", "Effect": "Allow", "Action": [ "s3:PutBucketNotification", "s3:GetBucketNotification" ], "Resource": [ "arn:aws:s3::: DOC-EXAMPLE-BUCKET " ] }` *DOC-EXAMPLE-BUCKET* を Amazon S3 バケット名に置き換えます。 • オプション 2: Amazon S3 コンソールを使用して EventBridge 通知を有効にする 1. https://console.aws.amazon.com/s3/でAmazon S3 コンソールを開きます。 2. バケット ページの汎用バケット タブで、このエラーに関連付けられたバケット名を選択します。 3. このバケットページで、プロパティタブを選択します。

ステータス	問題	ステータスの詳細	トラブルシューティングの手順
			4. Amazon EventBridge セクションで、編集 を選択します。 5. Amazon の編集 EventBridge ページで、このバケット 内のすべてのイベント EventBridge について Amazon に通知を送信するで、 で を選択します。 6. [変更の保存] を選択します。 ステータス列の値がアクティブ に変わるまでに数分かかる場合があります。

ステータス	問題	ステータスの詳細	トラブルシューティングの手順

	EventBridge S3 バケットイベントを受信する マネージドルールがありません。	ルール設定を管理するための EventBridge マネージド EventBridge ルールのアクセス許可がありません。	IAM ロールに次のアクセス許可ステートメントを追加します。
			
			{
			"Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
			"Effect": "Allow",
			"Action": [
			"events:PutRule",
			"events:DeleteRule",
			"events:PutTargets",
			"events:RemoveTargets"
			],
			"Resource": [
			"arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
			],
			"Condition": {
			"StringEquals": {
			"events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
			}
			}
			}
			
			ステータス列の値がアクティブ に変わるまでに数分かかる場合があります。

ステータス	問題	ステータスの詳細	トラブルシューティングの手順
	この S3 バケットは存在しません。	この S3 バケットはアカウントから削除され、存在しなくなりました。	S3 バケットの削除が意図的なものでなかった場合は、Amazon S3 コンソールを使用して新しいバケットを作成できます。 バケットが正常に作成されたら、ページの手順に従って Malware Protection for S3 を有効にしますバケットの S3 の Malware Protection の設定。

S3 オブジェクトスキャンステータスのモニタリング

GuardDuty ディテクター ID で Malware Protection for S3 を使用する場合、Amazon S3 オブジェクトが悪意のある可能性がある場合、 GuardDuty は を生成しますS3 検出結果タイプの Malware Protection。 GuardDuty コンソールと APIsを使用して、生成された結果を表示できます。この検出結果タイプを理解する方法については、「」を参照してください検出結果の詳細。

を有効にせずに Malware Protection for S3 を使用する場合 GuardDuty （ディテクター ID なし）、スキャンした Amazon S3 オブジェクトが悪意のある可能性がある場合でも、 GuardDuty は検出結果を生成できません。

次のリストは、潜在的な S3 オブジェクトスキャン結果の値を示しています。

- NO_THREATS_FOUND – スキャンされたオブジェクトに関連する潜在的な脅威 GuardDuty が検出されませんでした。
- THREATS_FOUND – スキャンされたオブジェクトに関連する潜在的な脅威 GuardDuty を検出しました。
- UNSUPPORTED –このタイプのオブジェクト GuardDuty のスキャンはサポートされていません。この S3 オブジェクトは、スキャン時にスキップされます。サポートされているオブジェクトの詳細については、「」を参照してくださいMalware Protection for S3 のクォータ。
- ACCESS_DENIED – GuardDuty スキャンのためにこのオブジェクトにアクセスできません。このバケットに関連付けられている IAM ロールのアクセス許可を確認します。詳細については、「前提条件 - IAM PassRole ポリシーを作成または更新する」を参照してください。

- FAILED - GuardDuty 内部エラーのため、このオブジェクトに対してマルウェアスキャンを実行できません。

S3 オブジェクトのスキャン結果をモニタリングする方法

- Amazon の使用 EventBridge
- Malware Protection プランの Amazon CloudWatch メトリクスの使用
- Malware Protection for S3 でのオブジェクトタグ付けの有効化

Amazon の使用 EventBridge

Amazon EventBridge は、アプリケーションをさまざまなソースのデータに簡単に接続できるサーバーレスイベントバスサービスです。 は、独自のアプリケーション、S oftware-as-aサービス (SaaS) アプリケーション、および AWS のサービスからリアルタイムデータのストリームを EventBridge 配信し、そのデータを Lambda などのターゲットにルーティングします。これにより、サービスで発生したイベントをモニタリングし、イベント駆動型アーキテクチャを構築できます。詳細については、「Amazon ユーザーガイド EventBridge 」を参照してください。

Malware Protection for S3 で保護されている S3 バケットの所有者アカウントとして、 GuardDuty は次のシナリオでデフォルトのイベントバス EventBridge に通知を発行します。

- 保護されたバケットの Malware Protection プランのリソースステータスが変更されます。さまざまなステータスについては、「」を参照してくださいMalware Protection プランのリソースステータス。
- 次の理由により、タグイベントが失敗します。
  - IAM にオブジェクトにタグを付けるアクセス許可 PassRole がありません。

    IAM ポリシーのアクセス許可の追加 テンプレートには、オブジェクトにタグを付ける GuardDuty ための のアクセス許可が含まれています。
  - IAM で指定されたバケットリソースまたはオブジェクトが存在し PassRole なくなりました。
  - 関連付けられた S3 オブジェクトが既にタグの上限に達しています。タグの制限の詳細については、「Amazon S3 ユーザーガイド」の「タグを使用したストレージの分類」を参照してください。 Amazon S3
- S3 オブジェクトのスキャン結果は、デフォルトの EventBridge イベントバスに発行されます。

EventBridge ルールの設定

アカウントで EventBridge ルールを設定して、リソースステータス、スキャン後のタグ失敗イベント、または S3 オブジェクトスキャン結果を別の に送信できます AWS のサービス。委任 GuardDuty 管理者アカウントとして、ステータスに変更があると、Malware Protection プランのリソースステータス通知を受け取ります。

標準 EventBridge 料金が適用されます。詳細については、「Malware Protection for S3 の料金」を参照してください。

##で表示される値はすべて、この例のプレースホルダーです。これらの値は、S3 オブジェクトのスキャン結果に基づいて変わります。

Malware Protection プランのリソースステータス

EventBridge イベントパターンは、次のシナリオに基づいて作成できます。

潜在的な**detail-type**値

- "GuardDuty Malware Protection Resource Status Active"
- "GuardDuty Malware Protection Resource Status Warning"
- "GuardDuty Malware Protection Resource Status Error"

イベントパターン

```
{
      "detail-type": ["potential detail-type"],
      "source": ["aws.guardduty"]
}
```

のサンプル通知スキーマ **GuardDuty Malware Protection Resource Status Active**

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status Active",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
```

```
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "DOC-EXAMPLE-BUCKET"
        },
        "resourceStatus": "ACTIVE"
    }
}
```

GuardDuty Malware Protection Resource Status Errorまたは のサンプル通知スキーマ GuardDuty Malware Protection Resource Status Warning

```
{
    "version": "0",
    "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
    "detail-type": "GuardDuty Malware Protection Resource Status Error or Warning",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "DOC-EXAMPLE-BUCKET"
        },
        "resourceStatus": "ERROR",
        "statusReasons": [{
            "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
        }, {
            "code": "PROTECTED_RESOURCE_DELETED"
        }]
    }
}
```

resourceStatus 値は Warning または Error のいずれかです。

保護されたバケットのステータス列が警告 またはエラー のいずれかに変わると、そのstatusReasons値は根本的な理由に基づいて入力されます。トラブルシューティングの手順については、「」を参照してくださいMalware Protection プランのステータス詳細のトラブルシューティング。

タグ後失敗イベント

イベントパターン：

```
{
      "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
      "source": "aws.guardduty"
 }
```

通知スキーマの例：

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "DOC-EXAMPLE-BUCKET",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6"
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "status": "FAILED",
            "failureReason": "ACCESS_DENIED"
        }]
    }
}
```

可能なfailureReason値には、 ACCESS_DENIEDと が含まれますMAX_TAG_LIMIT_EXCEEDED。

S3 オブジェクトスキャン結果

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

のサンプル通知スキーマ **NO_THREATS_FOUND**

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "versionId": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "DOC-EXAMPLE-BUCKET",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "NO_THREATS_FOUND",
            "threats": null
        }
    }
}
```

のサンプル通知スキーマ **THREATS_FOUND**

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
```

```
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "versionId": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "DOC-EXAMPLE-BUCKET",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "threats": [
                {
                    "name": "EICAR-Test-File (not a virus)"
                }
            ]
        }
    }
}
```


Malware Protection プランの Amazon CloudWatch メトリクスの使用

GuardDuty を使用して をモニタリングできます。 CloudWatchこれは raw データを収集し、読み取り可能なほぼリアルタイムのメトリクスに加工します。これらの統計は 15 か月間保持されるため、履歴情報にアクセスして、Malware Protection for S3 の動作をより的確に把握できます。また、特定のしきい値をモニタリングするアラームを設定し、しきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。

Malware Protection for S3 の CloudWatch メトリクスは、リソースレベルで利用できます。これらのメトリクスは、保護されたリソースごとに個別にクエリできます。メトリクスは AWS/GuardDuty/MalwareProtection名前空間で報告されます。特定のリソースにアラームを設定して、セキュリティ体制をモニタリングできます。

マルウェアスキャンステータスメトリクス

メトリクス	説明
CompletedScanCount	特定の期間内に完了した S3 オブジェクトマルウェアスキャンの数。 有効なディメンション： • Malware Protection Plan Id Resource Name 有効な統計: SUM 単位: カウント
FailedScanCount	特定の期間内に完了した S3 オブジェクトマルウェアスキャンの数。 有効なディメンション： • Malware Protection Plan Id Resource Name 有効な統計: Sum 単位: カウント
SkippedScanCount	特定の期間内にスキップされた S3 オブジェクトマルウェアスキャンの数。 有効なディメンション： • Malware Protection Plan Id Resource Name Skipped Reason

	考えられる値 • UnSupported • MissingPermissions 有効な統計: Sum 単位: カウント
マルウェアスキャン結果メトリクス	
InfectedScanCount	特定の期間内に悪意のある可能性のあるオブジェクトを検出した S3 オブジェクトマルウェアスキャンの数。 有効なディメンション： • Malware Protection Plan Id Resource Name 有効な統計: Sum 単位: カウント
CompletedScanBytes	特定の時間枠にスキャンされた S3 オブジェクトのバイト数。 有効なディメンション： • Malware Protection Plan Id Resource Name 有効な統計: Sum 単位: カウント

> **Note**
>
> デフォルトでは、 CloudWatch メトリクスの統計は AVG です。

Malware Protection for S3 メトリクスでは、次のディメンションがサポートされています。

ディメンション	説明
`Malware Protection Plan Id`	が保護されたリソース用に GuardDuty 作成する Malware Protection プランリソースに関連付けられている一意の識別子。
`Resource Name`	保護されたリソースの名前。
`Skipped Reason`	S3 オブジェクトのマルウェアスキャンがスキップされた理由。 考えられる値 • `UnSupported` • `MissingPermissions`

これらのメトリクスへのアクセスとクエリの詳細については、「Amazon ユーザーガイド」の「Amazon CloudWatch メトリクスの使用」を参照してください。 CloudWatch

アラームの設定の詳細については、「Amazon ユーザーガイド」の「Amazon CloudWatch アラームの使用」を参照してください。 CloudWatch

Malware Protection for S3 でのオブジェクトタグ付けの有効化

タグ付けを有効にするオプションを使用すると GuardDuty 、マルウェアスキャンの完了後に が Amazon S3 オブジェクトにタグを追加できます。

タグ付けを有効にする際の考慮事項

- が S3 オブジェクトに GuardDuty タグを付ける場合、関連する使用コストが発生します。詳細については、「Malware Protection for S3 の料金」を参照してください。

- このバケット PassRole に関連付けられた優先 IAM に必要なタグ付けアクセス許可を保持する必要があります。それ以外の場合は、スキャンされたオブジェクトにタグを追加 GuardDuty できません。IAM には、スキャンされた S3 オブジェクトにタグを追加するアクセス許可が PassRole 既に含まれています。詳細については、「前提条件 - IAM PassRole ポリシーを作成または更新する」を参照してください。
- デフォルトでは、最大 10 個のタグを S3 オブジェクトに関連付けることができます。詳細については、「タグベースのアクセスコントロール (TBAC) の使用」を参照してください。

S3 バケットまたは特定のプレフィックスのタグ付けを有効にすると、新しくアップロードされたスキャンされたオブジェクトには、次のキーと値のペア形式のタグが関連付けられます。

`GuardDutyMalwareScanStatus:`*`Scan-Status`*

潜在的なタグ値については、「」を参照してくださいタグベースのアクセスコントロール (TBAC) の使用。

Malware Protection for S3 でのタグベースのアクセスコントロール (TBAC) の使用

バケットで Malware Protection for S3 を有効にする場合、オプションでタグ付けを有効にするように選択できます。選択したバケットに新しくアップロードされた S3 オブジェクトをスキャンしようとすると、 はスキャンされたオブジェクトにタグ GuardDuty を追加して、マルウェアスキャンのステータスを提供します。タグ付けを有効にすると、直接使用コストがかかります。詳細については、「Malware Protection for S3 の料金」を参照してください。

GuardDuty は、 キーを としてGuardDutyMalwareScanStatus、 値をマルウェアスキャンステータスの 1 つとして、事前定義されたタグを使用します。これらの値の詳細については、「」を参照してくださいS3 object potential scan result value。

が S3 オブジェクト GuardDuty にタグを追加する際の考慮事項：

- デフォルトでは、オブジェクトに最大 10 個のタグを関連付けることができます。詳細については、「Amazon S3 ユーザーガイド」の「タグを使用したストレージの分類」を参照してください。 Amazon S3

  10 個のタグがすべて既に使用されている GuardDuty 場合、スキャンされたオブジェクトに事前定義されたタグを追加することはできません。 GuardDuty は、スキャン結果をデフォルトの

EventBridge イベントバスに発行します。詳細については、「Amazon の使用 EventBridge」を参照してください。

- 選択した IAM ロールに の S3 オブジェクト GuardDuty へのタグ付けのアクセス許可が含まれていない場合、保護されたバケットに対してタグ付けが有効になっている場合でも、 GuardDuty はこのスキャンされた S3 オブジェクトにタグを追加できません。タグ付けに必要な IAM ロールのアクセス許可の詳細については、「」を参照してください前提条件 - IAM PassRole ポリシーを作成または更新する。

  GuardDuty は、スキャン結果をデフォルトの EventBridge イベントバスに発行します。詳細については、「Amazon の使用 EventBridge」を参照してください。

S3 バケットリソースへの TBAC の追加

S3 バケットリソースポリシーを使用して、S3 オブジェクトのタグベースのアクセスコントロール (TBAC) を管理できます。特定のユーザーに S3 オブジェクトへのアクセスと読み取りを許可できます。を使用して作成された組織がある場合は AWS Organizations、 によって追加されたタグを誰も変更できないように強制する必要があります GuardDuty。詳細については、「 AWS Organizations ユーザーガイド」の「許可されたプリンシパルによるタグの変更の防止」を参照してください。リンクされたトピックで使用されている例では、 に言及していますec2。この例を使用する場合は、*ec2* を に置き換えますs3。

次のリストでは、TBAC を使用してできることについて説明します。

- Malware Protection for S3 サービスプリンシパルを除くすべてのユーザーが、次のタグキーと値のペアでまだタグ付けされていない S3 オブジェクトを読み取らないようにします。

  `GuardDutyMalwareScanStatus:`*`Potential key value`*

- スキャンされた S3 オブジェクト GuardDuty に、スキャン結果として値 `GuardDutyMalwareScanStatus` を持つタグキーのみを追加することを許可します。次のポリシーテンプレートでは、アクセス権を持つ特定のユーザーがタグのキーと値のペアを上書きできる可能性があります。

S3 バケットリソースポリシーの例：

`IAM-role-name` を、バケット内の Malware Protection for S3 の設定 PassRole に使用した IAM に置き換えます。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "NoReadExceptForClean",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                    "arn:aws:iam::555555555555:root",
                    "arn:aws:iam::555555555555:role/IAM-role-name",
                    "arn:aws:iam::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection"
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
 "NO_THREATS_FOUND"
                }
            }
        },
        {
            "Sid": "OnlyGuardDutyCanTag",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                    "arn:aws:iam::555555555555:root",
                    "arn:aws:iam::555555555555:role/IAM-role-name",
                    "arn:aws:iam::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection"
                ]
            },
            "Action": "s3:PutObjectTagging",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
```

```
        }
    ]
}
```

S3 リソースのタグ付けの詳細については、「タグ付けとアクセスコントロールポリシー」を参照してください。

保護されたバケットの S3 の Malware Protection の編集

次の手順を使用して、保護された S3 バケットの既存の設定を編集します。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、Malware Protection for S3 を選択します。
3. 保護対象バケット で、既存の設定を編集するバケットを選択します。
4. [編集] を選択します。
5. バケットの既存の設定と設定を更新し、変更を確認します。各セクションの説明と手順については、「」を参照してくださいバケットの S3 の Malware Protection を有効にする。

   この保護されたバケットのステータス列をモニタリングします。警告またはエラー として表示される場合は、「」を参照してくださいMalware Protection プランのステータス詳細のトラブルシューティング。

Malware Protection for S3 の使用状況とコストの表示

Malware Protection for S3 を 無料利用枠プランの特定の制限を超えて使用する場合、またはアカウントの 12 か月間の 無料利用枠プランが終了すると、アカウントで使用コストが発生します。無料利用枠プランの詳細については、「」を参照してくださいMalware Protection for S3 の料金。

使用コストを表示するには、https://console.aws.amazon.com/billing/ コンソールで Cost Explorer に移動します。 AWS アカウント 請求の詳細については、AWS Billing 「 ユーザーガイド」を参照してください。

保護されたバケットの S3 の Malware Protection を無効にする

保護されたバケットの Malware Protection for S3 を無効にすると、 はそのバケットに関連付けられた Malware Protection プラン ID GuardDuty を削除します。 GuardDuty は、新しいオブジェクトが

このバケットまたは選択したオブジェクトプレフィックスのいずれかにアップロードされると、マルウェアスキャンを開始しません。

を有効に GuardDuty して を一時停止または無効にする場合は GuardDuty、「」を参照してください一時停止または無効化 GuardDuty。Malware Protection for S3 にはディテクター ID の概念がないため、無効化または一時停止 GuardDuty しても、アカウント内の保護されたバケットのステータスには影響しません。Malware Protection for S3 機能は、関連する標準料金とは別に引き続き使用できます。詳細については、「Malware Protection for S3 の使用状況とコストの表示」を参照してください。Malware Protection for S3 の使用を停止するには、アカウント内のすべての保護対象バケットで使用を無効にする必要があります。バケットの Malware Protection for S3 のみを使用し GuardDuty 、無効にする場合は、次の手順は、有効にした GuardDuty サービスやその他の保護プランの設定には影響しません。

保護されたバケットの S3 の Malware Protection を無効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、Malware Protection for S3 を選択します。
3. 保護対象バケット で、S3 の Malware Protection を無効にするバケットを選択します。

   一度に選択できる保護対象バケットは 1 つだけです。複数のバケットに対して S3 の Malware Protection を無効にするには、別の S3 バケットに対してこれらのステップを再度実行します。
4. [無効化] を選択します。
5. Disable を選択して選択を確定します。

Malware Protection for S3 のクォータ

このセクションでは、多くの場合制限と呼ばれるデフォルトのクォータについて説明します。指定されていない限り、各クォータはリージョン固有です。基盤 (またはコア) GuardDuty サービスの使用に固有のデフォルトのクォータを表示するには、「」を参照してくださいAmazon GuardDuty クォータ。

次の表は、 に適用される複数のクォータを示しています AWS アカウント。

一般的なクォータ

AWS デフォルトのクォータ値	調整可能ですか？	説明
5 GB	なし	GuardDuty がマルウェアのスキャンを試みる S3 オブジェクトの最大サイズ。
5 GB	なし	アーカイブファイルから抽出および分析 GuardDuty できるデータの最大量 (GB 単位) 。アーカイブファイルに 5 GB 以上が含まれている場合でも、GuardDuty はこの値を超えてコンテンツをスキップします。
1,000	なし	アーカイブファイルで抽出および分析 GuardDuty できるファイルの最大数。ファイルに含まれるファイルが 1,000 個を超える場合、 GuardDuty はアーカイブされたファイルをスキップする必要があります。

AWS デフォルトのクォータ値	調整可能ですか？	説明
5	なし	が抽出 GuardDuty できるネストされたアーカイブの最大レベル。アーカイブにこの値を超えてネストされたファイルが含まれている場合、 GuardDuty はネストされたファイルをスキップします。
10	なし	Malware Protection for S3 を有効にできる S3 バケットの最大数。このクォータ値はリージョンレベルで適用されます。

AWS デフォルトのクォータ値	調整可能ですか？	説明
25	アカウントレベルで	各リージョンで 1 秒あたりに開始できるコントロールプレーンオペレーションの最大数。API オペレーションには、リソースの作成、読み取り、更新、削除が含まれます。このクォータ値は AWS アカウント レベルで適用されます。

マルウェアスキャンを通過するファイル

サポートは利用できますか？	説明
なし	ファイルがパスワードで保護されたアーカイブの場合、暗号化されたバイトがスキャンされます。アーカイブは抽出も解凍もされません。

Amazon S3 の特徴

サポートは利用できますか？	説明
あり	S3 オブジェクトは、非同期的に復元せずに取得できます。

サポートは利用できますか？	説明

サポートは利用できますか？	説明

サポートは利用できますか？	説明
条件付き	• インテリジェント階層化のサポートは、高頻度、低頻度、アーカイブインスタンスアクセス階層の S3 オブジェクトで利用できます。 • オプトインアーカイブ階層とディープアーカイブ階層はサポートされていません。 • インテリジェント階層化は常に高頻度アクセス階層に新しいオブジェクトを作成します。したがって、作成時のオブジェクトスキャンがサポートされています。 • 将来のインテリジェント階層化機能は、アーカイブでオブジェクトを起動する可能性があります。したがって、これはサポートされていません。

サポートは利用できますか？	説明
なし	GuardDuty は、Malware Protection for S3 の汎用バケットのみをサポートします。

サポートは利用できますか？	説明
なし	S3 オブジェクトにアクセスする前に復元する必要があります。
なし	S3 の Malware Protection は Outposts ではサポートされていません。

サポートは利用できますか？	説明
あり	アップロードされたすべての S3 オブジェクトがスキャンされ、マルウェアが検出されます。ファイルバージョン v1 のオブジェクトをアップロードし、すぐに v2 で別のバージョンの上書きをアップロードした場合、GuardDuty はオブジェクトファイルバージョン v1 と v2 の両方をスキャンします。ただし、スキャン開始時刻は同じ順序ではない場合があります。

サポートは利用できますか？	説明
あり	レプリケート先バケットが保護されたリソースである場合、 GuardDuty は、保護およびモニタリングされているプレフィックスにレプリケートされるすべての S3 オブジェクトをスキャンします。

サポートは利用できますか？	説明
なし	スキャン結果タグに基づいてレプリケーションルールを定義することはできません。Amazon S3 は、作成時のを除き、タグのレプリケーションをサポートしていません。

サポートは利用できますか？	説明
あり	GuardDuty は、 マネージドキーとカスタマーマネージドキーで暗号化された S3 オブジェクトのマルウェアスキャンをサポートします。IAM Passrole にキーを使用するアクセス許可が含まれていることを確認します。詳細については、「IAM ポリシーのアクセス許可の追加」を参照してください。

サポートは利用できますか？	説明
なし	Malware Protection for S3 は、アクセスできないキーで暗号化された S3 オブジェクトのスキャンをサポートしていません。
なし	S3 オブジェクトが Amazon S3 暗号化クライアントを使用して暗号化されている場合、オブジェクトは を含むサードパーティーに公開されません AWS。これがサポートされていない理由の詳細については、Amazon S3 ユーザーガイド」の「クライアント側の暗号化を使用したデータの保護」を参照してください。

サポートは利用できますか？	説明
あり	ロックされた S3 オブジェクトは、WORM - Write Once Read Many に基づいてロックされます。Malware Protection for S3 は、オブジェクトにアクセスしてスキャンできます。
あり	Malware Protection for S3 は、リクエスタ支払い で設定されたバケットをスキャンできます。リクエスタは S3 呼び出しに対して料金を支払います。詳細については、「Amazon S3 ユーザーガイド」の「ストレージ転送と使用量のリクエスタ支払いバケットの使用」を参照してください。

サポートは利用できますか？	説明
あり	スキャン結果タグに基づいてライフサイクルポリシーを定義できます。例えば、悪意のあるオブジェクトを自動削除します。lifcycle 設定の詳細については、「Amazon S3 ユーザーガイド」の「ストレージライフサイクルの管理」を参照してください。 Amazon S3
あり	S3 オブジェクトスキャン結果タグに基づいてバケットリソースポリシーを定義できます。例えば、まだスキャンされていない S3 オブジェクトや GuardDuty 検出された脅威へのアクセスを防止します。詳細については、「Malware Protection for S3 でのタグベースのアクセスコントロール (TBAC) の使用」を参照してください。

S3 リージョンクォータの Malware Protection

サポートは利用できますか？	説明
あり	S3 バケットを所有 AWS アカウント する は、Malware Protection プランリソースも所有しています。両方のリソースは同じ にあります AWS リージョン。
なし	Malware Protection プランリソースは、複数の にまたがることはできません AWS アカウント。 AWS アカウント に S3 バケットを所有 AWS アカウント する別の に Malware Protection プランリソースを作成するアクセス許可がある場合 (DOC-EXAMPLE-BUCKET1)、以前のアカウントは DOC-EXAMPLE-BUCKET1 のプランリソースを設定できます。

サポートは利用できますか？	説明
なし	Malware Protection プランのリソースをクロスリージョンで設定することはできません。

での RDS Protection GuardDuty

Amazon の RDS Protection は、Amazon Aurora データベース (Amazon Aurora MySQL 互換エディション および Aurora PostgreSQL 互換エディション) と Amazon RDS for PostgreSQL への潜在的なアクセス脅威について RDS ログインアクティビティ GuardDuty を分析し、プロファイリングします。 PostgreSQL この機能により、潜在的に疑わしいログイン動作を特定できます。RDS Protection は追加のインフラストラクチャが不要で、データベースインスタンスのパフォーマンスに影響を与えないように設計されています。

RDS Protection がデータベースへの脅威を示す潜在的に疑わしい、または異常なログイン試行を検出すると、 は侵害された可能性のあるデータベースに関する詳細を含む新しい検出結果 GuardDuty を生成します。

RDS Protection 機能は、Amazon 内で AWS リージョン この機能が利用可能な の任意のアカウントで GuardDuty、いつでも有効または無効にできます。既存の GuardDuty アカウントは、30 日間のトライアル期間で RDS Protection を有効にできます。新しい GuardDuty アカウントの場合、RDS Protection は既に有効になっており、30 日間の無料トライアル期間に含まれています。詳細については、「コストの見積もり」を参照してください。

> **Note**
>
> RDS Protection 機能が有効になっていない場合、 は RDS ログインアクティビティを収集せず、異常なログイン動作や疑わしいログイン動作も検出 GuardDuty しません。

AWS リージョン が RDS Protection をまだサポートしていない については、 GuardDuty 「」を参照してくださいリージョン固有機能の可用性。

サポートされている Amazon Aurora および Amazon RDS データベース

次の表は、サポートされている Aurora および Amazon RDS データベースのバージョンを示しています。

Amazon Aurora および Amazon RDS DB エンジン	サポート対象エンジンバージョン
Aurora MySQL	• 2.10.2 以降 • 3.02.1 以降
Aurora PostgreSQL	• 10.17 以降 • 11.12 以降 • 12.7 以降 • 13.3 以降 • 14.3 以降 • 15.2 以降 • 16.1 以降
RDS for PostgreSQL	• 14.5 以降 • 13.8 以降 • 12.12 以降 • 11.17 以降 • 10.22 以降 • RDS for PostgreSQL バージョン 15 • RDS for PostgreSQL バージョン 16

RDS Protection が RDS ログインアクティビティモニタリングを使用する仕組み

Amazon の RDS Protection GuardDuty は、アカウントでサポートされている Amazon Aurora (Aurora) データベースを保護するのに役立ちます。RDS Protection 機能を有効にすると、 は、アカウントの Aurora データベースからの RDS ログインアクティビティのモニタリングを GuardDuty 直ちに開始します。 は、以前には見られなかった外部アクターからの、アカウント内の Aurora データベースへの不正アクセスなどの疑わしいアクティビティについて、RDS ログインアクティビティ GuardDuty を継続的にモニタリングおよびプロファイリングします。RDS Protection を初めて有効にする場合、またはデータベースインスタンスを新しく作成した場合は、通常の動作をベースラインにするための学習期間が必要です。このため、新たに有効になったデータベースインスタンスや新し

く作成されたデータベースインスタンスでは、最長で 2 週間程度、関連する異常ログインが検出されないことがあります。詳細については、「RDS ログインアクティビティのモニタリング」を参照してください。

RDS Protection が一連の成功、失敗、または不完全なログイン試行で異常なパターンなどの潜在的な脅威を検出すると、 は侵害された可能性のあるデータベースインスタンスに関する詳細を含む新しい検出結果 GuardDuty を生成します。詳細については、「RDS Protection の検出結果タイプ」を参照してください。RDS Protection を無効にすると、 は RDS ログインアクティビティのモニタリングを GuardDuty 直ちに停止し、サポートされているデータベースインスタンスに対する潜在的な脅威を検出できません。

> **Note**
>
> GuardDuty は、 サポートされているデータベースまたは RDS ログインアクティビティを管理したり、RDS ログインアクティビティを利用できるようにしたりしません。

スタンドアロンアカウントの RDS Protection の設定

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[RDS Protection] を選択します。
3. [RDS Protection] ページにアカウントの現在のステータスが表示されます。[Enable] (有効化) または [Disable] (無効化) を選択することで、いつでもこの機能を有効または無効にできます。[Confirm] (確認) をクリックして、選択内容を確認します。

API/CLI

ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト `name` を `RDS_LOGIN_EVENTS` として、`status` を `ENABLED` または `DISABLED` として渡して、updateDetector API オペレーションを実行します。

次の AWS CLI コマンドを実行して、RDS Protection を有効または無効にすることもできます。必ずご自身の有効な `###### ID` を使用してください。

> **Note**
>
> 次のコードの例は RDS Protection を有効にします。無効にするには、ENABLED を DISABLED に置き換えます。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

マルチアカウント環境での RDS Protection の設定

マルチアカウント環境では、委任された GuardDuty 管理者アカウントのみが、組織内のメンバーアカウントの RDS Protection 機能を有効または無効にすることができます。 GuardDuty メンバーアカウントは、自分のアカウントからこの設定を変更することはできません。委任 GuardDuty 管理者アカウントは、 を使用してメンバーアカウントを管理します AWS Organizations。この委任 GuardDuty 管理者アカウントは、組織に参加するすべての新しいアカウントの RDS ログインアクティビティモニタリングを自動有効化することを選択できます。マルチアカウント環境の詳細については、「Amazon での複数のアカウントの管理 GuardDuty」を参照してください。

委任 GuardDuty 管理者アカウントの RDS Protection の設定

任意のアクセス方法を選択して、委任された GuardDuty 管理者アカウントの RDS ログインアクティビティモニタリングを設定します。

Console

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

   必ず管理アカウントの認証情報を使用してください。
2. ナビゲーションペインで、[RDS Protection] を選択します。
3. [RDS Protection] ページで、[編集] を選択します。
4. 次のいずれかを行います。

[すべてのアカウントについて有効にする] の使用

- [すべてのアカウントについて有効にする] を選択します。これにより、 AWS 組織に参加する新しい GuardDuty アカウントを含め、組織内のすべてのアクティブなアカウントに対して保護プランが有効になります。
- [保存] を選択します。

[アカウントを手動で設定] の使用

- 委任 GuardDuty 管理者アカウントアカウントに対してのみ保護プランを有効にするには、アカウントを手動で設定 を選択します。
- 委任 GuardDuty 管理者アカウント (このアカウント) セクションで 有効化 を選択します。
- [保存] を選択します。

API/CLI

ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト `name` を `RDS_LOGIN_EVENTS` として、`status` を `ENABLED` または `DISABLED` として渡して、updateDetector API オペレーションを実行します。

次の AWS CLI コマンドを実行して、RDS Protection を有効または無効にできます。委任 GuardDuty 管理者アカウントの有効な*###### ID* を使用してください。

> **Note**
>
> 次のコードの例は RDS Protection を有効にします。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

すべてのメンバーアカウントの RDS Protection を自動で有効にする

任意のアクセス方法を選択して、すべてのメンバーアカウントのために RDS Protection 機能を有効にします。これには、既存のメンバーアカウントと、組織に参加する新しいアカウントが含まれます。

Console

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。

2. 次のいずれかを行います。

   [RDS Protection] ページの使用

   1. ナビゲーションペインで、[RDS Protection] を選択します。
   2. [すべてのアカウントについて有効にする] を選択します。このアクションにより、組織内の既存のアカウントと新しいアカウントの両方について RDS Protection が自動的に有効になります。
   3. [保存] を選択します。

   > **Note**
   >
   > メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

   [アカウント] ページの使用

   1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
   2. [アカウント] ページで、[招待によるアカウントの追加] の前に [自動有効化] の詳細設定を選択します。
   3. [自動有効化の詳細設定を管理] ウィンドウで、[RDS ログインアクティビティモニタリング] の下の [すべてのアカウントについて有効にする] を選択します。
   4. [保存] を選択します。

   [すべてのアカウントについて有効にする] オプションを使用できない場合は、「メンバーアカウントを選択して RDS Protection を有効または無効にする」を参照してください。

API/CLI

- メンバーアカウントの RDS Protection を選択的に有効または無効にするには、ユーザー独自の*###### ID* を使用して updateMemberDetectors API オペレーションを起動します。
- 次の例では、単一のメンバーアカウントに RDS Protection を有効にする方法が示されます。無効にするには、ENABLED を DISABLED に置き換えます。

  アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

  > **Note**
  >
  > スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

すべての既存のアクティブなメンバーアカウントのために RDS Protection を有効にする

任意のアクセス方法を選択して、組織内のすべての既存のアクティブなメンバーアカウントのために RDS Protection を有効にします。

Console

すべての既存のアクティブなメンバーアカウントのために RDS Protection を設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任 GuardDuty 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[RDS Protection] を選択します。

3. [RDS Protection] ページでは、設定の現在のステータスを表示できます。[アクティブなメンバーアカウント] セクションで、[アクション] を選択します。
4. [アクション] ドロップダウンメニューから、[すべての既存のアクティブなメンバーアカウントについて有効にする] を選択します。
5. [確認] を選択します。

API/CLI

- メンバーアカウントの RDS Protection を選択的に有効または無効にするには、ユーザー独自の*###### ID* を使用して updateMemberDetectors API オペレーションを起動します。
- 次の例では、単一のメンバーアカウントに RDS Protection を有効にする方法が示されます。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

  > **Note**
  >
  > スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

新しいメンバーアカウントの RDS Protection を自動で有効にする

任意のアクセス方法を選択して、組織に参加する新しいアカウントに RDS ログインアクティビティを有効にします。

Console

委任 GuardDuty 管理者アカウントは、RDS Protection または Accounts ページを使用して、コンソールから組織内の新しいメンバーアカウントに対して を有効にできます。

新しいメンバーアカウントの RDS Protection を自動で有効にするには

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。

2. 次のいずれかを行います。

   - [RDS Protection] ページを使用する場合:

     1. ナビゲーションペインで、[RDS Protection] を選択します。
     2. [RDS Protection] ページで、[編集] を選択します。
     3. [アカウントを手動で設定] を選択します。
     4. [新しいメンバーアカウントについて自動的に有効にする] を選択します。このステップにより、新しいアカウントが組織に参加するたびに、そのアカウントのために RDS Protection が自動的に有効になります。この設定を変更できるのは、組織の委任 GuardDuty 管理者アカウントのみです。
     5. [保存] を選択します。

   - [Accounts] (アカウント) ページを使用する場合:

     1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
     2. [アカウント] ページで、[自動有効化] 設定を選択します。
     3. [自動有効化の詳細設定を管理] ウィンドウで、[RDS ログインアクティビティモニタリング] の下の [新しいアカウントについて有効にする] を選択します。
     4. [保存] を選択します。

API/CLI

- メンバーアカウントの RDS Protection を選択的に有効または無効にするには、ユーザー独自の`###### ID` を使用して UpdateOrganizationConfiguration API オペレーションを起動します。
- 次の例では、単一のメンバーアカウントに RDS Protection を有効にする方法が示されます。無効にするには、「メンバーアカウントを選択して RDS Protection を有効または無効にする」

を参照してください。組織に参加する新規アカウントすべてに対して有効にしたくない場合は、`autoEnable` を `NONE` に設定します。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

メンバーアカウントを選択して RDS Protection を有効または無効にする

任意のアクセス方法を選択して、メンバーアカウントのために RDS ログインアクティビティのモニタリングを選択的に有効または無効にします。

Console

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。

2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

   [アカウント] ページで、[RDS ログインアクティビティ] 列でメンバーアカウントのステータスを確認します。

3. RDS ログインアクティビティを選択的に有効または無効にするには

   RDS Protection を設定するアカウントを選択します。一度に複数のアカウントを選択できます。[保護プランの編集] ドロップダウンメニューで、[RDS ログインアクティビティ] を選択し、適切なオプションを選択します。

API/CLI

メンバーアカウントの RDS Protection を選択的に有効または無効にするには、ユーザー独自の`###### ID` を使用して updateMemberDetectors API オペレーションを起動します。

次の例では、単一のメンバーアカウントに RDS Protection を有効にする方法が示されます。無効にするには、`ENABLED` を `DISABLED` に置き換えます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

RDS Protection の機能

RDS ログインアクティビティのモニタリング

RDS ログインアクティビティは、 AWS 環境における サポートされている Amazon Aurora および Amazon RDS データベース へのログイン試行の成功と失敗の両方をキャプチャします。データベースを保護するために、 GuardDuty RDS Protection はログインアクティビティを継続的にモニタリングし、疑わしいログイン試行がないか調べます。例えば、攻撃者がデータベースのパスワードを推測して Amazon Aurora データベースへのブルートフォースアクセスを試みる可能性があります。

RDS Protection 機能を有効にすると、 はデータベースの RDS ログインアクティビティを Aurora サービスから直接 GuardDuty 自動的にモニタリングし始めます。異常なログイン動作の兆候がある場合、 は侵害された可能性のあるデータベースに関する詳細を含む検出結果 GuardDuty を生成しま

す。RDS Protection を初めて有効にする場合、またはデータベースインスタンスを新しく作成した場合は、通常の動作をベースラインにするための学習期間が必要です。このため、新たに有効になったデータベースインスタンスや新しく作成されたデータベースインスタンスでは、最長で 2 週間程度、関連する異常ログインが検出されないことがあります。

RDS Protection 機能では、追加のセットアップは必要ありません。既存の Amazon Aurora データベース設定には影響しません。サポートされているデータベースや RDS ログインアクティビティを管理 GuardDuty したり、RDS ログインアクティビティを利用したりすることはありません。

新しいメンバーアカウントが組織に加わるときに RDS Protection 機能を自動的に有効にすることを選択した場合、このアクションにより、それらの新しいメンバーアカウント GuardDuty に対して が自動的に有効になります。RDS ログインアクティビティのモニタリングを機能として設定する方法の詳細については、「での RDS Protection GuardDuty」を参照してください。

でのランタイムモニタリング GuardDuty

Runtime Monitoring は、オペレーティングシステムレベル、ネットワーク、ファイルイベントを監視および分析し、環境内の特定の AWS ワークロードで潜在的な脅威を検出するのに役立ちます。

GuardDuty は、Amazon Elastic Kubernetes Service (Amazon EKS) リソースのみをサポートする Runtime Monitoring を最初にリリースしました。ただし、Runtime Monitoring 機能を使用して、AWS Fargate Amazon Elastic Container Service (Amazon ECS) および Amazon Elastic Compute Cloud (Amazon EC2) リソースの脅威を検出できるようになりました。

このドキュメントおよび Runtime Monitoring に関連するその他のセクションでは、 はリソースタイプの用語 GuardDuty を使用して Amazon EKS、Fargate Amazon ECS、および Amazon EC2 リソースを参照します。

Runtime Monitoring は、ファイルアクセス、プロセス実行、コマンドライン引数、ネットワーク接続などのランタイム動作を可視化する GuardDuty セキュリティエージェントを使用します。潜在的な脅威をモニタリングするリソースタイプごとに、その特定のリソースタイプのセキュリティエージェントを自動または手動で管理できます (Fargate (Amazon ECS のみ) を除く) 。セキュリティエージェントの自動管理は、 がユーザーに代わってセキュリティエージェントをインストールおよび更新 GuardDuty することを許可することを意味します。一方、リソースのセキュリティエージェントを手動で管理する場合、必要に応じてセキュリティエージェントをインストールして更新する責任があります。

この拡張機能により、 GuardDuty は、個々のワークロードやインスタンスで実行されているアプリケーションやデータをターゲットとする可能性のある潜在的な脅威を特定して対応できます。例えば、脅威は、脆弱なウェブアプリケーションを実行している 1 つのコンテナを危険にさらすことから始まる可能性があります。このウェブアプリケーションには、基盤となるコンテナとワークロードへのアクセス権限が存在する可能性があります。この場合、認証情報が正しく設定されていないと、アカウントとその中に保存されているデータへのアクセスを制御できない可能性があります。

個々のコンテナとワークロードのランタイムイベントを分析することで、 GuardDuty は、コンテナおよび関連する AWS 認証情報の侵害を初期段階で特定し、特権、疑わしい API リクエスト、環境内のデータへの悪意のあるアクセスをエスカレートしようとする試みを検出できます。

内容

- Runtime Monitoring GuardDuty の有効化
- EKS Runtime Monitoring の設定 (API のみ)
- EKS Runtime Monitoring から Runtime Monitoring への移行
- リソースのランタイムカバレッジの評価
- CPU とメモリモニタリングの設定
- が GuardDuty 使用する収集済みランタイムイベントタイプ
- Amazon ECR リポジトリホスティング GuardDuty エージェント
- GuardDuty エージェントリリース履歴
- リソースの無効化とクリーンアップの影響

仕組み

Runtime Monitoring を使用するには、Runtime Monitoring を有効にしてから、 GuardDuty セキュリティエージェントを管理する必要があります。以下のリストでこの 2 つの手順を説明しています。

1. アカウントの Runtime Monitoring を有効にして、 が Amazon EC2 インスタンス、Amazon ECS クラスター、Amazon EKS ワークロードから受信したランタイムイベントを受け入れる GuardDuty ことができるようにします。
2. ランタイム動作をモニタリングする個々のリソースの GuardDuty エージェントを管理します。リソースタイプに基づいて、 GuardDuty セキュリティエージェントを手動でデプロイするか、自動エージェント設定と呼ばれる GuardDuty がユーザーに代わって管理できるようにするかを選択できます。

   GuardDuty は、各リソースタイプのセキュリティエージェントを認証するインスタンス ID ロールを使用して、関連するランタイムイベントを VPC エンドポイントに送信します。

> **Note**
>
> GuardDuty では、ランタイムイベントにアクセスすることはできません。

EC2 インスタンスの EKS Runtime Monitoring または Runtime Monitoring でセキュリティエージェントを (手動または を介して GuardDuty) 管理し、現在 Amazon EC2 インスタンスにデプロイされ、このインスタンス収集されたランタイムイベントタイプから を受け取った場合、 GuardDuty は

この Amazon EC2 インスタンスからの VPC フローログの分析 AWS アカウント に対して に課金 GuardDuty しません。これにより、アカウントの 2 倍の使用コスト GuardDuty を回避できます。

以下のトピックでは、Runtime Monitoring を有効にし、 GuardDuty セキュリティエージェントを管理する仕組みをリソースタイプごとに説明します。

内容

- Runtime Monitoring が Amazon EC2 インスタンスと連携する方法
- Runtime Monitoring と Fargate の連携方法 (Amazon ECS のみ)
- Runtime Monitoring が Amazon EKS クラスターと連携する方法
- EKS Runtime Monitoring 設定後

Runtime Monitoring が Amazon EC2 インスタンスと連携する方法

Amazon EC2 インスタンスは、 AWS 環境で複数のタイプのアプリケーションとワークロードを実行できます。Runtime Monitoring を有効にして GuardDuty セキュリティエージェントを管理すると、GuardDuty は既存の Amazon EC2 インスタンスと新しいインスタンスの脅威を検出するのに役立ちます。この機能は、Amazon ECS によって管理される Amazon EC2 インスタンスもサポートしています。

Runtime Monitoring を有効にすると、Amazon EC2 インスタンス内で現在実行中のプロセスと新しいプロセスからのランタイムイベントを消費する GuardDuty 準備が整います。EC2 インスタンスから にランタイムイベントを送信するには、セキュリティエージェント GuardDuty が必要です GuardDuty。

Amazon EC2 インスタンスの場合、 GuardDuty セキュリティエージェントはインスタンスレベルで動作します。アカウント内のすべての Amazon EC2 インスタンスまたは選択的な Amazon EC2 インスタンスをモニタリングするかどうかを決定できます。選択的インスタンスを管理する場合、セキュリティエージェントはこれらのインスタンスにのみ必要です。

GuardDuty は、Amazon ECS クラスター内の Amazon EC2 インスタンスで実行されている新しいタスクと既存のタスクからのランタイムイベントを使用することもできます。

GuardDuty セキュリティエージェントをインストールするには、Runtime Monitoring に次の 2 つのオプションがあります。

- 自動エージェント設定を使用する (推奨)、または
- セキュリティエージェントの手動管理

を使用して自動エージェント設定を使用する GuardDuty （ 推奨 ）

ユーザーに代わって が Amazon EC2 インスタンスにセキュリティエージェントをインストール GuardDuty することを許可する自動エージェント設定を使用します。 はセキュリティエージェントの更新 GuardDuty も管理します。

デフォルトでは、 GuardDuty はアカウント内のすべてのインスタンスにセキュリティエージェントをインストールします。選択した EC2 インスタンスのみのセキュリティエージェントをインストールおよび管理 GuardDuty する場合は、必要に応じて EC2 インスタンスに包含タグまたは除外タグを追加します。

アカウントに属するすべての Amazon EC2 インスタンスのランタイムイベントをモニタリングしたくない場合があります。限られた数のインスタンスのランタイムイベントをモニタリングする場合は、選択したインスタンスに包含タグを `GuardDutyManaged：true` として追加します。Amazon EC2 の自動エージェント設定の可用性以降、EC2 インスタンスに包含タグ (`GuardDutyManaged：true`） GuardDuty がある場合、自動エージェント設定を明示的に有効にしない場合でも、 はタグを尊重し、選択したインスタンスのセキュリティエージェントを管理します。

一方、ランタイムイベントをモニタリングしたくない EC2 インスタンスの数が制限されている場合は、選択したインスタンスに除外タグ (`GuardDutyManaged：false`) を追加します。 GuardDuty は、これらの EC2 リソースのセキュリティエージェントをインストールも管理もしないことで、除外タグを尊重します。

Impact

または組織で AWS アカウント 自動エージェント設定を使用する場合、 GuardDuty がユーザーに代わって次の手順を実行することを許可します。

- GuardDuty は、SSM が管理し、https://console.aws.amazon.com/systems-manager/ コンソールの Fleet Manager の下に表示されるすべての Amazon EC2 インスタンスに対して 1 つの SSM 関連付けを作成します。
- 自動エージェント設定を無効にして包含タグを使用する – Runtime Monitoring を有効にした後、自動エージェント設定を有効にせずに Amazon EC2 インスタンスに包含タグを追加すると、ユーザーに代わってセキュリティエージェントの管理 GuardDuty が許可されることを意味します。その後、SSM の関連付けは、包含タグ (`GuardDutyManaged：true`) を持つ各インスタンスにセキュリティエージェントをインストールします。
- 自動エージェント設定を有効にすると、SSM の関連付けによって、アカウントに属するすべての EC2 インスタンスにセキュリティエージェントがインストールされます。

- 自動エージェント設定で除外タグを使用する – 自動エージェント設定を有効にする前に、Amazon EC2 インスタンスに除外タグを追加すると、選択したインスタンスのセキュリティエージェントのインストールと管理を禁止することを GuardDuty に許可していることになります。

  これで、自動エージェント設定を有効にすると、SSM 関連付けは、除外タグでタグ付けされたインスタンスを除くすべての EC2 インスタンスにセキュリティエージェントをインストールおよび管理します。

- GuardDuty は、終了またはシャットダウンされたインスタンス状態にない Linux EC2 インスタンスが VPCs に少なくとも 1 VPCs を含むすべての VPC に VPC エンドポイントを作成します。さまざまなインスタンス状態の詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスのライフサイクル」を参照してください。 Amazon EC2

  GuardDuty は もサポートしています自動セキュリティエージェントで共有 VPC を使用する。組織と のすべての前提条件が考慮されると AWS アカウント、 GuardDuty は共有 VPC を使用してランタイムイベントを受信します。

  > **Note**
  >
  > VPC エンドポイントの使用に追加料金はかかりません。

セキュリティエージェントの手動管理

Amazon EC2 のセキュリティエージェントを手動で管理するには、次の 2 つの方法があります。

- で GuardDuty マネージドドキュメント AWS Systems Manager を使用して、すでに SSM 管理されている Amazon EC2 インスタンスにセキュリティエージェントをインストールします。

  新しい Amazon EC2 インスタンスを起動するたびに、SSM が有効になっていることを確認します。

- RPM パッケージマネージャー (RPM) スクリプトを使用して、SSM で管理されているかどうかにかかわらず、Amazon EC2 インスタンスにセキュリティエージェントをインストールします。

次のステップ

Amazon EC2 インスタンスをモニタリングするための Runtime Monitoring 設定を開始するには、「」を参照してくださいAmazon EC2 インスタンスサポートの前提条件。

Runtime Monitoring と Fargate の連携方法 (Amazon ECS のみ)

Runtime Monitoring を有効にすると、 はタスクのランタイムイベントを使用する準備が整 GuardDuty います。これらのタスクは Amazon ECS クラスター内で実行され、 AWS Fargate (Fargate) インスタンスで実行されます。 GuardDuty がこれらのランタイムイベントを受信するには、フルマネージド型の専用セキュリティエージェントを使用する必要があります。

現在、Runtime Monitoring は、 を介してのみ Amazon ECS クラスター (AWS Fargate) のセキュリティエージェントの管理をサポートしています GuardDuty。Amazon ECS クラスターでのセキュリティエージェントの手動管理はサポートされていません。

AWS アカウントまたは組織の自動エージェント設定を使用して、 GuardDuty がユーザーに代わって GuardDuty セキュリティエージェントを管理できます。 GuardDuty は、Amazon ECS クラスターで起動される新しい Fargate タスクにセキュリティエージェントのデプロイを開始します。次のリストは、 GuardDuty セキュリティエージェントを有効にするときに想定される内容を示しています。

GuardDuty セキュリティエージェントの有効化による影響

GuardDuty Virtual Private Cloud (VPC) エンドポイントを作成する

GuardDuty セキュリティエージェントをデプロイすると、 GuardDuty は、セキュリティエージェントがランタイムイベントを に配信する VPC エンドポイントを作成します GuardDuty。

> **Note**
>
> VPC エンドポイントの使用に追加料金はかかりません。

GuardDuty でサイドカーコンテナを追加

実行を開始する新しい Fargate タスクまたはサービスの場合、 GuardDuty コンテナ (サイドカー) は Amazon ECS Fargate タスク内の各コンテナにそれ自体をアタッチします。 GuardDuty セキュリティエージェントは、アタッチされた GuardDuty コンテナ内で実行されます。これにより GuardDuty 、これらのタスク内で実行されている各コンテナのランタイムイベントを収集できます。

Fargate タスクを開始するときに、 GuardDuty コンテナ (サイドカー) が正常な状態で起動できない場合、Runtime Monitoring はタスクの実行を妨げないように設計されています。

デフォルトでは、Fargate タスクはイミュータブルです。タスクがすでに実行状態にある場合、はサイドカーをデプロイ GuardDuty しません。すでに実行中のタスクでコンテナをモニタリングする場合は、タスクを停止して再度開始できます。

Runtime Monitoring が Amazon EKS クラスターと連携する方法

Runtime Monitoring は、 GuardDuty セキュリティエージェントとも呼ばれる EKS アドオン aws-guardduty-agentを使用します。セキュリティエージェントが EKS GuardDutyクラスターにデプロイされると、 GuardDuty はこれらの EKS クラスターのランタイムイベントを受信できます。

この機能は、Amazon EKS クラスターのランタイムイベントをアカウントレベルまたはクラスターレベルで監視できます。セキュリティ GuardDuty エージェントは、脅威の検出をモニタリングする Amazon EKS クラスターに対してのみ管理できます。 GuardDuty セキュリティエージェントは、手動で管理することも、自動エージェント設定を使用してユーザーに代わって GuardDuty が管理できるようにすることもできます。

自動エージェント設定アプローチを使用して、 GuardDuty がユーザーに代わってセキュリティエージェントのデプロイを管理できるようにすると、Amazon Virtual Private Cloud (Amazon VPC) エンドポイント が自動的に作成されます。セキュリティエージェントは、この Amazon VPC エンドポイントを使用してランタイムイベント GuardDuty を に配信します。

> **Note**
>
> VPC エンドポイントの使用に追加料金はかかりません。

現在、 は Amazon EC2 instances.does で実行されている Amazon EKS クラスター GuardDuty をサポートしています。 では、 で実行されている Amazon EKS クラスターはサポートされていません AWS Fargate。 GuardDuty

EKS Runtime Monitoring 設定後

「ランタイムカバレッジの評価」

Runtime Monitoring を有効にして GuardDuty セキュリティエージェントをデプロイしたら、セキュリティエージェントをデプロイしたリソースのカバレッジステータスを継続的に [1] 評価することをお勧めします。カバレッジステータスは「正常」または「異常」の場合があります。Healthy カバレッジステータス GuardDuty は、オペレーティングシステムレベルのアクティ

ビティがある場合、 が対応するリソースからランタイムイベントを受信していることを示します。

リソースのカバレッジステータスが正常になると、 GuardDuty はランタイムイベントを受信し、脅威検出のために分析できます。がコンテナワークロードとインスタンスで実行されているタスクまたはアプリケーションで潜在的なセキュリティ脅威 GuardDuty を検出すると、 は 1 つ以上の Runtime Monitoring 検出結果タイプ GuardDuty を生成します。

[1] また、カバレッジステータスが異常から正常に変わったときに通知を受け取るように Amazon EventBridge （ EventBridge) を設定することもできます。

詳細については、「リソースのランタイムカバレッジの評価」を参照してください。

GuardDuty が潜在的な脅威を検出する

GuardDuty がリソースのランタイムイベントを受信し始めると、それらのイベントの分析が開始されます。が Amazon EC2 インスタンス、Amazon ECS クラスター、または Amazon EKS クラスターのいずれかで潜在的なセキュリティ脅威 GuardDuty を検出すると、1 つ以上の が生成されますRuntime Monitoring の検出結果タイプ。検出の詳細にアクセスして、影響を受けたリソースの詳細を表示できます。

Runtime Monitoring の 30 日間の無料トライアルの仕組み

30 日間の無料トライアル期間は、Runtime Monitoring 機能が Amazon EC2 インスタンスおよび AWS Fargate (Amazon ECS のみ) に拡張される前に EKS Runtime Monitoring を既に有効にしている新しい GuardDuty アカウントと既存のアカウントでは、動作が異なります。

GuardDuty トライアル期間を使用しているか、EKS Runtime Monitoring を有効にしたことがない

次のリストでは、30 日間の無料トライアル期間を使用している場合、または EKS Runtime Monitoring を有効にしたことがない場合の GuardDuty 30 日間の無料トライアル期間の仕組みについて説明します。

- GuardDuty を初めて有効にすると、Runtime Monitoring と EKS Runtime Monitoring はデフォルトでは有効になっていません。

  アカウントまたは組織の Runtime Monitoring を有効にする場合は、脅威検出をモニタリングするリソース GuardDuty のセキュリティエージェントも設定してください。例えば、Amazon EC2 インスタンスに Runtime Monitoring を使用する場合は、Runtime Monitoring を有効にした

後、Amazon EC2 のセキュリティエージェントも設定する必要があります。これは、手動または を使用して自動的に実行できます GuardDuty。

- Runtime Monitoring 保護プランは、アカウントレベル で有効になっています。30 日間の無料トライアル期間は、リソースレベル で機能します。 GuardDuty セキュリティエージェントが特定のリソースタイプにデプロイされると、 がこのリソースタイプに関連付けられた最初のランタイムイベント GuardDuty を受信すると、30 日間の無料トライアルが開始されます。例えば、 GuardDuty エージェントをリソースレベル (Amazon EC2 インスタンス、Amazon ECS クラスター、Amazon EKS クラスターの場合) にデプロイしたとします。が Amazon EC2 インスタンスの最初のランタイムイベント GuardDuty を受信すると、Amazon EC2 に対してのみ 30 日間の無料トライアルが開始されます。
- EKS Runtime Monitoring のみを有効にする場合 – GuardDuty を初めて有効にすると、EKS Runtime Monitoring はデフォルトでは有効になっていません (Runtime Monitoring のリリース後) 。EKS Runtime Monitoring を有効にする必要があります。最適に使用するには、 GuardDuty セキュリティエージェントを手動で管理するか、自動エージェント設定を有効にして、 がユーザーに代わってエージェント GuardDuty を管理するようにします。EKS Runtime Monitoring の 30 日間の無料トライアル期間は、 が Amazon EKS リソースの最初のランタイムイベント GuardDuty を受信したときに開始されます。

Runtime Monitoring を開始する前に EKS Runtime Monitoring を有効にしました

- EKS Runtime Monitoring 保護プランが有効で、 GuardDuty コンソールエクスペリエンスを使用してこの保護プランを使用する既存の GuardDuty アカウントの場合 – Runtime Monitoring の発表により、EKS Runtime Monitoring コンソールエクスペリエンスが Runtime Monitoring に統合されました。EKS Runtime Monitoring の既存の設定は変わりません。API/CLI サポートを引き続き使用して、EKS Runtime Monitoring に関連するオペレーションを実行できます。
- EKS Runtime Monitoring を Runtime Monitoring の一部として使用するには、アカウントまたは組織の Runtime Monitoring を設定する必要があります。Runtime Monitoring の同じ設定を維持するには、「」を参照してくださいEKS Runtime Monitoring から Runtime Monitoring への移行。ただし、Amazon EKS リソースの 30 日間の無料トライアルには影響しません。
- Runtime Monitoring 保護プランは、リージョンごとのアカウントレベルで有効になっています。GuardDuty セキュリティエージェントが指定されたリソースタイプ (Amazon EC2 インスタンスと Amazon ECS クラスター) のいずれかにデプロイされると、 がリソースに関連付けられた最初のランタイムイベント GuardDuty を受信すると、30 日間の無料トライアルが開始されます。各リソースタイプには 30 日間の無料トライアルがあります。

例えば、Runtime Monitoring を有効にした後、Amazon EC2 インスタンスにのみ GuardDuty エージェントをデプロイすることを選択すると、このリソースの 30 日間の無料トライアルは、 が Amazon EC2 インスタンスの最初のランタイムイベント GuardDuty を受信したときにのみ開始されます。後で、Fargate (Amazon ECS のみ) の GuardDuty エージェントをデプロイすると、このリソースの 30 日間の無料トライアルは、 が Amazon ECS クラスターの最初のランタイムイベントを受信したときに GuardDutyのみ開始されます。アカウントに既に EKS Runtime Monitoring が有効になっていることを考慮すると、Amazon EKS GuardDuty リソースの 30 日間の無料トライアルをリセットしないでください。

主な概念 - GuardDuty セキュリティエージェントを管理するためのアプローチ

Amazon EKS クラスターと Amazon ECS クラスターのセキュリティエージェントの管理に役立つ主要な概念を検討してください。

内容

Fargate (Amazon ECS のみ) リソース - GuardDuty セキュリティエージェントを管理するためのアプローチ

Runtime Monitoring では、アカウント内のすべての Amazon ECS クラスター (アカウントレベル) または選択的クラスター (クラスターレベル) のいずれかで潜在的なセキュリティ脅威を検出できます。実行される各 Amazon ECS Fargate タスクの自動エージェント設定を有効にすると、 GuardDuty はそのタスク内の各コンテナワークロードにサイドカーコンテナを追加します。GuardDuty セキュリティエージェントがこのサイドカーコンテナにデプロイされます。これは、 が Amazon ECS タスク内のコンテナのランタイム動作を GuardDuty 可視化する方法です。

現在、Runtime Monitoring は、 を介してのみ Amazon ECS クラスター (AWS Fargate) のセキュリティエージェントの管理をサポートしています GuardDuty。Amazon ECS クラスターでのセキュリティエージェントの手動管理はサポートされていません。

アカウントを設定する前に、 GuardDuty セキュリティエージェントをどのように管理するかを評価し、Amazon ECS タスクに属するコンテナのランタイム動作をモニタリングする可能性があります。次のアプローチを参考にしてください。

トピック

- すべての Amazon ECS クラスター GuardDuty のセキュリティエージェントを管理する
- ほとんどの Amazon ECS クラスターのセキュリティエージェントを管理します GuardDuty が、一部の Amazon ECS クラスターは除外します。
- 選択的な Amazon ECS クラスターのセキュリティエージェントの管理 GuardDuty

すべての Amazon ECS クラスター GuardDuty のセキュリティエージェントを管理する

このアプローチは、潜在的なセキュリティ脅威をアカウントレベルで検出するのに役立ちます。このアプローチは GuardDuty 、アカウントに属するすべての Amazon ECS クラスターに対する潜在的なセキュリティ脅威を検出する場合に使用します。

ほとんどの Amazon ECS クラスターのセキュリティエージェントを管理します GuardDuty が、一部の Amazon ECS クラスターは除外します。

このアプローチは GuardDuty 、 AWS 環境内のほとんどの Amazon ECS クラスターの潜在的なセキュリティ脅威を検出し、一部のクラスターを除外する場合に使用します。このアプローチは、Amazon ECS タスク内のコンテナの実行時の動作をクラスターレベルで監視するのに役立ちます。例えば、アカウントに属する Amazon ECS クラスターの数は 1000 個です。ただし、監視したい Amazon ECS クラスターは 930 個だけです。

このアプローチでは、モニタリングしない Amazon ECS クラスターに事前定義された GuardDuty タグを追加する必要があります。詳細については、「Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ) 」を参照してください。

選択的な Amazon ECS クラスターのセキュリティエージェントの管理 GuardDuty

このアプローチは GuardDuty 、一部の Amazon ECS クラスターで潜在的なセキュリティ脅威を検出する場合に使用します。このアプローチは、Amazon ECS タスク内のコンテナの実行時の動作をクラスターレベルで監視するのに役立ちます。例えば、アカウントに属する Amazon ECS クラスターの数は 1000 個です。ただし、監視したいクラスターは 230 個だけです。

このアプローチでは、モニタリングする Amazon ECS クラスターに事前定義された GuardDuty タグを追加する必要があります。詳細については、「Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)」を参照してください。

Amazon EKS クラスター - GuardDuty セキュリティエージェントを管理するためのアプローチ

GuardDuty アカウントレベルまたはクラスターレベルで EKS クラスターからのランタイムイベントを使用するには、対応するクラスター GuardDuty のセキュリティエージェントを管理する必要があります。

セキュリティエージェントを管理する GuardDutyためのアプローチ

2023 年 9 月 13 日より前は、 を設定 GuardDuty してセキュリティエージェントをアカウントレベルで管理できます。この動作は、デフォルトで が に属するすべての EKS クラスターのセキュリティエージェント GuardDuty を管理することを示しています AWS アカウント。では、セキュリティエージェント GuardDuty を管理する EKS クラスターの選択に役立つきめ細かい機能 GuardDuty が提供されます。

「 GuardDuty セキュリティエージェントの手動管理」を選択した場合も、モニタリングする EKS クラスターを選択できます。ただし、エージェントを手動で管理するには、 AWS アカウント 用の Amazon VPC エンドポイントを作成することが前提条件になります。

> **Note**
>
> GuardDuty セキュリティエージェントの管理に使用するアプローチに関係なく、EKS Runtime Monitoring は常にアカウントレベルで有効になります。

トピック

- によるセキュリティエージェントの管理 GuardDuty
- GuardDuty セキュリティエージェントの手動管理

によるセキュリティエージェントの管理 GuardDuty

GuardDuty は、ユーザーに代わってセキュリティエージェントをデプロイおよび管理します。次のいずれかのアプローチを使用して、アカウント内の EKS クラスターをいつでもモニタリングできます。

トピック

すべての EKS クラスターのモニタリング

- このアプローチを使用するタイミング — アカウント内のすべての EKS クラスターのセキュリティエージェントを GuardDuty デプロイおよび管理する場合は、このアプローチを使用します。デフォルトでは、 GuardDuty はアカウントで作成された新しい EKS クラスターにセキュリティエージェントをデプロイします。
- このアプローチを使用した場合の影響:
  - GuardDuty は、 GuardDuty セキュリティエージェントがランタイムイベントを に配信する Amazon Virtual Private Cloud (Amazon VPC) エンドポイントを作成します GuardDuty。を通じてセキュリティエージェントを管理する場合、Amazon VPC エンドポイントの作成に追加コストはかかりません GuardDuty。
  - ワーカーノードには、アクティブな `guardduty-data` VPC エンドポイントへの有効なネットワークパスが必要です。 は、EKS クラスターにセキュリティエージェントを GuardDuty デプロイします。Amazon Elastic Kubernetes Service (Amazon EKS) が、EKS クラスター内のノードでのセキュリティエージェントのデプロイを調整します。
  - IP 可用性に基づいて、 は VPC エンドポイントを作成するサブネット GuardDuty を選択します。高度なネットワークトポロジを使用する場合は、接続が可能であることを検証する必要があります。
- 考慮事項 — 現在、このオプションを使用する場合、EKS Runtime Monitoring は共有 VPC を作成しません。

すべての EKS クラスターのモニタリングと選択的な EKS クラスターの除外

- このアプローチを使用するタイミング — アカウント内のすべての EKS クラスターのセキュリティエージェント GuardDuty を管理するが、選択的な EKS クラスターを除外する場合は、このアプローチを使用します。この方法では、ランタイムイベントを受信しない EKS クラスターにタグを付けることができる、タグベース[1]のアプローチを使用します。事前定義されたタグには、キーと値のペアとして `GuardDutyManaged-false` が必要です。
- このアプローチを使用した場合の影響:

- このアプローチでは、モニタリングから除外する EKS クラスターにタグを追加した後にのみ、GuardDuty エージェントの自動管理を有効にする必要があります。

  そのため、「によるセキュリティエージェントの管理 GuardDuty」の場合の影響がこのアプローチにも適用されます。 GuardDuty エージェントの自動管理を有効にする前にタグを追加すると、 はモニタリングから除外された EKS クラスターのセキュリティエージェントをデプロイも管理も GuardDuty しません。

- 考慮事項:
  - 自動エージェント設定を有効にする前に、選択的な EKS クラスターのタグキーと値のペアを `GuardDutyManaged`として`false`追加する必要があります。追加しないと、タグを使用するまで GuardDuty セキュリティエージェントがすべての EKS クラスターにデプロイされます。
  - 信頼できる ID 以外により、タグが変更されないようにする必要があります。

    > **Important**
    >
    > サービスコントロールポリシーまたは IAM ポリシーを使用して、EKS クラスターの `GuardDutyManaged` タグの値を変更する権限を管理します。詳細については、「 AWS Organizations ユーザーガイド」のSCPs)」または「IAM ユーザーガイド」の「 AWS リソースへのアクセスの制御」を参照してください。

  - モニタリングする必要のない、潜在的な新しい EKS クラスターについては、その EKS クラスターの作成時に必ず `GuardDutyManaged-false` のキーと値のペアを追加してください。
  - このアプローチには、「すべての EKS クラスターのモニタリング」で指定されているものと同じ考慮事項があります。

選択的な EKS クラスターのモニタリング

- このアプローチを使用するタイミング — アカウント内の選択的な EKS クラスターに対してのみ、セキュリティエージェントに更新を GuardDuty デプロイおよび管理する場合は、このアプローチを使用します。この方法では、ランタイムイベントを受信する EKS クラスターにタグを付けることができる、タグベース[1]のアプローチを使用します。
- このアプローチを使用した場合の影響:
  - 包含タグを使用すると、 は、キーと値のペアとして `GuardDutyManaged-true` でタグ付けされた選択的な EKS クラスターに対してのみ、セキュリティエージェント GuardDuty を自動的にデプロイおよび管理します。

  - このアプローチを使用した場合も、「すべての EKS クラスターのモニタリング」で指定されているものと同じ影響があります。
- 考慮事項:
  - `GuardDutyManaged` タグの値が `true` に設定されていないと、包含タグが期待どおりに機能せず、EKS クラスターのモニタリングに影響する可能性があります。
  - 選択的な EKS クラスターを確実にモニタリングするには、信頼できる ID 以外によりタグが変更されないようにする必要があります。

    > **Important**
    >
    > サービスコントロールポリシーまたは IAM ポリシーを使用して、EKS クラスターの `GuardDutyManaged` タグの値を変更する権限を管理します。詳細については、「 AWS Organizations ユーザーガイド」のSCPs)」または「IAM ユーザーガイド」の「 AWS リソースへのアクセスの制御」を参照してください。

  - モニタリングする必要のない、潜在的な新しい EKS クラスターについては、その EKS クラスターの作成時に必ず `GuardDutyManaged-false` のキーと値のペアを追加してください。
  - このアプローチには、「すべての EKS クラスターのモニタリング」で指定されているものと同じ考慮事項があります。

[1]選択的な EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS リソースのタグ付け」を参照してください。

GuardDuty セキュリティエージェントの手動管理

- このアプローチを使用するタイミング — このアプローチは、すべての EKS クラスターで GuardDuty セキュリティエージェントを手動でデプロイおよび管理する場合に使用します。アカウントで EKS Runtime Monitoring が有効になっていることを確認してください。EKS Runtime Monitoring GuardDutyを有効にしないと、セキュリティエージェントが期待どおりに動作しない可能性があります。
- このアプローチの使用による影響 – すべてのアカウントおよびこの機能 AWS リージョン が利用可能な EKS クラスター内の GuardDuty セキュリティエージェントソフトウェアのデプロイを調整する必要があります。
- 考慮事項 – 新しいクラスターやワークロードが継続的にデプロイされるにつれて、カバレッジのギャップをモニタリングして対処しながら、安全なデータフローをサポートする必要があります。

Runtime Monitoring GuardDuty の有効化

アカウントで Runtime Monitoring を有効にする前に、ランタイムイベントを監視したいリソースタイプがプラットフォームの要件を満たしていることを確認してください。詳細については、「前提条件」を参照してください。

Runtime Monitoring の開始前に EKS Runtime Monitoring を使用していた場合は、API を使用して EKS Runtime Monitoring の既存の設定を確認して更新できます。既存の設定を EKS Runtime Monitoring から Runtime Monitoring に移行することもできます。詳細については、「EKS Runtime Monitoring から Runtime Monitoring への移行」を参照してください。

> **Note**
>
> 現在、このドキュメントでは、アカウントと組織の Runtime Monitoring をコンソールでのみ有効にする手順を説明しています。API アクションまたは AWS CLI の GuardDutyを使用してランタイムモニタリングを有効にすることもできます。

Runtime Monitoring は、以下のトピックの手順を使用して設定できます。

内容

- Runtime Monitoring を有効にする前提条件
- スタンドアロンアカウントの Runtime Monitoring の有効化
- マルチアカウント環境の Runtime Monitoring の有効化
- GuardDuty セキュリティエージェントの管理

Runtime Monitoring を有効にする前提条件

Runtime Monitoring を有効にして GuardDuty セキュリティエージェントを管理するには、脅威検出をモニタリングする各リソースタイプの前提条件を満たす必要があります。

内容

- Amazon EC2 インスタンスサポートの前提条件
- AWS Fargate (Amazon ECS のみ) サポートの前提条件
- Amazon EKS クラスターサポートの前提条件

Amazon EC2 インスタンスサポートの前提条件

EC2 インスタンスを SSM 管理にする

ランタイムイベントを GuardDuty モニタリングする Amazon EC2 インスタンスは AWS Systems Manager 、 (SSM) 管理されている必要があります。これは、 GuardDuty を使用してセキュリティエージェントを自動的に管理するか、手動で管理するか (を除く方法 2 - Linux パッケージマネージャーを使用する) には関係ありません。

で Amazon EC2 インスタンスを管理するには AWS Systems Manager、「 ユーザーガイド」の Amazon EC2 インスタンス用の Systems Manager のセットアップAWS Systems Manager 」を参照してください。

アーキテクチャ要件の検証

OS ディストリビューションのアーキテクチャは、 GuardDuty セキュリティエージェントの動作に影響を与える可能性があります。Amazon EC2 インスタンスに Runtime Monitoring を使用する前に、次の要件を満たす必要があります。

- 次の表は、Amazon EC2 インスタンス GuardDuty のセキュリティエージェントをサポートすることが検証された OS ディストリビューションを示しています。

OS ディストリビューション	カーネルバージョン	カーネルサポート	CPU アーキテクチャ	
			x64 (AMD64)	Graviton (ARM64)
• AL2 と AL2023 • Ubuntu 20.04 および Ubuntu 22.04 • Debian 11 と Debian 12	5.4、5.10、5.15、6.1、6.5、6.8	eBPF、Tracepoints、Kprobe	サポート	サポート

- 追加要件 - Amazon ECS/Amazon EC2 をお持ちの場合のみ

  Amazon ECS/Amazon EC2 については、Amazon ECS に最適化された最新の AMI (2023 年 9 月 29 日以降) を使用するか、Amazon ECS エージェントバージョン v1.77.0 を使用することをお勧めします。

組織のサービスコントロールポリシーの検証

組織内のアクセス許可を管理するためのサービスコントロールポリシー (SCP) を設定している場合は、ポリシーがアクセス許可 を拒否していないことを確認してくださいいguardduty:SendSecurityTelemetry。では GuardDuty 、さまざまなリソースタイプでランタイムモニタリングをサポートする必要があります。

メンバーアカウントの場合は、関連する委任管理者に接続します。組織の SCPs「サービスコントロールポリシー (SCPs」を参照してください。

自動エージェント設定を使用する場合

には自動エージェント設定を使用する (推奨)、 が以下の前提条件を満たす AWS アカウント 必要があります。

- 自動エージェント設定で包含タグを使用する場合、 が新しいインスタンスの SSM 関連付け GuardDuty を作成するときは、新しいインスタンスが SSM 管理され、https://console.aws.amazon.com/systems-manager/ コンソールの Fleet Manager に表示されます。
- 自動エージェント設定で除外タグを使用する場合：
  - アカウントの GuardDuty 自動エージェントを設定する前に、GuardDutyManaged：false タグを追加します。

    Amazon EC2 インスタンスを起動する前に、必ず除外タグを追加してください。Amazon EC2 の自動エージェント設定を有効にすると、除外タグなしで起動する EC2 インスタンスは、GuardDuty 自動エージェント設定の対象となります。
  - 除外タグを機能させるには、インスタンス ID ドキュメントがインスタンスメタデータサービス (IMDS) で使用できるようにインスタンス設定を更新します。このステップを実行する手順は、既に アカウントの Runtime Monitoring の有効化 の一部です。

GuardDuty エージェントの CPU とメモリの制限

CPU 制限

Amazon EC2 インスタンスに関連付けられた GuardDuty セキュリティエージェントの CPU 上限は、vCPU コアの合計の 10% です。例えば、EC2 インスタンスに 4 つの vCPU コアがある場合、セキュリティエージェントは使用可能な合計 400% のうち最大 40% を使用できます。

メモリ制限

Amazon EC2 インスタンスに関連付けられたメモリから、 GuardDuty セキュリティエージェントが使用できるメモリは限られています。

次の表にメモリ制限を示します。

Amazon EC2 インスタンスのメモリ	GuardDuty エージェントの最大メモリ
8 GB 未満	128 MB
32 GB 未満	256 MB
32 GB 以上	1 GB

次のステップ

次のステップでは、Runtime Monitoring を設定し、セキュリティエージェントも (自動または手動で) 管理します。

AWS Fargate (Amazon ECS のみ) サポートの前提条件

アーキテクチャ要件の検証

使用するプラットフォームは、 GuardDuty セキュリティエージェントが Amazon ECS GuardDuty クラスターからランタイムイベントを受信する際に をサポートする方法に影響を与える可能性があります。検証済みのプラットフォームのいずれかを使用していることを検証する必要があります。

最初の検討事項:

Amazon ECS クラスターの AWS Fargate (Fargate) プラットフォームは Linux である必要があります。対応するプラットフォームバージョンは少なくとも `1.4.0` または `LATEST` である必要があります。有効なプラットフォームバージョンの詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「Linux プラットフォームのバージョン」を参照してください。

Windows プラットフォームバージョンはまだサポートされていません。

検証済みプラットフォーム

OS ディストリビューションと CPU アーキテクチャは、セキュリティエージェントが提供するサポートに影響します GuardDuty。次の表は、セキュリティエージェントのデプロイ GuardDutyと Runtime Monitoring の設定の検証済み設定を示しています。

OS ディストリビューション	カーネルサポート	CPU アーキテクチャ	
		x64 (AMD64)	Graviton (ARM64)
Linux	eBPF、Tracepoints、Kprobe	サポート	サポート

ECR アクセス許可とサブネットの詳細を指定する

Runtime Monitoring を有効にする前に、次の詳細を指定する必要があります。

アクセス許可を持つタスク実行ロールを提供する

タスク実行ロールには、特定の Amazon Elastic Container Registry (Amazon ECR) アクセス許可が必要です。AmazonECSTaskExecutionRolePolicy 管理ポリシーを使用するか、次のアクセス許可をTaskExecutionRoleポリシーに追加できます。

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Amazon ECR のアクセス許可をさらに制限するには、 GuardDuty セキュリティエージェントをホストする Amazon ECR リポジトリ URI を追加します AWS Fargate (Amazon ECS のみ）。詳細については、「での GuardDuty エージェントのリポジトリ AWS Fargate (Amazon ECS のみ）」を参照してください。

「タスク定義にサブネットの詳細を指定する」

タスク定義の入力としてパブリックサブネットを指定するか、Amazon ECR VPC エンドポイントを作成できます。

- タスク定義オプションの使用 — Amazon Elastic Container Service UpdateService APIs リファレンスの CreateServiceおよび API を実行するには、サブネット情報を渡す必要があります。詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS タスク定義」を参照してください。
- Amazon ECR VPC エンドポイントオプションの使用 - Amazon ECR へのネットワークパスを提供する - GuardDuty セキュリティエージェントをホストする Amazon ECR リポジトリ URI がネットワークにアクセスできることを確認します。Fargate タスクがプライベートサブネットで実行される場合、Fargate は GuardDuty コンテナをダウンロードするためのネットワークパスを必要とします。

  Fargate が GuardDuty コンテナをダウンロードできるようにする方法については、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS での Amazon ECR の使用」を参照してください。

組織のサービスコントロールポリシーの検証

組織内のアクセス許可を管理するためのサービスコントロールポリシー (SCP) を設定している場合は、ポリシーがアクセス許可 を拒否していないことを確認してくださいguardduty:SendSecurityTelemetry。では GuardDuty 、さまざまなリソースタイプでランタイムモニタリングをサポートする必要があります。

メンバーアカウントの場合は、関連する委任管理者に接続します。組織の SCPs「サービスコントロールポリシー (SCPs」を参照してください。

CPU とメモリの制限

Fargate タスク定義では、CPU 値とメモリの値をタスクレベルで指定する必要があります。次の表は、タスクレベルの CPU 値とメモリ値の有効な組み合わせと、 GuardDuty コンテナに対応する GuardDuty セキュリティエージェントの最大メモリ制限を示しています。

CPU の値	メモリの値	GuardDuty エージェントの最大メモリ制限
256 (.25 vCPU)	512 MiB、1 GB、2 GB	128 MB
512 (.5 vCPU)	1 GB、2 GB、3 GB、4 GB	
1,024 (1 vCPU)	2 GB、3 GB、4 GB	

CPU の値	メモリの値	GuardDuty エージェントの最大メモリ制限
	5 GB、6 GB、7 GB、8 GB	
2,048 (2 vCPU)	4 GB ~ 16 GB (1 GB のインクリメント)	
4,096 (4 vCPU)	8 GB ~ 20 GB (1 GB のインクリメント)	
8192 (8 vCPU)	16 GB ~ 28 GB (4 GB のインクリメント)	256 MB
	32 GB ~ 60 GB (4 GB のインクリメント)	512 MB
16384 (16 vCPU)	32 GB ~ 120 GB (8 GB のインクリメント)	1 GB

Runtime Monitoring を有効にして、クラスターのカバレッジステータスが [正常] と評価されると、コンテナインサイトメトリクスを設定および表示できます。詳細については、「Amazon ECS クラスターでの監視設定」。

次のステップでは、Runtime Monitoring を設定し、セキュリティエージェントを設定します。

Amazon EKS クラスターサポートの前提条件

アーキテクチャ要件の検証

使用するプラットフォームは、 GuardDuty セキュリティエージェントが EKS クラスターからランタイムイベント GuardDuty を受信する際に をサポートする方法に影響を与える可能性があります。検証済みのプラットフォームのいずれかを使用していることを検証する必要があります。 GuardDuty エージェントを手動で管理している場合は、Kubernetes バージョンが現在使用中の GuardDuty エージェントバージョンをサポートしていることを確認してください。

検証済みプラットフォーム

OS ディストリビューション、カーネルバージョン、CPU アーキテクチャは、 GuardDuty セキュリティエージェントが提供するサポートに影響します。次の表は、 GuardDuty セキュリティエージェントをデプロイし、EKS Runtime Monitoring を設定するための検証済み設定を示しています。

OS ディストリビューション	カーネルバージョン	カーネルサポート	CPU アーキテクチャ		サポートされている Kubernetes バージョン
			x64 (AMD64)	Graviton (ARM64) (Graviton2 以上) [1]	
Ubuntu AL2 AL2023[3]	5.4、5.10、5.15、6.1[2]	eBPF Tracepoints、Kprobe	サポート	サポート	v1.21 - v1.29
Bottlerocket					v1.23 - v1.29

1. Amazon EKS クラスターの Runtime Monitoring は、A1 インスタンスタイプなどの第 1 世代 Graviton インスタンスをサポートしていません。
2. 現在、カーネルバージョン では`6.1`、 GuardDuty Runtime Monitoring の検出結果タイプは に関連する を生成できませんDNS イベント。
3. Runtime Monitoring は、 GuardDuty セキュリティエージェント v1.6.0 以降のリリースで AL2023 をサポートしています。詳細については、「GuardDuty Amazon EKS クラスター用の セキュリティエージェント」を参照してください。

GuardDuty セキュリティエージェントがサポートする Kubernetes バージョン

次の表は、 GuardDuty セキュリティエージェントでサポートされている EKS クラスターの Kubernetes バージョンを示しています。

Kubernetes バージョン	Amazon EKS アドオン GuardDuty セキュリティエージェントのバージョン									
	v1.6.1	v1.6.0	v1.5.0	v1.4.1	v1.4.0	v1.3.1	v1.3.0	v1.2.0	v1.1.0	v1.0.0
1.29	サポート	サポート対象	サポート対象	サポート対象	サポート	サポートされません	サポートされません	サポートされません	サポートされません	サポートされません
1.28						サポート	サポート			
1.27								サポート		
1.26									サポート	
1.25										サポート
1.24										
1.23										
1.22										
1.21										

一部の GuardDuty セキュリティエージェントバージョンは、標準サポートを終了します。エージェントリリースバージョンの詳細については、「」を参照してくださいGuardDuty Amazon EKS クラスター用の セキュリティエージェント。

CPU とメモリの制限

次の表は、() の Amazon EKS アドオン GuardDutyの CPU とメモリの制限を示していますaws-guardduty-agent。

パラメータ	最小限度	最大限度
CPU	200m	1000m

パラメータ	最小限度	最大限度
「メモリ」	256 Mi	1024 Mi

Amazon EKS アドオンバージョン 1.5.0 以降を使用する場合、 は CPU 値とメモリ値のアドオンスキーマを設定する機能 GuardDuty を提供します。設定可能な範囲については、「」を参照してください設定可能なパラメータと値。

EKS Runtime Monitoring を有効にして、EKS クラスターのカバレッジステータスを評価すると、コンテナインサイトメトリクスを設定および表示できます。詳細については、「CPU とメモリモニタリングの設定」を参照してください。

次のステップ

次のステップでは、Runtime Monitoring を設定し、セキュリティエージェントを手動または 経由で自動的に管理します GuardDuty。

スタンドアロンアカウントの Runtime Monitoring の有効化

アカウントで Runtime Monitoring を有効にするには、次の手順を実行します。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[Runtime Monitoring] を選択します。
3. [設定] タブで [有効にする] を選択し、アカウントの EKS Runtime Monitoring を有効にします。
4. が Amazon EC2 インスタンス、Amazon ECS クラスター、または Amazon EKS クラスターの 1 つ以上のリソースタイプからランタイムイベント GuardDuty を受信するには、次のオプションを使用して、これらのリソースのセキュリティエージェントを管理します。

   GuardDuty セキュリティエージェントを有効にするには

   - Amazon EC2 インスタンスの自動セキュリティエージェントの管理
   - Amazon EC2 インスタンスのセキュリティエージェントの手動管理
   - Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)
   - Amazon EKS クラスターのセキュリティエージェントの自動管理

- Amazon EKS クラスターのセキュリティエージェントの手動管理

マルチアカウント環境の Runtime Monitoring の有効化

マルチアカウント環境では、委任された GuardDuty 管理者アカウントのみがメンバーアカウントの Runtime Monitoring を有効または無効にし、組織内のメンバーアカウントに属するリソースタイプの自動エージェント設定を管理できます。 GuardDuty メンバーアカウントは、自分のアカウントからこの設定を変更することはできません。委任 GuardDuty 管理者アカウントは、 を使用してメンバーアカウントを管理します AWS Organizations。マルチアカウント環境の詳細については、「複数のアカウントの管理」を参照してください。

委任 GuardDuty 管理者アカウントの場合

委任 GuardDuty 管理者アカウントの Runtime Monitoring を有効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[Runtime Monitoring] を選択します。
3. [設定] タブの [Runtime Monitoring 設定] セクションで [編集] を選択します。
4. [すべてのアカウントについて有効にする] の使用

   委任された GuardDuty 管理者アカウントを含む、組織に属するすべてのアカウントに対して Runtime Monitoring を有効にする場合は、すべてのアカウントに対して有効にする を選択します。
5. [アカウントを手動で設定] の使用

   メンバーアカウントごとに個別に Runtime Monitoring を有効にする場合は、[アカウントを手動で設定] を選択します。

   - [委任された管理者 (このアカウント)] セクションで [有効にする] を選択します。
6. が Amazon EC2 インスタンス、Amazon ECS クラスター、または Amazon EKS クラスターの 1 つ以上のリソースタイプからランタイムイベント GuardDuty を受信するには、次のオプションを使用して、これらのリソースのセキュリティエージェントを管理します。

   GuardDuty セキュリティエージェントを有効にするには

   - Amazon EC2 インスタンスの自動セキュリティエージェントの管理
   - Amazon EC2 インスタンスのセキュリティエージェントの手動管理

- Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)
- Amazon EKS クラスターのセキュリティエージェントの自動管理
- Amazon EKS クラスターのセキュリティエージェントの手動管理

すべてのメンバーアカウントの場合

組織内のすべてのメンバーアカウントの Runtime Monitoring を有効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任 GuardDuty 管理者アカウントを使用してサインインします。
2. ナビゲーションペインで、[Runtime Monitoring] を選択します。
3. Runtime Monitoring ページの Configuration タブで、Runtime Monitoring 設定セクションの Edit を選択します。
4. [すべてのアカウントについて有効にする] を選択します。
5. が Amazon EC2 インスタンス、Amazon ECS クラスター、または Amazon EKS クラスターの 1 つ以上のリソースタイプからランタイムイベント GuardDuty を受信するには、次のオプションを使用して、これらのリソースのセキュリティエージェントを管理します。

   GuardDuty セキュリティエージェントを有効にするには

   - Amazon EC2 インスタンスの自動セキュリティエージェントの管理
   - Amazon EC2 インスタンスのセキュリティエージェントの手動管理
   - Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)
   - Amazon EKS クラスターのセキュリティエージェントの自動管理
   - Amazon EKS クラスターのセキュリティエージェントの手動管理

既存のすべてのアクティブなメンバーアカウントの場合

組織内の既存のメンバーアカウントの Runtime Monitoring を有効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   組織の委任 GuardDuty 管理者アカウントを使用してサインインします。

2. ナビゲーションペインで、[Runtime Monitoring] を選択します。
3. [Runtime Monitoring] ページの [設定] タブで、Runtime Monitoring 設定の現在のステータスを表示できます。
4. [Runtime Monitoring] ペイン内の [アクティブなメンバーアカウント] セクションで、[アクション] を選択します。
5. [アクション] ドロップダウンメニューから、[すべての既存のアクティブなメンバーアカウントについて有効にする] を選択します。
6. [確認] を選択します。
7. が Amazon EC2 インスタンス、Amazon ECS クラスター、または Amazon EKS クラスターの 1 つ以上のリソースタイプからランタイムイベント GuardDuty を受信するには、次のオプションを使用して、これらのリソースのセキュリティエージェントを管理します。

   GuardDuty セキュリティエージェントを有効にするには

   - Amazon EC2 インスタンスの自動セキュリティエージェントの管理
   - Amazon EC2 インスタンスのセキュリティエージェントの手動管理
   - Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)
   - Amazon EKS クラスターのセキュリティエージェントの自動管理
   - Amazon EKS クラスターのセキュリティエージェントの手動管理

> **Note**
>
> メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

新しいメンバーアカウントに対してのみ Runtime Monitoring を自動的に有効にする

組織内の新しいメンバーアカウントの Runtime Monitoring を有効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   組織の指定された委任 GuardDuty 管理者アカウントを使用してサインインします。
2. ナビゲーションペインで、Runtime Monitoring を選択します。
3. [設定] タブの [Runtime Monitoring 設定] セクションで [編集] を選択します。
4. [アカウントを手動で設定] を選択します。

5. [新しいメンバーアカウントについて自動的に有効にする] を選択します。
6. が Amazon EC2 インスタンス、Amazon ECS クラスター、または Amazon EKS クラスターの 1 つ以上のリソースタイプからランタイムイベント GuardDuty を受信するには、次のオプションを使用して、これらのリソースのセキュリティエージェントを管理します。

   GuardDuty セキュリティエージェントを有効にするには

   - Amazon EC2 インスタンスの自動セキュリティエージェントの管理
   - Amazon EC2 インスタンスのセキュリティエージェントの手動管理
   - Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)
   - Amazon EKS クラスターのセキュリティエージェントの自動管理
   - Amazon EKS クラスターのセキュリティエージェントの手動管理

選択的アクティブメンバーアカウントのみ

個々のアクティブなメンバーアカウントの Runtime Monitoring を有効にするには

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

   委任 GuardDuty 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
3. [アカウント] ページで、[Runtime Monitoring] および [エージェントの自動管理] の列の値を確認します。これらの値は、対応するアカウントで Runtime Monitoring と GuardDuty エージェント管理が有効か無効かを示します。
4. [アカウント] テーブルから、Runtime Monitoring を有効にするアカウントを選択します。一度に複数のアカウントを選択できます。
5. [確認] を選択します。
6. [保護プランを編集] を選択します。適切なアクションを選択します。
7. [確認] を選択します。
8. が Amazon EC2 インスタンス、Amazon ECS クラスター、または Amazon EKS クラスターの 1 つ以上のリソースタイプからランタイムイベント GuardDuty を受信するには、次のオプションを使用して、これらのリソースのセキュリティエージェントを管理します。

   GuardDuty セキュリティエージェントを有効にするには

   - Amazon EC2 インスタンスの自動セキュリティエージェントの管理

- Amazon EC2 インスタンスのセキュリティエージェントの手動管理
- Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)
- Amazon EKS クラスターのセキュリティエージェントの自動管理
- Amazon EKS クラスターのセキュリティエージェントの手動管理

GuardDuty セキュリティエージェントの管理

モニタリングするリソース GuardDuty のセキュリティエージェントを管理できます。複数のリソースタイプをモニタリングする場合は、そのリソースの GuardDuty エージェントを必ず管理してください。

> **Important**
>
> Amazon EC2 インスタンス GuardDuty のセキュリティエージェントを使用する場合は、Amazon EKS クラスター内の基盤となるホストにエージェントをインストールして使用できます。その EKS クラスターにセキュリティエージェントを既にデプロイしている場合、同じホストで 2 つのセキュリティエージェントを同時に実行できます。このシナリオでの GuardDuty の仕組みについては、「」を参照してくださいデュアルセキュリティエージェントの処理。

以下のトピックは、セキュリティエージェントを管理する次の手順に役立ちます。

内容

- 自動セキュリティエージェントで共有 VPC を使用する
- ホストにインストールされたデュアルセキュリティエージェントの処理
- Amazon EC2 インスタンスの自動セキュリティエージェントの管理
- Amazon EC2 インスタンスのセキュリティエージェントの手動管理
- Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)
- Amazon EKS クラスターのセキュリティエージェントの自動管理
- Amazon EKS クラスターのセキュリティエージェントの手動管理

自動セキュリティエージェントで共有 VPC を使用する

セキュリティエージェントを自動的に GuardDuty 管理することを選択した場合、Runtime Monitoring は、 内の同じ組織 AWS アカウント に属する の共有 VPC の使用をサポートします AWS Organizations。ユーザーに代わって、組織の共有 VPC に関連付けられている詳細に基づいて Amazon VPC エンドポイントポリシー GuardDuty を設定できます。

このリリース以前は、 GuardDuty セキュリティエージェントを手動で管理することを選択した場合のみ、 は共有 VPCs の使用 GuardDuty をサポートしていました。

内容

仕組み

共有 VPC の所有者アカウントがいずれかのリソース (Amazon EKS または AWS Fargate (Amazon ECS のみ)) の Runtime Monitoring と自動エージェント設定を有効にすると、すべての共有 VPCs は、共有 VPC 所有者アカウント内の共有 Amazon VPC エンドポイントおよび関連するセキュリティグループの自動インストールの対象となります。共有 Amazon VPC に関連付けられた組織 ID GuardDuty を取得します。

これで、共有 Amazon VPC 所有者アカウントと同じ組織 AWS アカウント に属する は、同じ Amazon VPC エンドポイントを共有することもできます。共有 VPC 所有者アカウントまたは参加アカウントのいずれかに Amazon VPC エンドポイントが必要な場合、 は共有 VPC GuardDuty を作成します。Amazon VPC エンドポイントを必要とする例には GuardDuty、、Runtime Monitoring、EKS Runtime Monitoring の有効化、新しい Amazon ECS-Fargate タスクの起動などがあります。これらのアカウントが任意のリソースタイプの Runtime Monitoring と自動エージェント設定を有効にすると、 は Amazon VPC エンドポイント GuardDuty を作成し、共有 VPC 所有者アカウントと同じ組織 ID でエンドポイントポリシーを設定します。 は`GuardDutyManaged`タグ GuardDuty を追加して、 が GuardDuty 作成する Amazon VPC エンドポイント`true`の に設定します。共有 Amazon VPC 所有者アカウントが、どのリソースに対しても Runtime Monitoring または自動エージェント設定を有効にしていない場合、 GuardDuty は Amazon VPC エンドポイントポリシーを設定しません。共有 VPC 所有者アカウントで Runtime Monitoring を設定し、セキュリティエージェントを自動的に管理する方法については、「」を参照してくださいRuntime Monitoring GuardDuty の有効化。

同じ Amazon VPC エンドポイントポリシーを使用する各アカウントは、関連付けられた共有 Amazon VPC の参加者 AWS アカウントとして呼び出されます。

次の例は、共有 VPC 所有者アカウントと参加者アカウントのデフォルトの VPC エンドポイントポリシーを示しています。aws:PrincipalOrgID は、共有 VPC リソースに関連付けられた組織 ID を表示します。このポリシーの使用は、所有者アカウントの組織に存在する参加者アカウントに限定されます。

Example

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

共有 VPC を使用するための前提条件

初期設定の前提条件

共有 VPC の所有者になる AWS アカウント には、 で次の手順を実行します。

1. 組織の作成 — ユーザーガイドの「組織の作成と管理」の手順に従って組織AWS Organizations を作成します。

   メンバーアカウントの追加または削除については、「組織 AWS アカウント での の管理」を参照してください。

2. 共有 VPC リソースの作成 – 所有者アカウントから共有 VPC リソースを作成できます。詳細については、「Amazon VPC ユーザーガイド」の「VPC を他のアカウントと共有する」を参照してください。

Runtime Monitoring に GuardDuty固有の前提条件

次のリストは、 に固有の前提条件を示しています GuardDuty。

- 共有 VPC の所有者アカウントと参加アカウントは、 のさまざまな組織から取得できます GuardDuty。ただし、 内の同じ組織に属している必要があります AWS Organizations。これは、が Amazon VPC エンドポイントと共有 VPC のセキュリティグループを作成 GuardDuty するために必要です。共有 VPCs「Amazon VPC ユーザーガイド」の「他の アカウントと VPC を共有する」を参照してください。
- 共有 VPC 所有者アカウントと参加者アカウントの任意のリソースに対して、Runtime Monitoring または EKS Runtime Monitoring、および GuardDuty 自動エージェント設定を有効にします。詳細については、「Runtime Monitoring の有効化」を参照してください。

  これらの設定をすでに完了している場合は、次のステップに進みます。
- Amazon EKS または Amazon ECS (AWS Fargate のみ) タスクを操作する場合は、所有者アカウントに関連付けられた共有 VPC リソースを選択し、そのサブネットを選択してください。

よくある質問 (FAQ)

次のリストは、Runtime Monitoring で GuardDuty 自動エージェント設定が有効になっている共有 VPC リソースを使用する場合によくある質問のトラブルシューティング手順を示しています。

既に Runtime Monitoring (または EKS Runtime Monitoring) を使用しています。共有 VPC を有効にするにはどうすればよいですか？

共有 VPC を作成するための前提条件については、「」を参照してください前提条件。

共有 VPC 所有者アカウントと参加者アカウントの両方が前提条件を満たしている場合、 GuardDuty は Amazon VPC エンドポイントポリシーを自動的に設定しようとします。

このリリースより前に、共有 VPC がサポートされていないというカバレッジの問題 AWS アカウント が発生した場合は、前提条件に従ってください。リソースタイプ (Amazon EKS または Amazon ECS (AWS Fargate のみ) タスク) が共有 VPC エンドポイントの要件を呼び出すと、 GuardDuty は新しい VPC エンドポイントポリシーの設定を試みます。

共有 VPC 所有者アカウントとして、共有 VPC エンドポイントポリシーを組織内の参加者アカウントのサブセットに制限する必要があります。これを行うにはどうすればよいですか？

エンドポイントに関連付けられた `GuardDutyManaged : true` タグがある場合は、それを削除します。これにより GuardDuty 、 は共有 VPC の VPC エンドポイントポリシーを変更または上書きしようとできなくなります。

詳細については、「エンドポイントポリシーを使用して VPC エンドポイントへのアクセスを制御する」を参照してください。

共有 VPC エンドポイントが から **aws:PrincipalAccount**に変更されるのはなぜですか**aws:PrincipalOrgId**？ これを防ぐにはどうすればよいですか？

が 内の同じ組織の複数のアカウントによって VPC が共有されていること GuardDuty を検出する GuardDuty と AWS Organizations、 は組織 ID を指定するようにポリシーを変更しようとします。

これを防ぐには、共有 VPC エンドポイントから `GuardDutyManaged : true` タグを削除します。これにより GuardDuty 、 は共有 VPC の VPC エンドポイントポリシーを変更または上書きしようとできなくなります。

共有 VPC 所有者アカウントまたは参加者アカウントの 1 つが GuardDuty または Runtime Monitoring (または EKS Runtime Monitoring) を無効にした場合どうなりますか？

共有 VPC 所有者アカウントが GuardDuty または Runtime Monitoring (または EKS Runtime Monitoring) GuardDuty を無効にした場合、 は、参加者アカウントに属するリソースタイプが共有 VPC エンドポイントを使用したか、参加者アカウントが任意のリソースタイプに対して GuardDuty エージェント管理を有効にしたかどうかを確認します。「は GuardDuty い」の場合、VPC エンドポイントとセキュリティグループは削除しません。

共有 VPC 参加者アカウントが GuardDuty または Runtime Monitoring (または EKS Runtime Monitoring) を無効にした場合、共有 VPC 所有者アカウントには影響せず、所有者アカウントは共有 VPC リソースもセキュリティグループも削除しません。

共有 VPC リソースを削除するにはどうすればよいですか？ どのような影響がありますか？

共有 VPC 所有者アカウントとして、共有 VPC リソースは、アカウントまたは Runtime Monitoring の参加アカウントで使用されている場合でも削除できます。共有 VPC の削除とその影響の理解については、「」を参照してくださいTo delete a VPC endpoint。

ホストにインストールされたデュアルセキュリティエージェントの処理

Amazon EC2 インスタンスは、複数のタイプのワークロードをサポートできます。Amazon EC2 インスタンスで自動セキュリティエージェントを設定すると、同じ EC2 インスタンスに EKS 経由で別のセキュリティエージェントが含まれる場合があります。

概要

Runtime Monitoring を有効にしたシナリオを考えてみます。次に、 を使用して Amazon EKS の自動エージェントを有効にします GuardDuty。Amazon EC2 の自動エージェントも有効にしました。同じ基盤となるホストが、Amazon EKS 用と Amazon EC2 用の 2 つのセキュリティエージェントでインストールされる場合があります。これにより、同じホスト内で 2 つのセキュリティエージェントが実行され、ランタイムイベントが収集されて に送信され GuardDuty、重複した検出結果が発生する可能性があります。

Impact

- 同じホストで複数のセキュリティエージェントが実行されている場合、アカウントで CPU とメモリの処理ニーズが 2 倍になる可能性があります。各リソースタイプの CPU とメモリの制限については、そのリソースの前提条件「」を参照してください。
- GuardDuty は、同じ基盤となるホストからランタイムイベントを収集する 2 つのセキュリティエージェントが重複している場合でも、アカウントはランタイムイベントの 1 つのストリームに対してのみ課金されるように Runtime Monitoring 機能を設計しました。

が複数のエージェント GuardDuty を処理する方法

GuardDuty は、2 つのセキュリティエージェントが同じホストで実行されていることを検出し、そのうちの 1 つだけをランタイムイベントをアクティブに収集するセキュリティエージェントとして指定します。2 番目のエージェントは、アプリケーションのパフォーマンスへの影響を防ぐために、最小限のシステムリソースを消費します。

GuardDuty では、次のシナリオを考慮します。

- EC2 インスタンスが Amazon EKS と Amazon EC2 セキュリティエージェントの両方のスコープに属する場合、EKS セキュリティエージェントが優先されます。これは、Amazon EC2 でセキュリティエージェント v1.1.0 以降を使用している場合にのみ適用されます。古いエージェントバージョンは優先順位付けの影響を受けないため、古いエージェントバージョンは引き続き実行され、ランタイムイベントが収集されます。

- Amazon EKS と Amazon EC2 の両方に GuardDuty マネージドセキュリティエージェントがあり、Amazon EC2 インスタンスも SSM 管理されている場合、両方のセキュリティエージェントはホストレベルでインストールされます。エージェントをインストールすると、 はどのセキュリティエージェントが引き続き実行されるか GuardDuty を決定します。両方のセキュリティエージェントが実行されている場合、最終的にはそのうちの 1 つだけがランタイムイベントを収集します。
- EC2 と EKS の両方に関連付けられたセキュリティエージェントが同時に実行されると、 は重複期間中にのみ重複した検出結果を生成する GuardDuty 可能性があります。

  これは、次の場合に発生する可能性があります。

  - EC2 と EKS の両方のセキュリティエージェントは、 GuardDuty （ 自動的に) または
  - Amazon EKS リソースには自動セキュリティエージェントがあります。
- EKS セキュリティエージェントが既に実行されている場合、EC2 セキュリティエージェントを同じ基盤となるホストに手動でデプロイし、すべての前提条件を満たしている場合、2 番目のセキュリティエージェントをインストールしない GuardDuty 可能性があります。

Amazon EC2 インスタンスの自動セキュリティエージェントの管理

> **Note**
>
> 続行する前に、必ずすべての に従ってくださいAmazon EC2 インスタンスサポートの前提条件。

Amazon EC2 手動エージェントから自動エージェントへの移行

このセクションは、以前にセキュリティエージェントを手動で管理していて、自動 GuardDuty エージェント設定を使用したい AWS アカウント 場合に適用されます。これが当てはまらない場合は、アカウントのセキュリティエージェントの設定を続行します。

GuardDuty 自動エージェントを有効にすると、 がユーザーに代わってセキュリティエージェント GuardDuty を管理します。が GuardDuty 実行する手順については、「」を参照してください自動エージェント設定を使用する (推奨)。

リソースをクリーンアップする

SSM の関連付けを削除する

- Amazon EC2 のセキュリティエージェントを手動で管理していたときに作成した SSM 関連付けをすべて削除します。詳細については、「関連付けの削除」を参照してください。
- これは、アカウントレベルまたはインスタンスレベルで自動エージェントを使用するかどうか (包含タグまたは除外タグを使用) にかかわらず、 が SSM アクションの管理を引き GuardDuty 継ぐことができるように行われます。SSM アクションで実行できるアクションの詳細については、 GuardDuty 「」を参照してくださいのサービスにリンクされたロールのアクセス許可 GuardDuty。
- セキュリティエージェントを手動で管理するために以前に作成された SSM 関連付けを削除すると、 がセキュリティエージェントを自動的に管理するための SSM 関連付け GuardDuty を作成するときに、短時間の重複が生じることがあります。この間、SSM スケジューリングに基づいて競合が発生する可能性があります。詳細については、Amazon EC2 SSM スケジューリング」を参照してください。

Amazon EC2 インスタンスの包含タグと除外タグを管理する

- 包含タグ – GuardDuty 自動エージェント設定を有効にせず、Amazon EC2 インスタンスに包含タグ (`GuardDutyManaged : true`) GuardDuty をタグ付けすると、 は、選択した EC2 インスタンスにセキュリティエージェントをインストールして管理する SSM 関連付けを作成します。これは、選択した EC2 インスタンスでのみセキュリティエージェントを管理するのに役立つ想定される動作です。詳細については、「Runtime Monitoring が Amazon EC2 インスタンスと連携する方法」を参照してください。

  GuardDuty がセキュリティエージェントをインストールおよび管理できないようにするには、これらの EC2 インスタンスから包含タグを削除します。詳細については、「Amazon EC2 ユーザーガイド」の「タグの追加と削除」を参照してください。 Amazon EC2
- 除外タグ – アカウント内のすべての EC2 インスタンスの自動 GuardDuty エージェント設定を有効にする場合は、EC2 インスタンスに除外タグ (`GuardDutyManaged : false`) が付けられていないことを確認してください。

スタンドアロンアカウントの GuardDuty エージェントの設定

Configure for all instances

スタンドアロンアカウント内のすべてのインスタンスの Runtime Monitoring を設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[Runtime Monitoring] を選択します。
3. [設定] タブで、[編集] を選択します。
4. EC2 セクションで、 を有効にするを選択します。
5. [保存] を選択します。
6. GuardDuty が作成する SSM の関連付けが、アカウントに属するすべての EC2 リソースにセキュリティエージェントをインストールおよび管理することを確認できます。

   a. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。

   b. SSM 関連付けのターゲットタブを開きます (`GuardDutyRuntimeMonitoring-do-not-delete`)。タグキーが として表示されることを確認しますInstanceIds。

Using inclusion tag in selected instances

選択した Amazon EC2 インスタンスのセキュリティ GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. 潜在的な脅威を監視および検出するインスタンス GuardDuty に `GuardDutyManaged : true` タグを追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。
3. GuardDuty が作成する SSM 関連付けが、包含タグでタグ付けされた EC2 リソースにのみセキュリティエージェントをインストールおよび管理することを確認できます。

   https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。

- 作成される SSM 関連付けのターゲットタブを開きます (`GuardDutyRuntimeMonitoring-do-not-delete`)。タグキーはタグとして表示されますGuardDutyManaged。

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 インスタンスを起動する前に、必ず除外タグを追加してください。Amazon EC2 の自動エージェント設定を有効にすると、除外タグなしで起動する EC2 インスタンスは、 GuardDuty 自動エージェント設定の対象となります。

選択した Amazon EC2 インスタンスのセキュリティ GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. `GuardDutyManaged : false` タグを、潜在的な脅威をモニタリングおよび検出したくないインスタンス GuardDuty に追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。
3. インスタンスメタデータで除外タグを使用するには、次の手順を実行します。
   a. インスタンスの詳細タブで、インスタンスメタデータ のタグを許可するのステータスを表示します。

      現在 が無効になっている場合は、次の手順を使用してステータスを有効 に変更します。それ以外の場合は、この手順をスキップしてください。
   b. タグを許可するインスタンスを選択します。
   c. アクションメニューで、インスタンス設定 を選択します。
   d. インスタンスメタデータ でタグを許可する を選択します。
   e. インスタンスメタデータのタグへのアクセス で、 を許可する を選択します。
   f. [保存] を選択します。
4. 除外タグを追加したら、すべてのインスタンスの設定 タブで意味付けされたのと同じステップを実行します。

ランタイム を評価できるようになりましたAmazon EC2 インスタンスのカバレッジ。

マルチアカウント環境での GuardDuty エージェントの設定

委任 GuardDuty 管理者アカウントの場合

Configure for all instances

Runtime Monitoring のすべてのアカウントで を有効にする を選択した場合は、委任された GuardDuty 管理者アカウントで次のいずれかのオプションを選択します。

- オプション 1

  自動エージェント設定 の EC2 セクションで、すべてのアカウント に対して有効化 を選択します。
- オプション 2
  - 自動エージェント設定 の EC2 セクションで、アカウントを手動で設定 を選択します。
  - 「委任管理者 (このアカウント) 」で、「 を有効にする」を選択します。
- [保存] を選択します。

Runtime Monitoring 用にアカウントを手動で設定を選択した場合は、次の手順を実行します。

- 自動エージェント設定 の EC2 セクションで、アカウントを手動で設定 を選択します。
- 委任管理者 (このアカウント) で、 を有効にする を選択します。
- [保存] を選択します。

委任された GuardDuty 管理者アカウントの自動エージェント設定を有効にするオプションにかかわらず、 が GuardDuty 作成する SSM 関連付けがこのアカウントに属するすべての EC2 リソースにセキュリティエージェントをインストールおよび管理することを確認できます。

1. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。
2. SSM 関連付けのターゲットタブを開きます (`GuardDutyRuntimeMonitoring-do-not-delete`) 。タグキーが として表示されることを確認しますInstanceIds。

Using inclusion tag in selected instances

選択した Amazon EC2 インスタンスの GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. 潜在的な脅威を監視および検出するインスタンス GuardDuty に `GuardDutyManaged : true` タグを追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。

   このタグを追加すると、 はこれらの選択した EC2 インスタンスのセキュリティエージェントをインストールおよび管理 GuardDuty できます。自動エージェント設定を明示的に有効にする必要はありません。
3. GuardDuty が作成する SSM 関連付けが、包含タグでタグ付けされた EC2 リソースにのみセキュリティエージェントをインストールおよび管理することを確認できます。

   https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。

   - 作成される SSM 関連付けのターゲットタブを開きます (`GuardDutyRuntimeMonitoring-do-not-delete`)。タグキーはタグとして表示されますGuardDutyManaged。

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 インスタンスを起動する前に、必ず除外タグを追加してください。Amazon EC2 の自動エージェント設定を有効にすると、除外タグなしで起動する EC2 インスタンスは、 GuardDuty 自動エージェント設定の対象となります。

選択した Amazon EC2 インスタンスの GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。

2. 潜在的な脅威をモニタリングおよび検出したくないインスタンス GuardDuty に `GuardDutyManaged : false` タグを追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。
3. インスタンスメタデータで除外タグを使用するには、次の手順を実行します。

   a. インスタンスの詳細 タブで、インスタンスメタデータのタグを許可する のステータスを表示します。

      現在 が無効になっている場合は、次の手順を使用してステータスを有効 に変更します。それ以外の場合は、この手順をスキップしてください。

   b. アクションメニューで、インスタンス設定 を選択します。

   c. インスタンスメタデータ でタグを許可する を選択します。
4. 除外タグを追加したら、すべてのインスタンスの設定タブで指定したのと同じステップを実行します。

ランタイム を評価できるようになりましたAmazon EC2 インスタンスのカバレッジ。

すべてのメンバーアカウントの自動有効化

> **Note**
>
> メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

Configure for all instances

次の手順では、Runtime Monitoring セクションですべてのアカウントに対して を有効にする を選択していることを前提としています。

1. Amazon EC2 の自動エージェント設定セクションで、すべてのアカウントに対して有効化を選択します。
2. (`GuardDutyRuntimeMonitoring-do-not-delete`) GuardDuty を作成する SSM の関連付けが、このアカウントに属するすべての EC2 リソースにセキュリティエージェントをインストールおよび管理することを確認できます。

   a. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。

b. SSM 関連付けのターゲットタブを開きます。タグキーが として表示されることを確認しますInstanceIds。

Using inclusion tag in selected instances

選択した Amazon EC2 インスタンスの GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. 潜在的な脅威を監視および検出する EC2 インスタンス GuardDuty に `GuardDutyManaged : true` タグを追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。

   このタグを追加すると、 はこれらの選択した EC2 インスタンスのセキュリティエージェントをインストールおよび管理 GuardDuty できます。自動エージェント設定を明示的に有効にする必要はありません。
3. GuardDuty が作成する SSM 関連付けが、アカウントに属するすべての EC2 リソースにセキュリティエージェントをインストールおよび管理することを確認できます。

   a. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。

   b. SSM 関連付けのターゲットタブを開きます (`GuardDutyRuntimeMonitoring-do-not-delete`)。タグキーが として表示されることを確認しますInstanceIds。

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 インスタンスを起動する前に、必ず除外タグを追加してください。Amazon EC2 の自動エージェント設定を有効にすると、除外タグなしで起動する EC2 インスタンスは、 GuardDuty 自動エージェント設定の対象となります。

選択した Amazon EC2 インスタンスのセキュリティ GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。

2. 潜在的な脅威を監視および検出したくないインスタンス GuardDuty に `GuardDutyManaged : false` タグを追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。
3. インスタンスメタデータで除外タグを使用するには、次の手順を実行します。

   a. インスタンスの詳細タブで、インスタンスメタデータのタグを許可するのステータスを表示します。

      現在 が無効になっている場合は、次の手順を使用してステータスを有効 に変更します。それ以外の場合は、この手順をスキップしてください。

   b. アクションメニューで、インスタンス設定 を選択します。

   c. インスタンスメタデータ でタグを許可する を選択します。
4. 除外タグを追加したら、「すべてのインスタンスの設定」タブで指定したのと同じステップを実行します。

ランタイム を評価できるようになりましたAmazon EC2 インスタンスのカバレッジ。

新しいメンバーアカウントでのみ自動有効化

委任された GuardDuty 管理者アカウントは、Amazon EC2 リソースの自動エージェント設定を設定して、新しいメンバーアカウントが組織に参加するときに自動的に を有効にできます。

Configure for all instances

次の手順では、Runtime Monitoring セクションで、新しいメンバーアカウントに対して自動有効化を選択していることを前提としています。

1. ナビゲーションペインで、[Runtime Monitoring] を選択します。
2. Runtime Monitoring ページで、編集 を選択します。
3. [新しいメンバーアカウントについて自動的に有効にする] を選択します。このステップにより、新しいアカウントが組織に加わるたびに、Amazon EC2 の自動エージェント設定がアカウントに対して自動的に有効になります。この選択を変更できるのは、組織の委任 GuardDuty 管理者アカウントのみです。
4. [保存] を選択します。

新しいメンバーアカウントが組織に加わると、この設定は自動的に有効になります。が、この新しいメンバーアカウントに属する Amazon EC2 インスタンスのセキュリティエージェントを管理

する GuardDuty には、すべての前提条件EC2 インスタンスの場合が満たされていることを確認してください。

SSM 関連付けが作成されると (`GuardDutyRuntimeMonitoring-do-not-delete`)、SSM 関連付けが新しいメンバーアカウントに属するすべての EC2 インスタンスにセキュリティエージェントをインストールおよび管理することを確認できます。

- https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。
- SSM 関連付けのターゲットタブを開きます。タグキーが として表示されることを確認しますInstanceIds。

Using inclusion tag in selected instances

アカウント内の選択したインスタンスのセキュリティ GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. 潜在的な脅威を監視および検出するインスタンス GuardDuty に `GuardDutyManaged : true` タグを追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。

   このタグを追加すると、 はこれらの選択したインスタンスのセキュリティエージェントをインストールおよび管理 GuardDuty できます。自動エージェント設定を明示的に有効にする必要はありません。
3. GuardDuty が作成する SSM 関連付けが、包含タグでタグ付けされた EC2 リソースにのみセキュリティエージェントをインストールおよび管理することを確認できます。

   a. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。

   b. 作成される SSM 関連付けのターゲットタブを開きます。タグキーはタグとして表示されますGuardDutyManaged。

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 インスタンスを起動する前に、必ず除外タグを追加してください。Amazon EC2 の自動エージェント設定を有効にすると、除外タグなしで起動する EC2 インスタンスは、 GuardDuty 自動エージェント設定の対象となります。

スタンドアロンアカウントの特定のインスタンスに GuardDuty セキュリティエージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. 潜在的な脅威を監視および検出したくないインスタンス GuardDuty に `GuardDutyManaged : false` タグを追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。
3. インスタンスメタデータで除外タグを使用するには、次の手順を実行します。
   a. インスタンスの詳細タブで、インスタンスメタデータ のタグを許可するのステータスを表示します。

      現在 が無効になっている場合は、次の手順を使用してステータスを有効 に変更します。それ以外の場合は、この手順をスキップしてください。
   b. アクションメニューで、インスタンス設定 を選択します。
   c. インスタンスメタデータ でタグを許可する を選択します。
4. 除外タグを追加したら、「すべてのインスタンスの設定」タブで指定したのと同じステップを実行します。

ランタイム を評価できるようになりましたAmazon EC2 インスタンスのカバレッジ。

選択的メンバーアカウントのみ

Configure for all instances

1. アカウントページで、Runtime Monitoring-Automated エージェント設定 (Amazon EC2) を有効にするアカウントを 1 つ以上選択します。このステップで選択したアカウントで、Runtime Monitoring が既に有効になっていることを確認します。

2. 「保護プランの編集」から適切なオプションを選択して、Runtime Monitoring-Automated エージェント設定 (Amazon EC2) を有効にします。
3. [確認] を選択します。

Using inclusion tag in selected instances

選択したインスタンスのセキュリティ GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. 潜在的な脅威を監視および検出するインスタンス GuardDuty に `GuardDutyManaged : true` タグを追加します。このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。

   このタグを追加する GuardDuty と、 はタグ付けされた Amazon EC2 インスタンスのセキュリティエージェントを管理できるようになります。自動エージェント設定 (Runtime Monitoring - Automated Agent Configuration (EC2) を明示的に有効にする必要はありません。

Using exclusion tag in selected instances

> **Note**
>
> Amazon EC2 インスタンスを起動する前に、必ず除外タグを追加してください。Amazon EC2 の自動エージェント設定を有効にすると、除外タグなしで起動する EC2 インスタンスは、 GuardDuty 自動エージェント設定の対象となります。

選択したインスタンスのセキュリティ GuardDuty エージェントを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. `GuardDutyManaged : false` タグを、潜在的な脅威をモニタリングまたは検出したくない EC2 インスタンス GuardDuty に追加します。 このタグの追加については、「個々のリソースにタグを追加するには」を参照してください。

3. インスタンスメタデータで除外タグを使用するには、次の手順を実行します。

   a. インスタンスの詳細 タブで、インスタンスメタデータのタグを許可する のステータスを表示します。

      現在 が無効になっている場合は、次の手順を使用してステータスを有効 に変更します。それ以外の場合は、この手順をスキップしてください。

   b. アクションメニューで、インスタンス設定 を選択します。

   c. インスタンスメタデータ でタグを許可する を選択します。

4. 除外タグを追加したら、「すべてのインスタンスの設定」タブで指定したのと同じステップを実行します。

を評価できるようになりましたAmazon EC2 インスタンスのカバレッジ。

Amazon EC2 インスタンスのセキュリティエージェントの手動管理

Runtime Monitoring を有効にしたら、 GuardDuty セキュリティエージェントを手動でインストールする必要があります。エージェントをインストールすることで、 GuardDuty は Amazon EC2 インスタンスからランタイムイベントを受信します。

GuardDuty セキュリティエージェントを管理するには、Amazon VPC エンドポイントを作成し、手順に従ってセキュリティエージェントを手動でインストールする必要があります。

Amazon VPC エンドポイントの手動作成

GuardDuty セキュリティエージェントをインストールする前に、Amazon Virtual Private Cloud (Amazon VPC) エンドポイントを作成する必要があります。これにより、Amazon EC2 インスタンスのランタイムイベント GuardDuty を受信できます。

> **Note**
>
> VPC エンドポイントの使用に追加料金はかかりません。

Amazon VPC エンドポイントを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/vpc/ で Amazon VPC コンソールを開きます。

2. ナビゲーションペインの [VPC プライベートクラウド] で、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. [エンドポイントの作成] ページの [サービスカテゴリ] で [その他のエンドポイントサービス] を選択します。
5. [サービス名] に **com.amazonaws.*us-east-1*.guardduty-data** と入力します。

   必ず「*us-east-1*」をあなたの AWS リージョンに置き換えてください。これは、 AWS アカウント ID に属する Amazon EC2 インスタンスと同じリージョンである必要があります。
6. [サービスの確認] を選択します。
7. サービス名が正常に確認されたら、インスタンスが置かれている [VPC] を選択します。次のポリシーを追加して、Amazon VPC エンドポイントの使用を指定されたアカウントのみに制限します。このポリシー下で提供されている組織 Condition を使用して、次のポリシーを更新してエンドポイントへのアクセスを制限できます。組織内の特定のアカウント ID に Amazon VPC エンドポイントサポートを提供するには、「Organization condition to restrict access to your endpoint」を参照してください。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

aws:PrincipalAccount アカウント ID は、VPC と VPC エンドポイントを含むアカウントと一致する必要があります。次のリストは、VPC エンドポイントを他の AWS アカウント IDsと共有する方法を示しています。

- VPC エンドポイントにアクセスする複数のアカウントを指定するには、"aws:PrincipalAccount: "*111122223333*"を以下のブロックに置き換えます。

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
      ]
```

AWS アカウント IDs は、VPC エンドポイントにアクセスする必要があるアカウントのIDs に置き換えてください。

- 組織のすべてのメンバーが VPC エンドポイントにアクセスできるようにするには、"aws:PrincipalAccount: "*111122223333*" を以下のラインに置き換えます。

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

組織「*o-abcdef0123*」は必ず自分の組織 ID に置き換えてください。

- リソースへのアクセスを組織 ID で制限するには、ResourceOrgID をポリシーに追加します。詳細については、IAM ユーザーガイドaws:ResourceOrgIDの を参照してください。

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. [追加設定] で [DNS 名を有効にする] を選択します。
9. [サブネット] で、インスタンスが存在するサブネットを選択します。
10. [セキュリティグループ] で、VPC (または Amazon EC2 インスタンス) からのインバウンドポート 443 が有効になっているセキュリティグループを選択します。インバウンドポート 443 が有効になっているセキュリティグループがまだない場合は、「Amazon EC2 ユーザーガイド」の「セキュリティグループの作成」を参照してください。 Amazon EC2

    VPC (またはインスタンス) へのインバウンド許可を制限する際に問題が発生した場合は、任意の IP アドレス (0.0.0.0/0) からのインバウンド 443 ポートをサポートします。

セキュリティエージェントの手動インストール

GuardDuty には、Amazon EC2 インスタンスに GuardDuty セキュリティエージェントをインストールする次の 2 つの方法があります。 Amazon EC2

- 方法 1 - を使用する AWS Systems Manager – この方法では、Amazon EC2 インスタンス AWS Systems Manager を管理する必要があります。
- 方法 2 - Linux パッケージマネージャーを使用する – Amazon EC2 インスタンスが AWS Systems Manager 管理されているかどうかにかかわらず、この方法を使用できます。

方法 1 - AWS Systems Managerを使用する

この方法を使用するには、Amazon EC2 インスタンスが AWS Systems Manager 管理されていることを確認し、エージェントをインストールします。

AWS Systems Manager マネージド Amazon EC2 インスタンス

Amazon EC2 インスタンス AWS Systems Manager を管理できるようにするには、次の手順を実行します。

- AWS Systems Manager は、 AWS アプリケーションとリソースを管理し end-to-end 、大規模な安全な運用を可能にするのに役立ちます。

  で Amazon EC2 インスタンスを管理するには AWS Systems Manager、「 ユーザーガイド」の Amazon EC2 インスタンス用の Systems Manager のセットアップAWS Systems Manager 」を参照してください。
- 次の表に、新しい GuardDuty マネージド AWS Systems Manager ドキュメントを示します。

ドキュメント名	[Document type (ドキュメントタイプ)]	目的
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	ディストリビューター	GuardDuty セキュリティエージェントをパッケージ化するには。
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Command	インストール/アンインストールスクリプトを実行して GuardDuty セキュリティエー

ドキュメント名	[Document type (ドキュメントタイプ)]	目的
		ジェントをインストールするには。

の詳細については AWS Systems Manager、「 ユーザーガイド」のAmazon EC2 Systems Manager ドキュメントAWS Systems Manager 」を参照してください。

> **Debian サーバーの場合**
>
> が提供する Debian サーバー用の Amazon マシンイメージ (AMIs) では、 AWS Systems Manager エージェント (SSM エージェント) をインストール AWS する必要があります。Amazon EC2 Debian サーバーインスタンスを SSM で管理するには、SSM エージェントをインストールするための追加のステップを実行する必要があります。実行する必要がある手順については、「 AWS Systems Manager ユーザーガイド」の「Debian サーバーインスタンスに SSM エージェントを手動でインストールする」を参照してください。

を使用して Amazon EC2 インスタンスの GuardDuty エージェントをインストールするには AWS Systems Manager

1. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. Amazon が所有する で、 を選択しますAmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin。
4. [Run Command] を選択します。
5. 次の Run Command パラメータを入力します。
   - アクション: [インストール] を選択します。
   - インストールのタイプ: [インストール] または [アンインストール] を選択します。
   - 名前: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

- バージョン: これが空のままの場合、 GuardDuty 最新バージョンのセキュリティエージェントが表示されます。リリースバージョンの詳細については、「GuardDuty Amazon EC2 インスタンスのセキュリティエージェント」を参照してください。

6. 対象の Amazon EC2 インスタンス を選択します。複数の Amazon EC2 インスタンスを選択できます。詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager コンソールからコマンドを実行する」を参照してください。
7. GuardDuty エージェントのインストールが正常かどうかを検証します。詳細については、「GuardDuty セキュリティエージェントのインストールステータスの検証」を参照してください。

方法 2 - Linux パッケージマネージャーを使用する

この方法では、RPM スクリプトまたは Debian スクリプトを実行して GuardDuty セキュリティエージェントをインストールできます。オペレーティングシステムに基づいて、任意の方法を選択できます。

- RPM スクリプトを使用して、OS ディストリビューション AL2 または AL2023 にセキュリティエージェントをインストールします。
- Debian スクリプトを使用して、OS ディストリビューション Ubuntu または Debian にセキュリティエージェントをインストールします。サポートされている Ubuntu および Debian OS ディストリビューションの詳細については、「」を参照してくださいアーキテクチャ要件の検証。

RPM installation

> **Important**
> マシンにインストールする前に、 GuardDuty セキュリティエージェントの RPM 署名を確認することをお勧めします。

1. GuardDuty セキュリティエージェントの RPM 署名を検証する

   a. テンプレートを準備する

      適切なパブリックキー、x86_64 RPM の署名、arm64 RPM の署名、および Amazon S3 バケットでホストされている RPM スクリプトへの対応するアクセスリンクを使用し

てコマンドを準備します。RPM スクリプトにアクセスするには AWS リージョン、、AWS アカウント ID、および GuardDuty エージェントバージョンの値に置き換えます。

- パブリックキー :

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/
publickey.pem
```

- GuardDuty セキュリティエージェントの RPM 署名 :

  x86_64 RPM の署名

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/x86_64/
amazon-guardduty-agent-1.2.0.x86_64.sig
```

  arm64 RPM の署名

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/arm64/
amazon-guardduty-agent-1.2.0.arm64.sig
```

- Amazon S3 バケット内の RPM スクリプトへのアクセスリンク:

  x86_64 RPM 用アクセスリンク

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/x86_64/
amazon-guardduty-agent-1.2.0.x86_64.rpm
```

  arm64 RPM 用アクセスリンク

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/arm64/
amazon-guardduty-agent-1.2.0.arm64.rpm
```

AWS リージョン	リージョン名	AWS アカウント ID
eu-west-1	欧州 (アイルランド)	694911143906
us-east-1	米国東部 (バージニア北部)	593207742271
us-west-2	米国西部 (オレゴン)	733349766148

eu-west-3	欧州 (パリ)	665651866788
us-east-2	米国東部 (オハイオ)	307168627858
eu-central-1	欧州 (フランクフルト)	323658145986
ap-northeast-2	アジアパシフィック (ソウル)	914738172881
eu-north-1	欧州 (ストックホルム)	591436053604
ap-east-1	アジアパシフィック (香港)	258348409381
me-south-1	中東 (バーレーン)	536382113932
eu-west-2	欧州 (ロンドン)	892757235363
ap-northeast-1	アジアパシフィック (東京)	533107202818
ap-southeast-1	アジアパシフィック (シンガポール)	174946120834
ap-south-1	アジアパシフィック (ムンバイ)	251508486986
ap-southeast-3	アジアパシフィック (ジャカルタ)	510637619217
sa-east-1	南米 (サンパウロ)	758426053663
ap-northeast-3	アジアパシフィック (大阪)	273192626886
eu-south-1	欧州 (ミラノ)	266869475730
af-south-1	アフリカ (ケープタウン)	197869348890
ap-southeast-2	アジアパシフィック (シドニー)	005257825471

me-central-1	中東 (アラブ首長国連邦)	000014521398
us-west-1	米国西部 (北カリフォルニア)	684579721401
ca-central-1	カナダ (中部)	354763396469
ca-west-1	カナダ西部 (カルガリー)	339712888787
ap-south-2	アジアパシフィック (ハイデラバード)	950823858135
eu-south-2	欧州 (スペイン)	919611009337
eu-central-2	欧州 (チューリッヒ)	529164026651
ap-southeast-4	アジアパシフィック (メルボルン)	251357961535
il-central-1	イスラエル (テルアビブ)	870907303882

b. テンプレートをダウンロードする

次のコマンドで、適切なパブリックキー、x86_64 RPM の署名、arm64 RPM の署名、Amazon S3 バケットでホストされている RPM スクリプトへの対応するアクセスリンクをダウンロードするには、アカウント ID を適切な AWS アカウント ID に、リージョンを現在のリージョンに置き換えてください。

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/
x86_64/amazon-guardduty-agent-1.2.0.x86_64.rpm ./amazon-guardduty-
agent-1.2.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/
x86_64/amazon-guardduty-agent-1.2.0.x86_64.sig ./amazon-guardduty-
agent-1.2.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/
publickey.pem ./publickey.pem
```

c. パブリックキーをインポートする

次のコマンドを使用して、パブリックキーをデータベースにインポートします。

```
gpg --import publickey.pem
```

gpg はインポートの成功を示しています。

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. 署名を検証する

次のコマンドを使用して署名を確認します。

```
gpg --verify amazon-guardduty-agent-1.2.0.x86_64.sig amazon-guardduty-
agent-1.2.0.x86_64.rpm
```

検証に成功すると、次の結果のようなメッセージが表示されます。これで、RPM を使用して GuardDuty セキュリティエージェントのインストールに進むことができます。

出力例:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

検証に失敗した場合は、RPM の署名が改ざんされている可能性があることを意味します。パブリックキーをデータベースから削除して、検証プロセスを再試行する必要があります。

例 :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

次のコマンドを使用して、データベースからパブリックキーを削除します。

```
gpg --delete-keys AwsGuardDuty
```

次に、検証プロセスをもう一度試してください。

2. 「Linux または macOS から SSH で接続する」。
3. 次のコマンドを使用して、 GuardDuty セキュリティエージェントをインストールします。

```
sudo rpm -ivh amazon-guardduty-agent-1.2.0.x86_64.rpm
```

4. GuardDuty エージェントのインストールが正常かどうかを検証します。これらの手順の詳細については、「 GuardDuty セキュリティエージェントのインストールステータスの検証」を参照してください。

Debian installation

> **Important**
>
> マシンにインストールする前に、 GuardDuty セキュリティエージェントの Debian 署名を確認することをお勧めします。

1. GuardDuty セキュリティエージェントの Debian 署名を検証する

   a. 適切なパブリックキー、amd64 Debian パッケージの署名、arm64 Debian パッケージの署名、および Amazon S3 バケットでホストされている Debian スクリプトへの対応するアクセスリンク用のテンプレートを準備する

   次のテンプレートで、、 AWS アカウント ID AWS リージョン、および GuardDuty エージェントバージョンの値に置き換えて、Debian パッケージスクリプトにアクセスします。

   - パブリックキー :

   ```
   s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/
   publickey.pem
   ```

   - GuardDuty セキュリティエージェント Debian 署名 :

amd64 の署名

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/amd64/
amazon-guardduty-agent-1.2.0.amd64.sig
```

arm64 の署名

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/arm64/
amazon-guardduty-agent-1.2.0.arm64.sig
```

- Amazon S3 バケット の Debian スクリプトへのリンクにアクセスします。

  amd64 のアクセスリンク

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/amd64/
  amazon-guardduty-agent-1.2.0.amd64.deb
  ```

  arm64 のアクセスリンク

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/arm64/
  amazon-guardduty-agent-1.2.0.arm64.deb
  ```

AWS リージョン	リージョン名	AWS アカウント ID
eu-west-1	欧州 (アイルランド)	694911143906
us-east-1	米国東部 (バージニア北部)	593207742271
us-west-2	米国西部 (オレゴン)	733349766148
eu-west-3	欧州 (パリ)	665651866788
us-east-2	米国東部 (オハイオ)	307168627858
eu-central-1	欧州 (フランクフルト)	323658145986
ap-northeast-2	アジアパシフィック (ソウル)	914738172881

eu-north-1	欧州 (ストックホルム)	591436053604
ap-east-1	アジアパシフィック (香港)	258348409381
me-south-1	中東 (バーレーン)	536382113932
eu-west-2	欧州 (ロンドン)	892757235363
ap-northeast-1	アジアパシフィック (東京)	533107202818
ap-southeast-1	アジアパシフィック (シンガポール)	174946120834
ap-south-1	アジアパシフィック (ムンバイ)	251508486986
ap-southeast-3	アジアパシフィック (ジャカルタ)	510637619217
sa-east-1	南米 (サンパウロ)	758426053663
ap-northeast-3	アジアパシフィック (大阪)	273192626886
eu-south-1	欧州 (ミラノ)	266869475730
af-south-1	アフリカ (ケープタウン)	197869348890
ap-southeast-2	アジアパシフィック (シドニー)	005257825471
me-central-1	中東 (アラブ首長国連邦)	000014521398
us-west-1	米国西部 (北カリフォルニア)	684579721401
ca-central-1	カナダ (中部)	354763396469
ca-west-1	カナダ西部 (カルガリー)	339712888787

ap-south-2	アジアパシフィック (ハイデラバード)	950823858135
eu-south-2	欧州 (スペイン)	919611009337
eu-central-2	欧州 (チューリッヒ)	529164026651
ap-southeast-4	アジアパシフィック (メルボルン)	251357961535
il-central-1	イスラエル (テルアビブ)	870907303882

b. ダウンロードに適したパブリックキー、amd64 の署名、arm64 の署名、および Amazon S3 バケットでホストされている Debian スクリプトへの対応するアクセスリンクをダウンロードします。

次のコマンドで、アカウント ID を適切な AWS アカウント ID に置き換え、リージョンを現在のリージョンに置き換えます。

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/
amd64/amazon-guardduty-agent-1.2.0.amd64.deb ./amazon-guardduty-
agent-1.2.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/
amd64/amazon-guardduty-agent-1.2.0.amd64.sig ./amazon-guardduty-
agent-1.2.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/
publickey.pem ./publickey.pem
```

c. プライベートキーをデータベースにインポートします。

```
gpg --import publickey.pem
```

gpg はインポートの成功を示しています。

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. 署名を検証する

```
gpg --verify amazon-guardduty-agent-1.2.0.amd64.sig amazon-guardduty-
agent-1.2.0.amd64.deb
```

検証に成功すると、次のようなメッセージが表示されます。

出力例:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

これで、Debian を使用して GuardDuty セキュリティエージェントのインストールに進むことができます。

ただし、検証に失敗した場合、Debian パッケージの署名が改ざんされた可能性があります。

例：

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

次のコマンドを使用して、データベースからパブリックキーを削除します。

```
gpg --delete-keys AwsGuardDuty
```

次に、検証プロセスを再試行してください。

2. 「Linux または macOS から SSH で接続する」。
3. 次のコマンドを使用して、 GuardDuty セキュリティエージェントをインストールします。

```
sudo dpkg -i amazon-guardduty-agent-1.2.0.amd64.deb
```

4. GuardDuty エージェントのインストールが正常かどうかを検証します。これらの手順の詳細については、「 GuardDuty セキュリティエージェントのインストールステータスの検証」を参照してください。

メモリ不足エラー

Amazon EC2 GuardDuty のセキュリティエージェントを手動でインストールまたは更新する際にout-of-memoryエラーが発生した場合は、「」を参照してくださいメモリ不足の問題のトラブルシューティング。

GuardDuty セキュリティエージェントのインストールステータスの検証

GuardDuty セキュリティエージェントが正常かどうかを検証するには

1. 「Linux または macOS から SSH で接続する」。
2. 次のコマンドを実行して、 GuardDuty セキュリティエージェントのステータスを確認します。

```
sudo systemctl status amazon-guardduty-agent
```

セキュリティエージェントのインストールログを表示する場合は、 で確認できます/var/log/amzn-guardduty-agent/。

ログを表示するには、 を実行しますsudo journalctl -u amazon-guardduty-agent。

GuardDuty セキュリティエージェントの手動更新

Run コマンド を使用して、 GuardDuty セキュリティエージェントを更新できます。 GuardDuty セキュリティエージェントのインストールに使用したのと同じ手順を実行できます。

セキュリティエージェントの手動アンインストール

このセクションでは、Amazon EC2 リソースから GuardDuty セキュリティエージェントをアンインストールする方法について説明します。Runtime Monitoring をさらに無効にする場合は、「」を参照してください無効化の影響。

方法 1 - Run Command を使用する

Run コマンドを使用して GuardDuty セキュリティエージェントをアンインストールするには

1. GuardDuty セキュリティエージェントは、「 AWS Systems Manager ユーザーガイド」のAWS Systems Manager 「Run Command」で指定されている手順に従ってアンインストールできます。パラメータで Uninstall アクションを使用して、 GuardDuty セキュリティエージェントをアンインストールします。

[ターゲット] セクションで、セキュリティエージェントをアンインストールする Amazon EC2 インスタンスにのみ影響があることを確認してください。

次の GuardDuty ドキュメントとディストリビューターを使用します。

- ドキュメント名: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
- ディストリビューター: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

2. すべての詳細を入力した後、[実行する] を選択すると、対象の Amazon EC2 インスタンスにデプロイされたセキュリティエージェントが削除されます。

   Amazon VPC エンドポイント設定を削除するには、Runtime Monitoring と Amazon EKS Runtime Monitoring の両方を無効にする必要があります。

方法 2 - Linux パッケージマネージャーを使用する

1. 「Linux または macOS から SSH で接続する」。
2. アンインストールするコマンド

   次のコマンドは、接続先の Amazon EC2 インスタンスから GuardDuty セキュリティエージェントをアンインストールします。

   - RPM の場合:

     ```
     sudo rpm -e amazon-guardduty-agent
     ```

   - Debian の場合：

     ```
     sudo dpkg --purge amazon-guardduty-agent
     ```

   コマンドを実行した後、コマンドに関連付けられたログを確認することもできます。

Amazon VPC エンドポイントの削除

Runtime Monitoring を無効にしたり、アカウントの GuardDuty セキュリティエージェントをアンインストールしたりする場合は、手動で作成された Amazon VPC エンドポイントを削除することもできます (Amazon VPC エンドポイントの手動作成)。

コンソールを使用して、Amazon VPC エンドポイントを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Endpoints] (エンドポイント) を選択します。
3. Runtime Monitoring を有効化した時点で手動で作成されたエンドポイントを選択します。
4. [Actions] (アクション)、[Delete VPC endpoints] (VPC エンドポイントを削除) の順に選択します。
5. 確認を求められたら、**delete** をクリックします。
6. [削除] を選択します。

を使用して Amazon VPC エンドポイントを削除するには AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- Remove-EC2VpcEndpoint コマンドレット (Tools for Windows PowerShell)

Fargate の自動セキュリティエージェントの管理 (Amazon ECS のみ)

スタンドアロンアカウントの GuardDuty エージェントの設定

現在、Runtime Monitoring は、 を介してのみ Amazon ECS クラスター (AWS Fargate) のセキュリティエージェントの管理をサポートしています GuardDuty。Amazon ECS クラスターでのセキュリティエージェントの手動管理はサポートされていません。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[Runtime Monitoring] を選択します。
3. [設定] タブ:

   a. すべての Amazon ECS クラスターの自動エージェント設定を管理するには (アカウントレベル)

      の「自動エージェント設定」セクションの「有効化」を選択します AWS Fargate (ECS のみ)。新しい Fargate Amazon ECS タスクが起動 GuardDuty すると、 はセキュリティエージェントのデプロイを管理します。

- [保存] を選択します。

b. Amazon ECS クラスターの一部を除外して自動エージェント設定を管理するには (クラスターレベル)

i. すべてのタスクを除外する Amazon ECS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged–false` である必要があります。

ii. 信頼できるエンティティ以外は、これらのタグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
```

```
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. [設定] タブの [自動エージェント設定] セクションで [有効化] を選択します。

> **Note**
>
> アカウントの GuardDuty エージェント自動管理を有効にする前に、必ず Amazon ECS クラスターに除外タグを追加してください。追加しないと、セキュリティエージェントは対応する Amazon ECS クラスター内で起動されるすべてのタスクにデプロイされます。

除外されていない Amazon ECS クラスターの場合、 GuardDuty はサイドカーコンテナ内のセキュリティエージェントのデプロイを管理します。

iv. [保存] を選択します。

c. Amazon ECS クラスターの一部を含めて自動エージェント設定を管理するには (クラスターレベル)

i. すべてのタスクを含む Amazon ECS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged–true` である必要があります。

ii. 信頼できるエンティティ以外は、これらのタグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

マルチアカウント環境用の GuardDuty エージェントの設定

マルチアカウント環境では、委任された GuardDuty 管理者アカウントのみが、メンバーアカウントの自動エージェント設定を有効または無効にし、組織内のメンバーアカウントに属する Amazon ECS クラスターの自動エージェント設定を管理できます。 GuardDuty メンバーアカウントはこの設定を変更できません。委任 GuardDuty 管理者アカウントは、 を使用してメンバーアカウントを管理します AWS Organizations。マルチアカウント環境の詳細については、「 での複数のアカウントの管理 GuardDuty」を参照してください。

委任された GuardDuty 管理者アカウントの自動エージェント設定の有効化

Manage for all Amazon ECS clusters (account level)

Runtime Monitoring の [すべてのアカウントについて有効にする] を選択した場合、次のオプションがあります。

- 自動エージェント設定セクションで、すべてのアカウントに対して有効化を選択します。 GuardDuty は、起動されるすべての Amazon ECS タスクのセキュリティエージェントをデプロイおよび管理します。
- [アカウントを手動で設定] を選択します。

[Runtime Monitoring] セクションで [アカウントを手動で設定] を選択した場合、次の操作を行います。

1. [自動エージェント設定] セクションで [アカウントを手動で設定する] を選択します。
2. 委任された GuardDuty 管理者アカウント (このアカウント) セクションで 有効化 を選択します。

[保存] を選択します。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. この Amazon ECS クラスターに、キーと値のペアを`GuardDutyManaged-false` というタグを追加します。
2. 信頼できるエンティティ以外は、タグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。

5.

> **Note**
>
> アカウントの自動エージェント設定を有効にする前に、必ず Amazon ECS クラスターに除外タグを追加してください。追加しないと、 GuardDuty サイドカーコンテナが起動される Amazon ECS タスクのすべてのコンテナにアタッチされます。

[設定] タブの [自動エージェント設定] で [有効化] を選択します。

除外されていない Amazon ECS クラスターの場合、 GuardDuty はサイドカーコンテナ内のセキュリティエージェントのデプロイを管理します。

6. [保存] を選択します。

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. すべてのタスクを含む Amazon ECS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged–true` である必要があります。
2. 信頼できるエンティティ以外は、これらのタグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
```

```
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
```

```
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS クラスターに包含タグを使用する場合、自動 GuardDuty エージェント統合でエージェントを明示的に有効にする必要はありません。

すべてのメンバーアカウントの自動有効化

Manage for all Amazon ECS clusters (account level)

以下の手順は、[Runtime Monitoring] セクションで [すべてのアカウントで有効化] を選択したことを前提としています。

1. 自動エージェント設定セクションで、すべてのアカウントに対して有効化を選択します。GuardDuty は、起動されるすべての Amazon ECS タスクのセキュリティエージェントをデプロイおよび管理します。
2. [保存] を選択します。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. この Amazon ECS クラスターに、キーと値のペアを`GuardDutyManaged-false` というタグを追加します。
2. 信頼できるエンティティ以外は、タグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

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

```
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。
5.

> **Note**
>
> アカウントの自動エージェント設定を有効にする前に、必ず Amazon ECS クラスターに除外タグを追加してください。追加しないと、 GuardDuty サイドカーコンテナが起動される Amazon ECS タスクのすべてのコンテナにアタッチされます。

   [設定] タブで、[編集] を選択します。
6. [自動エージェント設定] セクションで [すべてのアカウントについて有効にする] を選択します。

   除外されていない Amazon ECS クラスターの場合、 GuardDuty はサイドカーコンテナ内のセキュリティエージェントのデプロイを管理します。
7. [保存] を選択します。

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Runtime Monitoring をどのように有効にするかにかかわらず、以下の手順は組織内のすべてのメンバーアカウントで選択する Amazon ECS Fargate タスクを監視するのに役立ちます。

1. [自動エージェント設定] セクションの設定はどれも有効にしないでください。Runtime Monitoring の設定は、前の手順で選択したものと同じにします。
2. [保存] を選択します。
3. 信頼できるエンティティ以外は、これらのタグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
```

```
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS クラスターに包含タグを使用する場合、GuardDuty エージェントの自動管理を明示的に有効にする必要はありません。

既存のアクティブなメンバーアカウントでエージェントの自動設定を有効にする

Manage for all Amazon ECS clusters (account level)

1. [Runtime Monitoring] ページの [設定] タブで、自動エージェント 設定の現在のステータスを表示できます。
2. [自動エージェント設定] ペイン内の [アクティブメンバーアカウント] セクションで、[アクション] を選択します。
3. [アクション] から、[すべての既存のアクティブなメンバーアカウントについて有効にする] を選択します。
4. [確認] を選択します。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. この Amazon ECS クラスターに、キーと値のペアを`GuardDutyManaged-false` というタグを追加します。
2. 信頼できるエンティティ以外は、タグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。
5.

> **Note**
>
> アカウントの自動エージェント設定を有効にする前に、必ず Amazon ECS クラスターに除外タグを追加してください。追加しないと、 GuardDuty サイドカーコンテナが起動される Amazon ECS タスクのすべてのコンテナにアタッチされます。

   [自動エージェント設定] セクションの [設定] タブから [アクティブなメンバーアカウント] で [アクション] を選択します。
6. [アクション] から、[すべてのアクティブなメンバーアカウントについて有効にする] を選択します。

   除外されていない Amazon ECS クラスターの場合、 GuardDuty はサイドカーコンテナ内のセキュリティエージェントのデプロイを管理します。
7. [確認] を選択します。

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. すべてのタスクを含む Amazon ECS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged–true` である必要があります。

2. 信頼できるエンティティ以外は、これらのタグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS クラスターに包含タグを使用する場合、[自動エージェント設定] を明示的に有効にする必要はありません。

新規メンバー用の自動エージェント設定を自動有効化

Manage for all Amazon ECS clusters (account level)

1. [Runtime Monitoring] ページで、[編集] を選択して既存の設定を更新します。
2. [自動エージェント設定] セクションで [すべてのアカウントについて有効にする] を選択します。
3. [保存] を選択します。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. この Amazon ECS クラスターに、キーと値のペアを`GuardDutyManaged-false` というタグを追加します。
2. 信頼できるエンティティ以外は、タグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
```

```
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。
5.

> **Note**
>
> アカウントの自動エージェント設定を有効にする前に、必ず Amazon ECS クラスターに除外タグを追加してください。追加しないと、 GuardDuty サイドカーコンテナが起動される Amazon ECS タスクのすべてのコンテナにアタッチされます。

   [設定] タブの [自動エージェント設定] セクションで、[新しいメンバーアカウントについて自動的に有効にする] を選択します。

   除外されていない Amazon ECS クラスターの場合、 GuardDuty はサイドカーコンテナ内のセキュリティエージェントのデプロイを管理します。
6. [保存] を選択します。

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. すべてのタスクを含む Amazon ECS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged–true` である必要があります。
2. 信頼できるエンティティ以外は、これらのタグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS クラスターに包含タグを使用する場合、[自動エージェント設定] を明示的に有効にする必要はありません。

アクティブなメンバーアカウントの自動エージェント設定を選択的に有効にする

Manage for all Amazon ECS (account level)

1. [アカウント] ページで、Runtime Monitoring 自動エージェント設定 (ECS-Fargate) を有効にするアカウントを選択します。複数のアカウントを選択できます。この手順で選択したアカウントで Runtime Monitoring が既に有効になっていることを確認してください。
2. [保護プランの編集] から、適切なオプションを選択して [Runtime Monitoring 自動エージェントを設定 (ECS-Fargate)] を有効にします。
3. [確認] を選択します。

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. この Amazon ECS クラスターに、キーと値のペアを`GuardDutyManaged-false` というタグを追加します。

2. 信頼できるエンティティ以外は、タグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。
5.

> **Note**
>
> アカウントの GuardDuty エージェント自動管理を有効にする前に、必ず Amazon ECS クラスターに除外タグを追加してください。追加しないと、 GuardDutyサイドカーコンテナが起動される Amazon ECS タスク内のすべてのコンテナにアタッチされます。

[アカウント] ページで、Runtime Monitoring 自動エージェント設定 (ECS-Fargate) を有効にするアカウントを選択します。複数のアカウントを選択できます。この手順で選択したアカウントで Runtime Monitoring が既に有効になっていることを確認してください。

除外されていない Amazon ECS クラスターの場合、 GuardDuty はサイドカーコンテナ内のセキュリティエージェントのデプロイを管理します。

6. [保護プランの編集] から、適切なオプションを選択して [Runtime Monitoring 自動エージェントを設定 (ECS-Fargate)] を有効にします。
7. [保存] を選択します。

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 監視する Amazon ECS クラスターを含む選択したアカウントで、[自動エージェント設定] (または [Runtime Monitoring 自動エージェント設定 (ECS-Fargate)]) を有効にしていないことを確認してください。
2. すべてのタスクを含む Amazon ECS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged–true` である必要があります。
3. 信頼できるエンティティ以外は、これらのタグを変更しないようにしてください。「AWS Organizations ユーザーガイド」の「認められている原則による場合を除き、タグが変更されないようにする」に記載されているポリシーが、ここに適用できるように変更されました。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Amazon ECS クラスターに包含タグを使用する場合、[自動エージェント設定] を明示的に有効にする必要はありません。

Amazon EKS クラスターのセキュリティエージェントの自動管理

スタンドアロンアカウント用の自動エージェントの設定

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[Runtime Monitoring] を選択します。
3. [設定]タブで[有効にする]を選択し、アカウントの自動エージェント設定を有効にします。

GuardDuty セキュリティエージェントをデプロイするための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty (すべての EKS クラスターのモニタリング)	1. 自動エージェント設定セクションの「有効化」を選択します。 GuardDuty は、アカウント内のすべての既存および潜在的に新しい EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 2. [保存] を選択します。

GuardDuty セキュリティエージェントをデプロイするための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	次の手順から、該当するシナリオを 1 つ選択してください。 GuardDuty セキュリティエージェントがこのクラスターにデプロイされていない場合に EKS クラスターをモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *`ec2:CreateTags`* を `eks:TagResource` に置き換えます。 • *`ec2:DeleteTags`* を `eks:UntagResource` に置き換えます。 • *`access-project`* を `GuardDutyManaged` に置き換えます。 • *`123456789012`* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。

GuardDuty セキュリティエージェントをデプロイするための推奨アプローチ	ステップ

```
"aws:PrincipalArn":["arn:aws:iam::12
3456789012:role/org-admins/iam-
admin", "arn:aws:iam::123456789012:
role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/ia
m-admin"]
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。

> **Note**
>
> アカウントの GuardDuty エージェント自動管理を有効にする前に、必ず EKS クラスターに除外タグを追加してください。追加しないと、 GuardDuty セキュリティエージェントはアカウント内のすべての EKS クラスターにデプロイされます。

5. 設定タブで、GuardDuty エージェント管理セクションの有効化を選択します。

   モニタリングから除外されていない EKS クラスターの場合、 GuardDuty は GuardDuty セキュリティエージェントのデプロイと更新を管理します。
6. [保存] を選択します。

GuardDuty セキュリティエージェントをデプロイするための推奨アプローチ	ステップ
	GuardDuty セキュリティエージェントが既にこのクラスターにデプロイされた後、EKS クラスターをモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 このステップの後、 はこのクラスターのセキュリティエージェントを更新 GuardDuty しません。ただし、セキュリティエージェントはデプロイされたままになり GuardDuty 、この EKS クラスターからランタイムイベントを受信し続けます。これにより、使用統計に影響を与える可能性があります。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を `eks:TagResource` に置き換えます。 • *ec2:DeleteTags* を `eks:UntagResource` に置き換えます。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

GuardDuty セキュリティエージェントをデプロイするための推奨アプローチ	ステップ
	信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. このクラスターからのランタイムイベントの受信を停止するには、デプロイされたセキュリティエージェントをこの EKS クラスターから削除する必要があります。デプロイされたセキュリティエージェントを削除する方法の詳細については、「リソースの無効化とクリーンアップの影響」を参照してください。

GuardDuty セキュリティエージェントをデプロイするための推奨アプローチ	ステップ
包含タグを使用した選択的な EKS クラスターのモニタリング	1. 必ず [自動エージェント設定] セクションで [無効化] を選択してください。Runtime Monitoring は有効のままにします。 2. [保存] を選択します。 3. キーを `GuardDutyManaged` 、値を `true` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 GuardDuty は、モニタリングする選択的な EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 4. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *`ec2:CreateTags`* を `eks:TagResource` に置き換えます。 • *`ec2:DeleteTags`* を `eks:UntagResource` に置き換えます。 • *`access-project`* を `GuardDutyManaged` に置き換えます。 • *`123456789012`* を信頼されたエンティティの AWS アカウント ID に置き換えます。

GuardDuty セキュリティエージェントをデプロイするための推奨アプローチ	ステップ
	信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
エージェントの手動管理	1. 必ず [自動エージェント設定] セクションで [無効化] を選択してください。Runtime Monitoring は有効のままにします。 2. [保存] を選択します。 3. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

マルチアカウント環境の自動エージェントの設定

マルチアカウント環境では、委任された GuardDuty 管理者アカウントのみが、メンバーアカウントの自動エージェント設定を有効または無効にし、組織内のメンバーアカウントに属する EKS クラスターの自動エージェントを管理できます。 GuardDuty メンバーアカウントは、自分のアカウントからこの設定を変更することはできません。委任 GuardDuty 管理者アカウントは、 を使用してメンバーアカウントを管理します AWS Organizations。マルチアカウント環境の詳細については、「複数のアカウントの管理」を参照してください。

委任された GuardDuty 管理者アカウントの自動エージェント設定の設定

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty (すべての EKS クラスターのモニタリング)	[Runtime Monitoring] セクションで [すべてのアカウントについて有効にする] を選択した場合、次のオプションがあります。 • 自動エージェント設定セクションで、すべてのアカウントに対して有効化を選択します。 GuardDuty は、委任された GuardDuty 管理者アカウントに属するすべての EKS クラスターと、組織内のすべての既存および潜在的に新しいメンバーアカウントに属するすべての EKS クラスターに対して、セキュリティエージェントをデプロイおよび管理します。 • [アカウントを手動で設定] を選択します。 [Runtime Monitoring] セクションで [アカウントを手動で設定] を選択した場合、次の操作を行います。 1. [自動エージェント設定] セクションで [アカウントを手動で設定する] を選択します。 2. 委任 GuardDuty 管理者アカウント (このアカウント) セクションで 有効化 を選択します。 [保存] を選択します。
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	次の手順から、該当するシナリオを 1 つ選択してください。 セキュリティエージェントがこのクラスターにデプロイされていない場合に GuardDuty EKS クラスターをモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ

Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。

2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。

   - *ec2:CreateTags* を に置き換えますeks:TagResource 。
   - *ec2:DeleteTags* を に置き換えますeks:UntagResource 。
   - *access-project* を GuardDutyManaged に置き換えます。
   - *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

     信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。

     ```
     "aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
     ```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ

> **Note**
>
> アカウントの GuardDuty エージェント自動管理を有効にする前に、必ず EKS クラスターに除外タグを追加してください。追加しないと、 GuardDuty セキュリティエージェントはアカウント内のすべての EKS クラスターにデプロイされます。

5. 設定タブで、GuardDuty エージェント管理セクションの有効化を選択します。

   モニタリングから除外されていない EKS クラスターの場合、GuardDuty は GuardDuty セキュリティエージェントのデプロイと更新を管理します。
6. [保存] を選択します。

セキュリティエージェントがこのクラスターにデプロイされたときに EKS クラスターを GuardDutyモニタリングから除外するには

1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。

   Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。
2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。

   - *`ec2:CreateTags`* を に置き換えます`eks:TagResource` 。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ

- *ec2:DeleteTags* を に置き換えますeks:Untag Resource 。
- *access-project* を GuardDutyManaged に置き換えます。
- *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

  信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. この EKS クラスターで自動エージェントを有効にしていた場合、このステップの後、 GuardDuty はこのクラスターのセキュリティエージェントを更新しません。ただし、セキュリティエージェントはデプロイされたままになり GuardDuty 、この EKS クラスターからランタイムイベントを受信し続けます。これにより、使用統計に影響を与える可能性があります。

   このクラスターからのランタイムイベントの受信を停止するには、デプロイされたセキュリティエージェントをこの EKS クラスターから削除する必要があります。デプロイされたセキュリティエージェントを削除する方法の詳細については、「リソースの無効化とクリーンアップの影響」を参照してください。
4. この EKS クラスター GuardDuty のセキュリティエージェントを手動で管理していた場合は、「」を参照してくださいリソースの無効化とクリーンアップの影響。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
包含タグを使用した選択的な EKS クラスターのモニタリング	Runtime Monitoring をどのように有効にするかにかかわらず、以下のステップはアカウント内の選択的な EKS クラスターをモニタリングするために役立ちます。 1. 自動エージェント設定セクションで、委任 GuardDuty 管理者アカウント (このアカウント) の無効化を必ず選択してください。Runtime Monitoring の設定は、前のステップで設定したものと同じにします。 2. [保存] を選択します。 3. キーを `GuardDutyManaged` 、値を `true` として、EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 GuardDuty は、モニタリングする選択的な EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 4. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *`ec2:CreateTags`* を `eks:TagResource` に置き換えます。 • *`ec2:DeleteTags`* を `eks:UntagResource` に置き換えます。 • *`access-project`* を `GuardDutyManaged` に置き換えます。 • *`123456789012`* を信頼されたエンティティの AWS アカウント ID に置き換えます。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
	信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
GuardDuty セキュリティエージェントを手動で管理する	Runtime Monitoring をどのように有効にするかにかかわらず、EKS クラスターのセキュリティエージェントを手動で管理できます。 1. 自動エージェント設定セクションで、委任 GuardDuty 管理者アカウント (このアカウント) の無効化を必ず選択してください。Runtime Monitoring の設定は、前のステップで設定したものと同じにします。 2. [保存] を選択します。 3. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

すべてのメンバーアカウントの自動エージェントを自動で有効にする

> **Note**
>
> メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty (すべての EKS クラスターのモニタリング)	このトピックは、すべてのメンバーアカウントの Runtime Monitoring を有効にするためのものです。そのため、以下のステップでは、[Runtime Monitoring] セクションで [すべてのアカウントについて有効にする] を選択していることを前提としています。 1. 自動エージェント設定セクションのすべてのアカウントに対して有効化を選択します。 GuardDuty は、委任された GuardDuty 管理者アカウントに属するすべての EKS クラスターと、組織内のすべての既存および潜在的に新しいメンバーアカウントに属するすべての EKS クラスターに対して、セキュリティエージェントをデプロイおよび管理します。 2. [保存] を選択します。
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	次の手順から、該当するシナリオを 1 つ選択してください。 セキュリティエージェントがこのクラスターにデプロイされていない場合に GuardDuty EKS クラスターをモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *`ec2:CreateTags`* を に置き換えます`eks:TagResource` 。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ

- *ec2:DeleteTags* を に置き換えますeks:Untag Resource 。
- *access-project* を GuardDutyManaged に置き換えます。
- *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

  信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。

> **Note**
>
> アカウントの自動エージェントを有効にする前に、必ず EKS クラスターに除外タグを追加してください。追加しないと、 GuardDuty セキュリティエージェントはアカウント内のすべての EKS クラスターにデプロイされます。

5. [設定] タブの [Runtime Monitoring 設定] セクションで [編集] を選択します。
6. [自動エージェント設定] セクションで [すべてのアカウントについて有効にする] を選択します。モニタリングから除外されていない EKS クラスターの場合、 GuardDuty は GuardDuty セキュリティエージェントのデプロイと更新を管理します。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
	7. [保存] を選択します。 セキュリティエージェントがこのクラスターにデプロイされたときに EKS クラスターを GuardDutyモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 2. この EKS クラスターで自動エージェント設定を有効にしていた場合、このステップの後、 GuardDuty はこのクラスターのセキュリティエージェントを更新しません。ただし、セキュリティエージェントはデプロイされたままになり GuardDuty 、この EKS クラスターからランタイムイベントを受信し続けます。これにより、使用統計に影響を与える可能性があります。 このクラスターからのランタイムイベントの受信を停止するには、デプロイされたセキュリティエージェントをこの EKS クラスターから削除する必要があります。デプロイされたセキュリティエージェントを削除する方法の詳細については、「リソースの無効化とクリーンアップの影響」を参照してください。 3. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えます`eks:TagResource` 。 • *ec2:DeleteTags* を に置き換えます`eks:UntagResource` 。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ

- *access-project* を GuardDutyManaged に置き換えます。
- *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

  信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

4. この EKS クラスター GuardDuty のセキュリティエージェントを手動で管理していた場合は、「」を参照してくださいリソースの無効化とクリーンアップの影響。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
包含タグを使用した選択的な EKS クラスターのモニタリング	Runtime Monitoring をどのように有効にするかにかかわらず、以下のステップは組織内のすべてのメンバーアカウントの選択的な EKS クラスターをモニタリングするために役立ちます。 1. [自動エージェント設定] セクションの設定はどれも有効にしないでください。Runtime Monitoring の設定は、前のステップで設定したものと同じにします。 2. [保存] を選択します。 3. キーを `GuardDutyManaged` 、値を `true` として、EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 GuardDuty は、モニタリングする選択的な EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 4. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *`ec2:CreateTags`* を `eks:TagResource` に置き換えます。 • *`ec2:DeleteTags`* を `eks:UntagResource` に置き換えます。 • *`access-project`* を `GuardDutyManaged` に置き換えます。 • *`123456789012`* を信頼されたエンティティの AWS アカウント ID に置き換えます。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
	信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
GuardDuty セキュリティエージェントを手動で管理する	Runtime Monitoring をどのように有効にするかにかかわらず、EKS クラスターのセキュリティエージェントを手動で管理できます。 1. [自動エージェント設定] セクションの設定はどれも有効にしないでください。Runtime Monitoring の設定は、前のステップで設定したものと同じにします。 2. [保存] を選択します。 3. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

すべての既存のアクティブなメンバーアカウントの自動エージェントを有効にする

> **Note**
>
> メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

組織内の既存のアクティブなメンバーアカウントの GuardDuty セキュリティエージェントを管理するには

- が組織内の既存のアクティブなメンバーアカウントに属する EKS クラスターからランタイムイベント GuardDuty を受信するには、これらの EKS クラスター GuardDuty のセキュリティエージェントを管理するための推奨アプローチを選択する必要があります。上記の各アプローチの詳

細については、「セキュリティエージェントを管理する GuardDutyためのアプローチ」を参照してください。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty (すべての EKS クラスターのモニタリング)	既存のすべてのアクティブなメンバーアカウントのすべての EKS クラスターをモニタリングするには 1. [Runtime Monitoring] ページの [設定] タブで、自動エージェント 設定の現在のステータスを表示できます。 2. [自動エージェント設定] ペイン内の [アクティブなメンバーアカウント] セクションで、[アクション] を選択します。 3. [アクション] から、[すべての既存のアクティブなメンバーアカウントについて有効にする] を選択します。 4. [確認] を選択します。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	次の手順から、該当するシナリオを 1 つ選択してください。 GuardDuty セキュリティエージェントがこのクラスターにデプロイされていない場合に EKS クラスターをモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *`ec2:CreateTags`* を `eks:TagResource` に置き換えます。 • *`ec2:DeleteTags`* を `eks:UntagResource` に置き換えます。 • *`access-project`* を `GuardDutyManaged` に置き換えます。 • *`123456789012`* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ

```
"aws:PrincipalArn":["arn:aws:iam::12
3456789012:role/org-admins/iam-
admin", "arn:aws:iam::123456789012:
role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/ia
m-admin"]
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
4. ナビゲーションペインで、[Runtime Monitoring] を選択します。

> **Note**
>
> アカウントの自動エージェント設定を有効にする前に、必ず EKS クラスターに除外タグを追加してください。追加しないと、GuardDuty セキュリティエージェントはアカウント内のすべての EKS クラスターにデプロイされます。

5. [自動エージェント設定] ペイン内の [設定] タブから、[アクティブなメンバーアカウント] で、[アクション] を選択します。
6. [アクション] から、[すべてのアクティブなメンバーアカウントについて有効にする] を選択します。
7. [確認] を選択します。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	GuardDuty セキュリティエージェントが既にこのクラスターにデプロイされた後に EKS クラスターをモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 このステップの後、 はこのクラスターのセキュリティエージェントを更新 GuardDuty しません。ただし、セキュリティエージェントはデプロイされたままになり GuardDuty 、この EKS クラスターからランタイムイベントを受信し続けます。これにより、使用統計に影響を与える可能性があります。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えます `eks:TagResource` 。 • *ec2:DeleteTags* を に置き換えます `eks:UntagResource` 。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. セキュリティエージェントの管理方法 (GuardDuty または手動) にかかわらず、このクラスターからのランタイムイベントの受信を停止するには、デプロイされたセキュリティエージェントをこの EKS クラスターから削除する必要があります。デプロイされたセキュリティエージェントを削除する方法の詳細については、「リソースの無効化とクリーンアップの影響」を参照してください。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
包含タグを使用した選択的な EKS クラスターのモニタリング	1. [アカウント] ページで、Runtime Monitoring を有効にした後は、[Runtime Monitoring 自動エージェント設定] を有効にしないでください。 2. モニタリングする選択したアカウントに属する EKS クラスターにタグを追加します。タグのキーと値のペアは `GuardDutyManaged -true` である必要があります。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 GuardDuty は、モニタリングする選択的な EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 3. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を `eks:TagResource` に置き換えます。 • *ec2:DeleteTags* を `eks:UntagResource` に置き換えます。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
GuardDuty セキュリティエージェントを手動で管理する	1. [自動エージェント設定] セクションで [有効化] を選択しないようにしてください。Runtime Monitoring は有効のままにします。 2. [保存] を選択します。 3. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

新規メンバー用の自動エージェント設定を自動有効化

セキュリティエージェントを管理する GuardDutyための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty (すべての EKS クラスターのモニタリング)	1. [Runtime Monitoring] ページで、[編集] を選択して既存の設定を更新します。 2. [自動エージェント設定] セクションで [すべてのアカウントについて有効にする] を選択します。 3. [保存] を選択します。

セキュリティエージェントを管理する GuardDutyための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	次の手順から、該当するシナリオを 1 つ選択してください。 セキュリティエージェントがこのクラスターにデプロイされていない場合に GuardDuty EKS クラスターをモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を `eks:TagResource` に置き換えます。 • *ec2:DeleteTags* を `eks:UntagResource` に置き換えます。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-`

セキュリティエージェントを管理する GuardDutyための推奨アプローチ	ステップ
	admins/iam-admin", "arn:aws:iam::1234 56789012:role/org-admins/iam-admin"]
	3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。 4. ナビゲーションペインで、[Runtime Monitoring] を選択します。 **Note** アカウントの自動エージェント設定を有効にする前に、必ず EKS クラスターに除外タグを追加してください。追加しないと、 GuardDuty セキュリティエージェントがアカウント内のすべての EKS クラスターにデプロイされます。 5. 設定 タブで、GuardDuty エージェント管理セクションの新規メンバーアカウントに対して自動的に有効にするを選択します。 モニタリングから除外されていない EKS クラスターの場合、 GuardDuty は GuardDuty セキュリティエージェントのデプロイと更新を管理します。 6. [保存] を選択します。
	セキュリティエージェントがこのクラスターにデプロイされたときに EKS クラスターを GuardDutyモニタリングから除外するには 1. GuardDuty セキュリティエージェントを で管理 GuardDuty するか、手動で管理するかにかかわらず、キーを に、`GuardDutyManaged` 値を として、この EKS クラスターにタグを追加します`false`。

セキュリティエージェントを管理する GuardDutyための推奨アプローチ	ステップ
	Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 この EKS クラスターで自動エージェントを有効にしていた場合、このステップの後、 GuardDuty はこのクラスターのセキュリティエージェントを更新しません。ただし、セキュリティエージェントはデプロイされたままになり GuardDuty 、この EKS クラスターからランタイムイベントを受信し続けます。これにより、使用統計に影響を与える可能性があります。 このクラスターからのランタイムイベントの受信を停止するには、デプロイされたセキュリティエージェントをこの EKS クラスターから削除する必要があります。デプロイされたセキュリティエージェントを削除する方法の詳細については、「リソースの無効化とクリーンアップの影響」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えますeks:TagResource 。 • *ec2:DeleteTags* を に置き換えますeks:UntagResource 。 • *access-project* を GuardDutyManaged に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

セキュリティエージェントを管理する GuardDutyための推奨アプローチ	ステップ
	信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. この EKS クラスター GuardDuty のセキュリティエージェントを手動で管理していた場合は、「」を参照してくださいリソースの無効化とクリーンアップの影響。

セキュリティエージェントを管理する GuardDutyための推奨アプローチ	ステップ
包含タグを使用した選択的な EKS クラスターのモニタリング	Runtime Monitoring をどのように有効にするかにかかわらず、以下のステップは組織内の新しいメンバーアカウントの選択的な EKS クラスターをモニタリングするために役立ちます。 1. [自動エージェント設定] セクションの [新しいメンバーアカウントについて自動的に有効にする] を必ずオフにしてください。Runtime Monitoring の設定は、前のステップで設定したものと同じにします。 2. [保存] を選択します。 3. キーを `GuardDutyManaged` 、値を `true` として、EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 GuardDuty は、モニタリングする選択的な EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 4. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *`ec2:CreateTags`* を `eks:TagResource` に置き換えます。 • *`ec2:DeleteTags`* を `eks:UntagResource` に置き換えます。 • *`access-project`* を `GuardDutyManaged` に置き換えます。

セキュリティエージェントを管理する GuardDutyための推奨アプローチ	ステップ
	• *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
GuardDuty セキュリティエージェントを手動で管理する	Runtime Monitoring をどのように有効にするかにかかわらず、EKS クラスターのセキュリティエージェントを手動で管理できます。 1. [GuardDuty エージェント管理] セクションの [新しいメンバーアカウントについて自動的に有効にする] のチェックボックスを必ずオフにしてください。Runtime Monitoring の設定は、前のステップで設定したものと同じにします。 2. [保存] を選択します。 3. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

アクティブなメンバーアカウントの自動エージェントを選択的に設定する

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty (すべての EKS クラスターのモニタリング)	1. [アカウント] ページで、[自動エージェント設定] を有効にするアカウントを選択します。一度に複数のアカウントを選択することもできます。このステップで選択したアカウントで EKS Runtime Monitoring が既に有効になっていることを確認してください。 2. [保護プランの編集] から、適切なオプションを選択して [Runtime Monitoring 自動エージェント設定] を有効にします。 3. [確認] を選択します。
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	次の手順から、該当するシナリオを 1 つ選択してください。 セキュリティエージェントがこのクラスターにデプロイされていない場合に GuardDuty EKS クラスターをモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えます`eks:TagResource` 。 • *ec2:DeleteTags* を に置き換えます`eks:UntagResource` 。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ

- *access-project* を GuardDutyManaged に置き換えます。
- *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

  信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   > **Note**
   >
   > アカウントの自動エージェント設定を有効にする前に、必ず EKS クラスターに除外タグを追加してください。追加しないと、 GuardDuty セキュリティエージェントがアカウント内のすべての EKS クラスターにデプロイされます。

4. [アカウント] ページで、[エージェントの自動管理] を有効にするアカウントを選択します。一度に複数のアカウントを選択することもできます。
5. [保護プランの編集] から、適切なオプションを選択して選択したアカウントの [Runtime Monitoring 自動エージェント設定] を有効にします。

   モニタリングから除外されていない EKS クラスターの場合、GuardDuty は GuardDuty セキュリティエージェントのデプロイと更新を管理します。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
	6. [保存] を選択します。 セキュリティエージェントがこのクラスターにデプロイされたときに EKS クラスターを GuardDutyモニタリングから除外するには 1. キーを `GuardDutyManaged` 、値を `false` として、この EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 以前にこの EKS クラスターで自動エージェント設定を有効にしていた場合、このステップの後、 GuardDuty はこのクラスターのセキュリティエージェントを更新しません。ただし、セキュリティエージェントはデプロイされたままになり GuardDuty 、この EKS クラスターからランタイムイベントを受信し続けます。これにより、使用統計に影響を与える可能性があります。 このクラスターからのランタイムイベントの受信を停止するには、デプロイされたセキュリティエージェントをこの EKS クラスターから削除する必要があります。デプロイされたセキュリティエージェントを削除する方法の詳細については、「リソースの無効化とクリーンアップの影響」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えます`eks:TagResource` 。 • *ec2:DeleteTags* を に置き換えます`eks:UntagResource` 。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ

- *access-project* を GuardDutyManaged に置き換えます。
- *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。

  信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. この EKS クラスター GuardDuty のセキュリティエージェントを手動で管理していた場合は、削除する必要があります。詳細については、「リソースの無効化とクリーンアップの影響」を参照してください。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
包含タグを使用した選択的な EKS クラスターのモニタリング	Runtime Monitoring をどのように有効にするかにかかわらず、以下のステップは選択したアカウントに属する選択的な EKS クラスターをモニタリングするために役立ちます。 1. モニタリングする EKS クラスターを含む選択したアカウントについて、[Runtime Monitoring 自動エージェント設定] を有効にしていないことを確認してください。 2. キーを `GuardDutyManaged` 、値を `true` として、EKS クラスターにタグを追加します。 Amazon EKS クラスターのタグ付けの詳細については、「Amazon EKS ユーザーガイド」の「コンソールでのタグの処理」を参照してください。 タグを追加すると、 はモニタリングする選択的な EKS クラスターのセキュリティエージェントのデプロイと更新 GuardDuty を管理します。 3. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *`ec2:CreateTags`* を `eks:TagResource` に置き換えます。 • *`ec2:DeleteTags`* を `eks:UntagResource` に置き換えます。 • *`access-project`* を `GuardDutyManaged` に置き換えます。 • *`123456789012`* を信頼されたエンティティの AWS アカウント ID に置き換えます。

セキュリティエージェントを管理する GuardDuty ための推奨アプローチ	ステップ
	信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
GuardDuty セキュリティエージェントを手動で管理する	1. Runtime Monitoring の設定は、前のステップで設定したものと同じにします。選択したどのアカウントでも、[Runtime Monitoring 自動エージェント設定] を有効にしていないことを確認してください。 2. [確認] を選択します。 3. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

Amazon EKS クラスターのセキュリティエージェントの手動管理

このセクションでは、Runtime Monitoring を有効にした後に Amazon EKS アドオンエージェント (GuardDuty エージェント) を管理する方法について説明します。Runtime Monitoring を使用するには、Runtime Monitoring を有効にして Amazon EKS アドオン `aws-guardduty-agent` を設定する必要があります。これら 2 つのステップのうち 1 つだけを実行しても、潜在的な脅威 GuardDuty の検出や結果の生成には役立ちません。

GuardDuty セキュリティエージェントをデプロイするための前提条件

このセクションでは、EKS クラスターのセキュリティ GuardDuty エージェントを手動でデプロイするための前提条件について説明します。先に進む前に、アカウントに Runtime Monitoring が既に設定されていることを確認してください。Runtime Monitoring を設定しないと、 GuardDuty セキュリティエージェント (EKS アドオン) は機能しません。詳細については、「Runtime Monitoring GuardDuty の有効化」を参照してください。次のステップが完了したら、「 GuardDuty セキュリティエージェントのデプロイ」を参照してください。

任意のアクセス方法を選択して、Amazon VPC エンドポイントを作成します。

Console

VPC エンドポイントを作成する

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインの [仮想プライベートクラウド] で、[VPC] を選択します。
3. [エンドポイントの作成] を選択します。
4. [エンドポイントの作成] ページの [サービスカテゴリ] で [その他のエンドポイントサービス] を選択します。
5. [サービス名] に **com.amazonaws.*us-east-1*.guardduty-data** と入力します。

   必ず *us-east-1* を正しいリージョンに置き換えてください。これは、 AWS アカウント ID に属する EKS クラスターと同じリージョンである必要があります。
6. [サービスの確認] を選択します。
7. サービス名が正常に確認されたら、クラスターが置かれている [VPC] を選択します。次のポリシーを追加して、VPC エンドポイントの使用を指定されたアカウントのみに制限します。このポリシー下で提供されている組織 Condition を使用して、次のポリシーを更新してエンドポイントへのアクセスを制限できます。組織内の特定のアカウント ID に VPC エンドポイントサポートを提供するには、「Organization condition to restrict access to your endpoint」を参照してください。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
```

```
    "Resource": "*",
    "Effect": "Deny",
    "Principal": "*"
   }
  ]
}
```

aws:PrincipalAccount アカウント ID は、VPC と VPC エンドポイントを含むアカウントと一致する必要があります。次のリストは、VPC エンドポイントを他の AWS アカウント ID と共有する方法を示しています。

エンドポイントへのアクセスを制限する組織の条件

- VPC エンドポイントにアクセスする複数のアカウントを指定するには、"aws:PrincipalAccount": "*111122223333*"を以下に置き換えます。

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- 組織のすべてのメンバーが VPC エンドポイントにアクセスできるようにするには、"aws:PrincipalAccount": "*111122223333*" を以下に置き換えます。

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- リソースへのアクセスを組織 ID に制限するには、ResourceOrgID をポリシーに追加します。

  詳細については、ResourceOrg「 ID 」を参照してください。

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. [追加設定] で [DNS 名を有効にする] を選択します。
9. [サブネット] で、クラスターが存在するサブネットを選択します。
10. [セキュリティグループ] で、VPC (または EKS クラスター) からのインバウンドポート 443 が有効になっているセキュリティグループを選択します。インバウンドポート 443 が有効になっているセキュリティグループがまだない場合は、セキュリティグループを作成します。

VPC (またはクラスター) へのインバウンド許可を制限する際に問題が発生した場合は、任意の IP アドレス (`0.0.0.0/0`) からのインバウンド 443 ポートをサポートします。

API/CLI

- を呼び出しますCreateVpcEndpoint。
- パラメータで以下の値を使用します。
  - [サービス名] に **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** と入力します。

    必ず *`us-east-1`* を正しいリージョンに置き換えてください。これは、 AWS アカウント ID に属する EKS クラスターと同じリージョンである必要があります。
  - DNSOptions には、プライベート DNS オプションを `true` に設定して有効にします。
- については AWS Command Line Interface、「」を参照してくださいcreate-vpc-endpoint。

Amazon EKS GuardDuty のセキュリティエージェント (アドオン) パラメータを設定する

Amazon EKS GuardDuty のセキュリティエージェントの特定のパラメータを設定できます。このサポートは、 GuardDuty セキュリティエージェントバージョン 1.5.0 以降で利用できます。最新のアドオンバージョンについては、「」を参照してくださいGuardDuty Amazon EKS クラスター用の セキュリティエージェント。

セキュリティエージェント設定スキーマを更新する理由

GuardDuty セキュリティエージェントの設定スキーマは、Amazon EKS クラスター内のすべてのコンテナで同じです。デフォルト値が関連するワークロードとインスタンスサイズと一致しない場合は、CPU 設定、メモリ設定、、`PriorityClass`および `dnsPolicy`設定を構成することを検討してください。Amazon EKS クラスターの GuardDuty エージェントを管理する方法に関係なく、これらのパラメータの既存の設定を設定または更新できます。

設定済みパラメータによるエージェント設定動作の自動

がユーザーに代わってセキュリティエージェント (EKS アドオン) GuardDuty を管理する場合、必要に応じてアドオンを更新します。 GuardDuty は設定可能なパラメータの値をデフォルト値に設定します。ただし、パラメータを希望の値に更新することはできます。これが競合につながる場合、resolveConflicts のデフォルトオプションは ですNone。

設定可能なパラメータと値

アドオンパラメータを設定する手順については、以下を参照してください。

- GuardDuty セキュリティエージェントのデプロイ または
- セキュリティエージェントの手動更新

次の表は、Amazon EKS アドオンを手動でデプロイしたり、既存のアドオン設定を更新したりするために使用できる範囲と値を示しています。

CPU 設定

パラメータ	デフォルト値	設定可能な範囲
リクエスト	200m	200 m から 10000 m の間、両方を含む
制限	1000m	

メモリ設定

パラメータ	デフォルト値	設定可能な範囲
リクエスト	256Mi	256Mi から 20000Mi の間、両方を含む
制限	1024Mi	

`PriorityClass` 設定

が Amazon EKS アドオン GuardDuty を作成すると、割り当てられた `PriorityClass`は になりますaws-guardduty-agent.priorityclass。つまり、エージェントポッドの優先度に基づいてアクションは実行されません。このアドオンパラメータは、次のいずれか`PriorityClass`のオプションを選択して設定できます。

設定可能 **PriorityClass**	**preemptionPolicy** 値	**preemptionPolicy** 説明	ポッド値
aws-guardduty-agent.priorityclass	Never	アクションなし	1000000
aws-guardduty-agent.priorityclass-high	PreemptLowerPriority	この値を割り当てると、エージェントポッド値よりも低い優先度の値で実行されているポッドが優先されます。	100000000
system-cluster-critical [1]	PreemptLowerPriority		2000000000
system-node-critical [1]	PreemptLowerPriority		2000001000

[1] Kubernetes には、 system-cluster-criticalと の 2 つのPriorityClassオプションがありますsystem-node-critical。詳細については、Kubernetes ドキュメントPriorityClassの「」を参照してください。

dnsPolicy 設定

Kubernetes がサポートする次の DNS ポリシーオプションのいずれかを選択します。設定が指定されていない場合、 ClusterFirst がデフォルト値として使用されます。

- ClusterFirst
- ClusterFirstWithHostNet
- Default

これらのポリシーの詳細については、Kubernetes ドキュメントの「ポッドの DNS ポリシー」を参照してください。

GuardDuty セキュリティエージェントのデプロイ

このセクションでは、特定の EKS クラスターに GuardDuty セキュリティエージェントを初めてデプロイする方法について説明します。このセクションに進む前に、アカウントの前提条件をセットアップし、Runtime Monitoring を有効にしていることを確認してください。Runtime Monitoring GuardDutyを有効にしない場合、セキュリティエージェント (EKS アドオン) は機能しません。

任意のアクセス方法を選択して、 GuardDuty セキュリティエージェントを初めてデプロイします。

Console

1. https://console.aws.amazon.com/eks/home#/clusters で Amazon EKS コンソールを開きます。
2. [クラスター名] を選択します。
3. [アドオン] タブを選択します。
4. [その他のアドオンを入手] を選択します。
5. アドオンの選択ページで、Amazon GuardDuty Runtime Monitoring を選択します。
6. [選択したアドオン設定の設定] ページで、デフォルトの設定を使用します。EKS アドオンのステータスがアクティベーション を必要とする場合は、アクティブ化 GuardDutyを選択します。このアクションにより、 GuardDuty コンソールが開き、アカウントの Runtime Monitoring が設定されます。
7. アカウントに Runtime Monitoring を設定したら、Amazon EKS コンソールに戻ってください。EKS アドオンの [ステータス] は、[インストール準備完了] に変わっているはずです。
8. (オプション) EKS アドオン設定スキーマの提供

   アドオンバージョン では、v1.5.0 以降を選択した場合、Runtime Monitoring は GuardDuty エージェントの特定のパラメータの設定をサポートします。パラメータ範囲の詳細については、「」を参照してくださいEKS アドオンパラメータを設定する。

   a. オプションの設定を展開して、設定可能なパラメータとその想定値と形式を表示します。
   b. パラメータを設定します。値は、 で指定された範囲内である必要がありますEKS アドオンパラメータを設定する。
   c. 変更を保存 を選択して、詳細設定に基づいてアドオンを作成します。
   d. 競合解決方法 では、パラメータの値をデフォルト以外の値に更新するときに、選択したオプションを使用して競合を解決します。リストされているオプションの詳細については、「Amazon EKS API リファレンス」のresolveConflicts」を参照してください。

9. [次へ] をクリックします。
10. [確認と作成] ページで、すべての詳細を確認し、[作成] を選択します。
11. クラスターの詳細に戻り、[リソース] タブを選択します。
12. 新しいポッドは、プレフィックス で表示できますaws-guardduty-agent。

API/CLI

Amazon EKS アドオンエージェント (aws-guardduty-agent) は、次のオプションのいずれかを使用して設定できます。

- アカウントCreateAddonに対して を実行します。
-

> **Note**
>
> アドオン で versionv1.5.0 以上を選択した場合、Runtime Monitoring は GuardDuty エージェントの特定のパラメータの設定をサポートします。詳細については、「EKS アドオンパラメータを設定する」を参照してください。

リクエストパラメータに以下の値を使用します。

- addonName に「aws-guardduty-agent」と入力します。

アドオンバージョン v1.5.0 以降でサポートされている設定可能な値を使用する場合は、次の AWS CLI 例を使用できます。赤で強調表示されているプレースホルダー値と、設定された値Example.jsonに関連付けられている を必ず置き換えてください。

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
```

```
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- サポートされている addonVersion については、「 GuardDuty セキュリティエージェントがサポートする Kubernetes バージョン」を参照してください。
- または、 を使用することもできます AWS CLI。詳細については、「create-addon」を参照してください。

セキュリティエージェントの手動更新

セキュリティエージェントを手動で管理する場合は、アカウントの GuardDuty セキュリティエージェントを更新する責任があります。新しいエージェントバージョンに関する通知については、RSS フィードを にサブスクライブできますGuardDuty エージェントリリース履歴。

セキュリティエージェントを最新バージョンに更新して、追加されたサポートと改善を活用できます。現在のエージェントバージョンが標準サポートを終了している場合は、Runtime Monitoring (または EKS Runtime Monitoring) を引き続き使用するには、現在のエージェントバージョンを更新する必要があります。リリースバージョンの詳細については、「」を参照してくださいGuardDuty Amazon EKS クラスター用の セキュリティエージェント。

前提条件

セキュリティエージェントのバージョンを更新する前に、現在使用する予定のエージェントのバージョンが Kubernetes バージョンと互換性があることを確認してください。詳細については、「 GuardDuty セキュリティエージェントがサポートする Kubernetes バージョン」を参照してください。

Console

1. https://console.aws.amazon.com/eks/home#/clusters で Amazon EKS コンソールを開きます。
2. [クラスター名] を選択します。
3. アドオン を選択します。
4. アドオン で、GuardDutyランタイムモニタリング を選択します。

5. 編集 を選択してエージェントの詳細を更新します。
6. GuardDuty ランタイムモニタリングの設定ページで、詳細を更新します。
7. (オプション) アドオン設定パラメータの更新

   EKS アドオンバージョンが 1.5.0 以降の場合は、アドオン設定を更新することもできます。

   a. オプションの設定を展開して、設定スキーマを表示します。
   b. で指定された範囲に基づいてパラメータ値を更新しますEKS アドオンパラメータを設定する。
   c. [変更を保存] を選択して更新を開始します。
   d. 競合解決方法 では、パラメータの値をデフォルト以外の値に更新するときに、選択したオプションを使用して競合を解決します。リストされているオプションの詳細については、「Amazon EKS API リファレンス」のresolveConflicts」を参照してください。

API/CLI

Amazon EKS クラスター GuardDuty のセキュリティエージェントを更新するには、「アドオンの更新」を参照してください。

> **Note**
>
> アドオン で versionv1.5.0 以上を選択した場合、Runtime Monitoring は GuardDuty エージェントの特定のパラメータの設定をサポートします。パラメータ範囲の詳細については、「」を参照してくださいEKS アドオンパラメータを設定する。

アドオンバージョン v1.5.0 以降でサポートされている設定可能な値を使用する場合は、次の AWS CLI 例を使用できます。赤で強調表示されているプレースホルダー値と、設定された値Example.jsonに関連付けられている を必ず置き換えてください。

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Example.json

```
{
```

```
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Amazon EKS アドオンバージョンが 1.5.0 以降で、アドオンスキーマを設定している場合は、クラスターに値が正しく表示されるかどうかを確認できます。詳細については、「設定スキーマの更新の検証」を参照してください。

設定スキーマの更新の検証

パラメータを設定したら、次のステップを実行して、設定スキーマが更新されていることを確認します。

1. https://console.aws.amazon.com/eks/home#/clusters で Amazon EKS コンソールを開きます。
2. ナビゲーションペインで [クラスター] を選択します。
3. クラスターページで、更新を検証するクラスター名を選択します。
4. [リソース] タブを選択します。
5. リソースタイプペインのワークロード で、 を選択しますDaemonSets。
6. を選択しますaws-guardduty-agent。
7. aws-guardduty-agent ページで、未加工ビューを選択して、フォーマットされていない JSON レスポンスを表示します。設定可能なパラメータに、指定した値が表示されていることを確認します。

確認したら、 GuardDuty コンソールに切り替えます。対応する AWS リージョン を選択し、Amazon EKS クラスターのカバレッジステータスを表示します。詳細については、「Amazon EKS クラスターのカバレッジ」を参照してください。

EKS Runtime Monitoring の設定 (API のみ)

アカウントで EKS Runtime Monitoring を設定する前に、現在使用されている Kubernetes バージョンをサポートしている検証済みプラットフォームのいずれかを使用していることを確認してください。詳細については、「アーキテクチャ要件の検証」を参照してください。

GuardDuty は、EKS Runtime Monitoring のコンソールエクスペリエンスを Runtime Monitoring に統合しました。 GuardDuty は EKS Runtime Monitoring 設定ステータスの確認と を推奨しますEKS Runtime Monitoring から Runtime Monitoring への移行。

Runtime Monitoring への移行の一環として、 を必ず に移行してくださいEKS Runtime Monitoring を無効にする。これは、後で Runtime Monitoring を無効にし、EKS Runtime Monitoring を無効にしない場合、EKS Runtime Monitoring の使用コストが引き続き発生するため、重要です。

スタンドアロンアカウントの EKS Runtime Monitoring の設定

AWS Organizations に関連するアカウントについては、「マルチアカウント環境の EKS Runtime Monitoring の設定」を参照してください。

任意のアクセス方法を選択して、アカウントのために EKS Runtime Monitoring を有効にします。

API/CLI

「セキュリティエージェントを管理する GuardDutyためのアプローチ」に基づいて、推奨アプローチを選択し、次の表に示すステップに従うことができます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty （ すべての EKS クラスターのモニタリング ）	1. ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト名を `EKS_RUNTIME_MONITORING` として、ステータスを `ENABLED` として渡して、updateDetector API を実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `ENABLED` に設定します。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	GuardDuty は、アカウント内のすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 2. または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING と EKS_ADDON_MANAGEMENT の両方を有効にします。 `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged -false` です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を `eks:TagResource` に置き換えます。 • *ec2:DeleteTags* を `eks:UntagResource` に置き換えます。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	3. **Note** STATUS の を に設定する前に、必ず EKS クラスターEKS_RUNTIME_MONITORING に除外タグを追加してくださいENABLED。追加しないと、 GuardDuty セキュリティエージェントがアカウント内のすべての EKS クラスターにデプロイされます。 ユーザー独自のリージョンレベルのディテクター ID を使用し、features オブジェクト名を EKS_RUNTIME_MONITORING として、ステータスを ENABLED として渡して、updateDetector API を実行します。 EKS_ADDON_MANAGEMENT のステータスを ENABLED に設定します。 GuardDuty は、モニタリングから除外されていないすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING と EKS_ADDON_MANAGEMENT の両方を有効にします。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
選択的な EKS クラスターのモニタリング (包含タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは GuardDutyManaged -true です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えますeks:TagResource 。 • *ec2:DeleteTags* を に置き換えますeks:UntagResource 。 • *access-project* を GuardDutyManaged に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	3. ユーザー独自のリージョンレベルのディテクター ID を使用し、features オブジェクト名を EKS_RUNTIME_MONITORING として、ステータスを ENABLED として渡して、updateDetector API を実行します。 EKS_ADDON_MANAGEMENT のステータスを DISABLED に設定します。 GuardDuty は、 GuardDutyManaged -true ペアでタグ付けされたすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING を有効にして、EKS_ADDON_MANAGEMENT を無効にしています。 `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
セキュリティエージェントの手動管理	1. ユーザー独自のリージョンレベルのディテクター ID を使用し、features オブジェクト名を EKS_RUNTIME_MONITORING として、ステータスを ENABLED として渡して、updateDetector API を実行します。 EKS_ADDON_MANAGEMENT のステータスを DISABLED に設定します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING を有効にして、EKS_ADDON_MANAGEMENT を無効にしています。 `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` 2. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

マルチアカウント環境の EKS Runtime Monitoring の設定

マルチアカウント環境では、委任された GuardDuty 管理者アカウントのみがメンバーアカウントの EKS Runtime Monitoring を有効または無効にし、組織内のメンバーアカウントに属する EKS クラス

ターの GuardDuty エージェント管理を管理できます。 GuardDuty メンバーアカウントは、自分のアカウントからこの設定を変更することはできません。委任 GuardDuty 管理者アカウントは、 を使用してメンバーアカウントを管理します AWS Organizations。マルチアカウント環境の詳細については、「複数のアカウントの管理」を参照してください。

委任 GuardDuty 管理者アカウントの EKS Runtime Monitoring の設定

任意のアクセス方法を選択して EKS Runtime Monitoring を有効にし、委任 GuardDuty 管理者アカウントに属する EKS クラスターのセキュリティエージェントを管理します GuardDuty。

API/CLI

「セキュリティエージェントを管理する GuardDutyためのアプローチ」に基づいて、推奨アプローチを選択し、次の表に示すステップに従うことができます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty（ すべての EKS クラスターのモニタリング ）	ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト名を `EKS_RUNTIME_MONITORING` として、ステータスを `ENABLED` として渡して、updateDetector API を実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `ENABLED` に設定します。 GuardDuty は、アカウント内のすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、`EKS_RUNTIME_MONITORING` と `EKS_ADDON_MANAGEMENT` の両方を有効にします。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged -false` です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を `eks:TagResource` に置き換えます。 • *ec2:DeleteTags* を `eks:UntagResource` に置き換えます。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	3. **Note** STATUS の を に設定する前に、必ず EKS クラスターEKS_RUNTIME_MONITORING に除外タグを追加してくださいENABLED。追加しないと、 GuardDuty セキュリティエージェントがアカウント内のすべての EKS クラスターにデプロイされます。 ユーザー独自のリージョンレベルのディテクター ID を使用し、features オブジェクト名を EKS_RUNTIME_MONITORING として、ステータスを ENABLED として渡して、updateDetector API を実行します。 EKS_ADDON_MANAGEMENT のステータスを ENABLED に設定します。 GuardDuty は、モニタリングから除外されていないすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING と EKS_ADDON_MANAGEMENT の両方を有効にします。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	aws guardduty update-detector --detector-id *12abc34d567e8fa901bc2d34e56789f0* --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " *ENABLED*", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " *ENABLED*"}]]'

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
選択的な EKS クラスターのモニタリング (包含タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは GuardDuty Managed -true です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えますeks:TagResource 。 • *ec2:DeleteTags* を に置き換えますeks:UntagResource 。 • *access-project* を GuardDutyManaged に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	3. ユーザー独自のリージョンレベルのディテクター ID を使用し、features オブジェクト名を EKS_RUNTIME_MONITORING として、ステータスを ENABLED として渡して、updateDetector API を実行します。 EKS_ADDON_MANAGEMENT のステータスを DISABLED に設定します。 GuardDuty は、 GuardDutyManaged -true ペアでタグ付けされたすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING を有効にして、EKS_ADDON_MANAGEMENT を無効にしています。 `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
セキュリティエージェントの手動管理	1. ユーザー独自のリージョンレベルのディテクター ID を使用し、features オブジェクト名を EKS_RUNTIME_MONITORING として、ステータスを ENABLED として渡して、updateDetector API を実行します。 EKS_ADDON_MANAGEMENT のステータスを DISABLED に設定します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING を有効にして、EKS_ADDON_MANAGEMENT を無効にしています。 `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

すべてのメンバーアカウントのために EKS Runtime Monitoring を自動的に有効にする

任意のアクセス方法を選択して、すべてのメンバーアカウントのために EKS Runtime Monitoring を有効にします。これには、委任された GuardDuty 管理者アカウント、既存のメンバーアカウント、

および組織に参加する新しいアカウントが含まれます。これらのメンバーアカウントに属する EKS クラスター GuardDuty のセキュリティエージェントを管理するための任意のアプローチを選択します。

API/CLI

「セキュリティエージェントを管理する GuardDutyためのアプローチ」に基づいて、推奨アプローチを選択し、次の表に示すステップに従うことができます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty（ すべての EKS クラスターのモニタリング ）	メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `ENABLED` に設定します。 GuardDuty は、アカウント内のすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、`EKS_RUNTIME_MONITORING` と `EKS_ADDON_MANAGEMENT` の両方を有効にします。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	Note スペースで区切られたアカウント ID のリストを渡すこともできます。 コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged -false` です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えます`eks:TagResource` 。 • *ec2:DeleteTags* を に置き換えます`eks:UntagResource` 。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** STATUS の を に設定する前に、必ず EKS クラスターEKS_RUNTIME_MONITORING に除外タグ

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	を追加してくださいENABLED。追加しないと、GuardDuty セキュリティエージェントがアカウント内のすべての EKS クラスターにデプロイされます。 ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト名を `EKS_RUNTIME_MONITORING` として、ステータスを `ENABLED` として渡して、updateDetector API を実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `ENABLED` に設定します。 GuardDuty は、モニタリングから除外されていないすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、`EKS_RUNTIME_MONITORING` と `EKS_ADDON_MANAGEMENT` の両方を有効にします。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	> **Note** スペースで区切られたアカウント ID のリストを渡すこともできます。 コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
選択的な EKS クラスターのモニタリング (包含タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは GuardDutyManaged -true です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えますeks:TagResource 。 • *ec2:DeleteTags* を に置き換えますeks:UntagResource 。 • *access-project* を GuardDutyManaged に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. ユーザー独自のリージョンレベルのディテクター ID を使用し、features オブジェクト名を EKS_RUNTIME_MONITORING として、ステータスを ENABLED として渡して、updateDetector API を実行します。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	EKS_ADDON_MANAGEMENT のステータスを DISABLED に設定します。 GuardDuty は、 GuardDutyManaged -true ペアでタグ付けされたすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING を有効にして、EKS_ADDON_MANAGEMENT を無効にしています。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** スペースで区切られたアカウント ID のリストを渡すこともできます。 コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
セキュリティエージェントの手動管理	1. ユーザー独自のリージョンレベルのディテクター ID を使用し、`features` オブジェクト名を `EKS_RUNTIME_MONITORING` として、ステータスを `ENABLED` として渡して、updateDetector API を実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `DISABLED` に設定します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンの `detectorId` を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、`EKS_RUNTIME_MONITORING` を有効にして、`EKS_ADDON_MANAGEMENT` を無効にしています。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

すべての既存のアクティブなメンバーアカウントの EKS Runtime Monitoring の設定

任意のアクセス方法を選択して EKS Runtime Monitoring を有効にし、組織内の既存のアクティブなメンバーアカウントの GuardDuty セキュリティエージェントを管理します。

API/CLI

「セキュリティエージェントを管理する GuardDutyためのアプローチ」に基づいて、推奨アプローチを選択し、次の表に示すステップに従うことができます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty（すべての EKS クラスターのモニタリング）	メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `ENABLED` に設定します。 GuardDuty は、アカウント内のすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、`EKS_RUNTIME_MONITORING` と `EKS_ADDON_MANAGEMENT` の両方を有効にします。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** スペースで区切られたアカウント ID のリストを渡すこともできます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは GuardDutyManaged -false です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えますeks:TagResource 。 • *ec2:DeleteTags* を に置き換えますeks:UntagResource 。 • *access-project* を GuardDutyManaged に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** STATUS の を に設定する前に、必ず EKS クラスターEKS_RUNTIME_MONITORING に除外タグ

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	を追加してくださいENABLED。追加しないと、GuardDuty セキュリティエージェントがアカウント内のすべての EKS クラスターにデプロイされます。 メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを実行します。 EKS_ADDON_MANAGEMENT のステータスを ENABLED に設定します。 GuardDuty は、モニタリングから除外されていないすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING と EKS_ADDON_MANAGEMENT の両方を有効にします。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	Note スペースで区切られたアカウント ID のリストを渡すこともできます。 コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
選択的な EKS クラスターのモニタリング (包含タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは GuardDutyManaged -true です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えますeks:TagResource 。 • *ec2:DeleteTags* を に置き換えますeks:UntagResource 。 • *access-project* を GuardDutyManaged に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の*###### ID* を使用し、updateMemberDetectors API オペレーションを実行します。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ

EKS_ADDON_MANAGEMENT のステータスを DISABLED に設定します。

GuardDuty は、 GuardDutyManaged -true ペアでタグ付けされたすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。

または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

次の例では、EKS_RUNTIME_MONITORING を有効にして、EKS_ADDON_MANAGEMENT を無効にしています。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " DISABLED"}] ]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
セキュリティエージェントの手動管理	1. メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `DISABLED` に設定します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、`EKS_RUNTIME_MONITORING` を有効にして、`EKS_ADDON_MANAGEMENT` を無効にしています。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

新規メンバーの EKS Runtime Monitoring を自動有効化

委任 GuardDuty 管理者アカウントは、EKS Runtime Monitoring を自動有効化し、組織に参加する新しいアカウントの GuardDuty セキュリティエージェントを管理する方法を選択できます。

API/CLI

「セキュリティエージェントを管理する GuardDutyためのアプローチ」に基づいて、推奨アプローチを選択し、次の表に示すステップに従うことができます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty（ すべての EKS クラスターのモニタリング ）	新しいアカウントの EKS Runtime Monitoring を選択的に有効にするには、自身の`###### ID` を使用し、UpdateOrganizationConfiguration API オペレーションを実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `ENABLED` に設定します。 GuardDuty は、アカウント内のすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、1 つのアカウントで `EKS_RUNTIME_MONITORING` と `EKS_ADDON_MANAGEMENT` の両方を有効にします。スペースで区切られたアカウント ID のリストを渡すこともできます。 アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	`aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged -false` です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を `eks:TagResource` に置き換えます。 • *ec2:DeleteTags* を `eks:UntagResource` に置き換えます。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	3. **Note** STATUS の を に設定する前に、必ず EKS クラスターEKS_RUNTIME_MONITORING に除外タグを追加してくださいENABLED。追加しないと、 GuardDuty セキュリティエージェントがアカウント内のすべての EKS クラスターにデプロイされます。 新しいアカウントの EKS Runtime Monitoring を選択的に有効にするには、自身の###### *ID* を使用し、UpdateOrganizationConfiguration API オペレーションを実行します。 EKS_ADDON_MANAGEMENT のステータスを ENABLED に設定します。 GuardDuty は、モニタリングから除外されていないすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、1 つのアカウントで EKS_RUNTIME_MONITORING と EKS_ADDON_MANAGEMENT の両方を有効にします。スペースで区切られたアカウント ID のリストを渡すこともできます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、ListDetectors API を実行します。 `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
選択的な EKS クラスターのモニタリング (包含タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは GuardDutyManaged -true です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えますeks:TagResource 。 • *ec2:DeleteTags* を に置き換えますeks:UntagResource 。 • *access-project* を GuardDutyManaged に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	3. 新しいアカウントの EKS Runtime Monitoring を選択的に有効にするには、自身の`###### ID` を使用し、UpdateOrganizationConfiguration API オペレーションを実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `DISABLED` に設定します。 GuardDuty は、`GuardDutyManaged -true` ペアでタグ付けされたすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、1 つのアカウントで `EKS_RUNTIME_MONITORING` を有効にし、`EKS_ADDON_MANAGEMENT` を無効にします。スペースで区切られたアカウント ID のリストを渡すこともできます。 アカウントと現在のリージョン`detectorId` の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、ListDetectors API を実行します。 `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING",`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	<pre>"AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre> コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
セキュリティエージェントの手動管理	1. 新しいアカウントの EKS Runtime Monitoring を選択的に有効にするには、自身の`###### ID` を使用し、UpdateOrganizationConfiguration API オペレーションを実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `DISABLED` に設定します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンの `detectorId` を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、1 つのアカウントで `EKS_RUNTIME_MONITORING` を有効にし、`EKS_ADDON_MANAGEMENT` を無効にします。スペースで区切られたアカウント ID のリストを渡すこともできます。 アカウントと現在のリージョンの `detectorId` を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、ListDetectors API を実行します。 `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。 2. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

個々のアクティブなメンバーアカウントの EKS Runtime Monitoring の有効化

API/CLI

「セキュリティエージェントを管理する GuardDutyためのアプローチ」に基づいて、推奨アプローチを選択し、次の表に示すステップに従うことができます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
によるセキュリティエージェントの管理 GuardDuty （ すべての EKS クラスターのモニタリング ）	メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `ENABLED` に設定します。 GuardDuty は、アカウント内のすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING と EKS_ADDON_MANAGEMENT の両方を有効にします。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** スペースで区切られたアカウント ID のリストを渡すこともできます。 コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
一部を除外したすべての EKS クラスターのモニタリング (除外タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは `GuardDutyManaged -false` です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を `eks:TagResource` に置き換えます。 • *ec2:DeleteTags* を `eks:UntagResource` に置き換えます。 • *access-project* を `GuardDutyManaged` に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の `PrincipalArn` を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	3. **Note** STATUS の を に設定する前に、必ず EKS クラスターEKS_RUNTIME_MONITORING に除外タグを追加してくださいENABLED。追加しないと、 GuardDuty セキュリティエージェントがアカウント内のすべての EKS クラスターにデプロイされます。 メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを実行します。 EKS_ADDON_MANAGEMENT のステータスを ENABLED に設定します。 GuardDuty は、モニタリングから除外されていないすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING と EKS_ADDON_MANAGEMENT の両方を有効にします。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	aws guardduty update-member-detectors --detector-id *12abc34d567e8fa901bc2d34e56789f0* --account-ids *111122223333* --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "*ENABLED*", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " *ENABLED*"}]]' **Note** スペースで区切られたアカウント ID のリストを渡すこともできます。 コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
選択的な EKS クラスターのモニタリング (包含タグの使用)	1. モニタリングから除外する EKS クラスターにタグを追加します。キーと値のペアは GuardDuty Managed -true です。タグの追加の詳細については、「Amazon EKS ユーザーガイド」の「CLI、API または eksctl でのタグの操作」を参照してください。 2. 信頼できるエンティティ以外によるタグの変更を防ぐには、「AWS Organizations ユーザーガイド」の「許可されたプリンシパル以外のタグが変更されないようにする」に記載されているポリシーを使用してください。このポリシーで、以下の詳細を置き換えます。 • *ec2:CreateTags* を に置き換えますeks:TagResource 。 • *ec2:DeleteTags* を に置き換えますeks:UntagResource 。 • *access-project* を GuardDutyManaged に置き換えます。 • *123456789012* を信頼されたエンティティの AWS アカウント ID に置き換えます。 信頼できるエンティティが複数ある場合は、次の例を使用して複数の PrincipalArn を追加します。 `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	3. メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の`###### ID` を使用し、updateMemberDetectors API オペレーションを実行します。 `EKS_ADDON_MANAGEMENT` のステータスを `DISABLED` に設定します。 GuardDuty は、`GuardDutyManaged -true` ペアでタグ付けされたすべての Amazon EKS クラスターのセキュリティエージェントのデプロイと更新を管理します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンの `detectorId` を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、`EKS_RUNTIME_MONITORING` を有効にして、`EKS_ADDON_MANAGEMENT` を無効にしています。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
	> **Note** スペースで区切られたアカウント ID のリストを渡すこともできます。 コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

GuardDuty セキュリティエージェントを管理するための推奨アプローチ	ステップ
セキュリティエージェントの手動管理	1. メンバーアカウントの EKS Runtime Monitoring を選択的に有効にするには、自分の###### *ID* を使用し、updateMemberDetectors API オペレーションを実行します。 EKS_ADDON_MANAGEMENT のステータスを DISABLED に設定します。 または、独自のリージョンレベルのディテクター ID を使用して AWS CLI コマンドを使用することもできます。アカウントと現在のリージョンdetectorId の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。 次の例では、EKS_RUNTIME_MONITORING を有効にして、EKS_ADDON_MANAGEMENT を無効にしています。 `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. セキュリティエージェントを管理するには、「Amazon EKS クラスターのセキュリティエージェントの手動管理」を参照してください。

EKS Runtime Monitoring から Runtime Monitoring への移行

GuardDuty Runtime Monitoring のリリースにより、脅威検出力バレッジが Amazon ECS コンテナと Amazon EC2 インスタンスに拡張されました。EKS Runtime Monitoring エクスペリエンスが Runtime Monitoring に統合されました。Runtime Monitoring を有効にし、ランタイム動作をモニタリングするリソースタイプ (Amazon EC2 インスタンス、Amazon ECS クラスター、Amazon EKS クラスター) ごとに個々の GuardDuty セキュリティエージェントを管理できます。

GuardDuty は、EKS Runtime Monitoring のコンソールエクスペリエンスを Runtime Monitoring に統合しました。 GuardDuty は EKS Runtime Monitoring 設定ステータスの確認と を推奨しますEKS Runtime Monitoring から Runtime Monitoring への移行。

Runtime Monitoring への移行の一環として、 を必ず に移行してくださいEKS Runtime Monitoring を無効にする。後で Runtime Monitoring を無効にし、EKS Runtime Monitoring を無効にしない場合、EKS Runtime Monitoring の使用コストが引き続き発生するため、これは重要です。

EKS Runtime Monitoring から Runtime Monitoring に移行するには

1. GuardDuty コンソールは、Runtime Monitoring の一部として EKS Runtime Monitoring をサポートしています。

   組織やアカウントの EKS Runtime Monitoring 設定ステータスの確認 ごとに Runtime Monitoring の使用を開始できます。

   Runtime Monitoring を有効にする前に、EKS Runtime Monitoring を無効にしないでください。EKS Runtime Monitoring を無効にすると、Amazon EKS アドオン管理も無効になります。リストされた順序で次のステップに進みます。
2. すべての Runtime Monitoring を有効にする前提条件 を満たしていることを確認してください。
3. Runtime Monitoring を有効にするには、EKS Runtime Monitoring と同じ組織設定を Runtime Monitoring にレプリケートします。詳細については、「Runtime Monitoring の有効化」を参照してください。
   - スタンドアロンアカウントをお持ちの場合は、Runtime Monitoring を有効にする必要があります。

     GuardDuty セキュリティエージェントが既にデプロイされている場合、対応する設定は自動的にレプリケートされるため、設定を再度設定する必要はありません。
   - 自動有効化設定を行っている組織がある場合は、必ず同じ自動有効化設定を Runtime Monitoring に複製してください。

- 既存のアクティブなメンバーアカウントに対して個別に設定されている組織がある場合は、Runtime Monitoring を有効にし、これらのメンバーのセキュリティ GuardDuty エージェントを個別に設定してください。

4. Runtime Monitoring と GuardDuty セキュリティエージェントの設定が正しいことを確認したら、API または AWS CLI コマンドを使用して EKS Runtime Monitoring を無効にします。
5. （オプション) GuardDuty セキュリティエージェントに関連付けられたリソースをクリーンアップする場合は、「」を参照してくださいリソースの無効化とクリーンアップの影響。

Runtime Monitoring を有効にせずに EKS Runtime Monitoring を引き続き使用する場合は、「」を参照してくださいEKS Runtime Monitoring の設定 (API のみ)。

EKS Runtime Monitoring 設定ステータスの確認

EKS Runtime Monitoring の既存の設定ステータスを確認するには、次の APIs または AWS CLI コマンドを使用します。

アカウント内の既存の EKS Runtime Monitoring 設定ステータスを確認するには

- GetDetector を実行して、自分のアカウントの設定ステータスを確認します。
- または、 AWS CLIを使用して以下のコマンドを実行できます。

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

と現在のリージョンのディテクター ID AWS アカウント を必ず置き換えてください。アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

組織の既存の EKS Runtime Monitoring 設定ステータスを確認するには (委任 GuardDuty 管理者アカウントとしてのみ)

- DescribeOrganizationConfiguration を実行して、組織の設定ステータスを確認します。

  または、 AWS CLIを使用して以下のコマンドを実行できます。

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

ディテクター ID を委任された GuardDuty 管理者アカウントのディテクター ID に置き換え、 リージョンを現在のリージョンに置き換えてください。アカウントと現在のリージョンdetectorIdのを検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

Runtime Monitoring への移行後に EKS Runtime Monitoring を無効にする

アカウントまたは組織の既存の設定が Runtime Monitoring に複製されたことを確認したら、EKS Runtime Monitoring を無効にできます。

EKS Runtime Monitoring を無効にするには

- 自分のアカウントで EKS Runtime Monitoring を無効にするには

  独自のリージョンレベルの *detector-id* を使用して UpdateDetector API を実行します。

  または、次の AWS CLI コマンドを使用できます。*12abc34d567e8fa901bc2d34e56789f0* を独自のリージョンレベルの *detector-id* に置き換えます。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
```

- 組織内のメンバーアカウントの EKS Runtime Monitoring を無効にするには

  組織の委任 GuardDuty 管理者アカウントのリージョンレベルの *detector-id* を使用して UpdateMemberDetectors API を実行します。

  または、次の AWS CLI コマンドを使用できます。*12abc34d567e8fa901bc2d34e56789f0* を組織の委任 GuardDuty 管理者アカウントのリージョンレベルの *detector-id* に、*111122223333* をこの機能を無効にするメンバーアカウントの AWS アカウント ID に置き換えます。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- 組織の EKS Runtime Monitoring の自動有効化設定を更新するには

EKS Runtime Monitoring の自動有効化設定を、組織内の新しい (NEW) またはすべての (ALL) メンバーアカウントに設定した場合にのみ、次の手順を実行します。既に として設定している場合はNONE、このステップをスキップできます。

> **Note**
>
> EKS Runtime Monitoring の自動有効化設定を に設定すると、EKS Runtime Monitoring は既存のメンバーアカウントまたは新しいメンバーアカウントが組織に参加するときに自動的に有効にならないNONEことを意味します。

組織の委任 GuardDuty 管理者アカウントのリージョンレベルの *detector-id* を使用して UpdateOrganizationConfiguration API を実行します。

または、次の AWS CLI コマンドを使用できます。*12abc34d567e8fa901bc2d34e56789f0* を組織の委任 GuardDuty 管理者アカウントのリージョンレベルの *detector-id* に置き換えます。*EXISTING_VALUE* を、 を自動有効化するための現在の設定に置き換えます GuardDuty。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

リソースのランタイムカバレッジの評価

Runtime Monitoring を有効にし、 GuardDuty セキュリティエージェントがリソースにデプロイされると、 GuardDuty は、対応するリソースタイプのカバレッジ統計と、アカウントに属するリソースの個々のカバレッジステータスを提供します。カバレッジステータスは、Runtime Monitoring を有効にし、Amazon VPC エンドポイントが作成され、対応するリソース GuardDuty のセキュリティエージェントがデプロイされたことを確認することで決定されます。Healthy カバレッジステータスは、リソースに関連するランタイムイベントがある場合、Amazon VPC GuardDuty エンドポイントを介してそのランタイムイベントを受信し、動作をモニタリングできることを示します。Runtime Monitoring の設定、Amazon VPC エンドポイントの作成、またはセキュリティエージェントのデプロイ GuardDuty時に問題が発生した場合、カバレッジステータスは「異常」と表示されます。カバレッジステータスが異常の場合、 は対応するリソースのランタイム動作を受信またはモニタリングしたり、Runtime Monitoring の検出結果を生成したり GuardDuty することはできません。

以下のトピックは、カバレッジ統計の確認、 EventBridge 通知の設定、特定のリソースタイプのカバレッジ問題のトラブルシューティングに役立ちます。

内容

Amazon EC2 インスタンスのカバレッジ

Amazon EC2 リソースの場合、ランタイムカバレッジはインスタンスレベルで評価されます。Amazon EC2 インスタンスは、 AWS 環境内のさまざまなタイプのアプリケーションやワークロードを実行できます。この機能は Amazon ECS によって管理されている Amazon EC2 インスタンスもサポートしており、Amazon EC2 インスタンスで Amazon ECS クラスターを実行している場合、インスタンスレベルでのカバレッジの問題は Amazon EC2 ランタイムカバレッジに表示されます。

トピック

カバレッジ統計の確認

自分のアカウントまたはメンバーアカウントに関連付けられた Amazon EC2 インスタンスのカバレッジ統計は、選択した AWS リージョンのすべての EC2 インスタンスに対する正常な EC2 インスタンスの割合です。次の式はこれを次のように表します。

(正常なインスタンス/すべてのインスタンス)*100

Amazon ECS クラスター GuardDuty のセキュリティエージェントもデプロイしている場合、Amazon EC2 インスタンスで実行されている Amazon ECS クラスターに関連するインスタンスレベルのカバレッジの問題は、Amazon EC2 インスタンスのランタイムカバレッジの問題として表示されます。

いずれかのアクセス方法を選択して、アカウントのカバレッジ統計を確認してください。

Console

- にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
- ナビゲーションペインで、[Runtime Monitoring] を選択します。
- [ランタイムカバレッジ] タブを選択します。
- [EC2 インスタンスのランタイムカバレッジ] タブでは、[クラスターリスト] テーブルにある各 Amazon EC2 インスタンスのカバレッジステータス別に集計されたカバレッジ統計を表示できます。
  - [インスタンスリスト] テーブルは次の列でフィルタリングできます。
    - アカウント ID
    - [エージェント管理タイプ]
    - [エージェントバージョン]
    - [カバレッジステータス]
    - [インスタンス ID]
    - クラスター ARN
- EC2 インスタンスのいずれかの [カバレッジステータス] が [異常] の場合、[問題] 列には、ステータスが [異常] である理由に関する追加情報が含まれています。

API/CLI

- 独自の有効なディテクター ID、現在のリージョン、およびサービスエンドポイントを使用して ListCoverage API を実行します。この API を使用して、インスタンスリストをフィルタリングしたり、ソートしたりできます。
  - 以下の `CriterionKey` のオプションのいずれかを使用して例 `filter-criteria` を変更できます。
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
    - `CLUSTER_ARN`

- に EC2 RESOURCE_TYPEとして filter-criteriaが含まれている場合、Runtime Monitoring は としての ISSUE の使用をサポートしていませんAttributeName。これを使用すると、API レスポンスは になりますInvalidInputException。

  以下のオプションで sort-criteria の例 AttributeName を変更できます。

  - ACCOUNT_ID
  - COVERAGE_STATUS
  - INSTANCE_ID
  - UPDATED_AT
- *max-results* (最大 50) を変更できます。
- アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- GetCoverageStatistics API を実行して、 に基づいてカバレッジ集計統計を取得しますstatisticsType。
  - 例 statisticsType を次のオプションのいずれかに変更できます。
    - COUNT_BY_COVERAGE_STATUS - カバレッジステータス別に集計された EKS クラスターのカバレッジ統計を表します。
    - COUNT_BY_RESOURCE_TYPE – リスト内の AWS リソースのタイプに基づいて集計されたカバレッジ統計。
    - コマンドで例 filter-criteria を変更できます。CriterionKey に対して次のオプションを設定できます。
      - ACCOUNT_ID
      - RESOURCE_TYPE
      - COVERAGE_STATUS
      - AGENT_VERSION
      - MANAGEMENT_TYPE

    - INSTANCE_ID
    - CLUSTER_ARN
- アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

EC2 インスタンスのカバレッジステータスが [異常] である場合は、「カバレッジ問題のトラブルシューティング」を参照してください。

カバレッジステータス変更通知の設定

Amazon EC2 インスタンスのカバレッジステータスが [異常] と表示される場合があります。カバレッジステータスの変化を検出するためにカバレッジステータスを定期的に監視し、ステータスが [異常] の場合はトラブルシューティングすることをお勧めします。または、Amazon EventBridge ルールを作成して、カバレッジステータスが異常から正常に変わったとき、または正常に変わったときに通知を受け取ることもできます。デフォルトでは、 はこれをアカウントのEventBridge バスにGuardDuty 発行します。

通知スキーマの例

EventBridge ルールでは、事前定義されたサンプルイベントとイベントパターンを使用して、カバレッジステータス通知を受信できます。 EventBridge ルールの作成の詳細については、「Amazon ユーザーガイド」の「ルールの作成」を参照してください。 EventBridge

さらに、次の通知スキーマの例を使用して、カスタムイベントパターンを作成します。アカウントの値を必ず置き換えてください。Amazon EC2 インスタンスのカバレッジステータスがから Healthyに変わったときに通知を受け取るにはUnhealthy、 が *GuardDuty Runtime Protection Unhealthy* detail-typeである必要があります。カバレッジステータスが から Unhealthyに変わったときに通知を受け取るにはHealthy、 の値を *GuardDuty Runtime Protection Healthy* detail-typeに置き換えます。

```
{
  "version": "0",
```

```
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ##### ID",
  "time": "event timestamp (string)",
  "region": "AWS #####",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

カバレッジ問題のトラブルシューティング

Amazon EC2 インスタンスのカバレッジステータスが [異常] の場合、その理由を [問題] 列で確認できます。

EC2 インスタンスが EKS クラスターに関連付けられていて、EKS のセキュリティエージェントが手動または自動エージェント設定でインストールされている場合は、「」を参照してカバレッジの問題をトラブルシューティングしてくださいAmazon EKS クラスターのカバレッジ。

次の表に、問題タイプと対応するトラブルシューティング手順を示します。

問題タイプ	発行メッセージ	トラブルシューティングのステップ
エージェントレポートなし	SSM 通知の待機	Amazon EC2 インスタンスが既に SSM 管理されていることを確認します。SSM 通知の受信には数分かかる場合があります。
	（意図的に空）	GuardDuty セキュリティエージェントを手動で管理する場合は、「」のステップに従っていることを確認してくださいAmazon EC2 インスタンスのセキュリティエージェントの手動管理。
		自動エージェント設定を有効にしている場合： • EC2 インスタンスは SSM 管理されています。 • セキュリティエージェントのステータスを定期的に表示します。詳細については、「GuardDuty セキュリティエージェントのインストールステータスの検証」を参照してください。
		組織にサービスコントロールポリシー (SCP) がある場合は、アクセスguardduty:SendSecurityTelemetry 許可が拒否されていないことを確認してください。詳細については、「組織のサービスコントロールポリシーの検証」を参照してください。
	エージェントが切断されました	• セキュリティエージェントのステータスを表示します。詳細については、「GuardDuty セキュリティエージェントのインストールステータスの検証」を参照してください。 • セキュリティエージェントのログを表示して、潜在的な根本原因を特定します。ログには、問題のトラブルシューティングに使用できる詳細なエラーが表示されます。ログファイルは にあります/var/log/amzn-guardduty-agent/ 。 sudo journalctl -u amazon-guardduty-agent を行います。

問題タイプ	発行メッセージ	トラブルシューティングのステップ
SSM 関連付けの作成に失敗しました	GuardDuty SSM の関連付けがアカウントに既に存在する	1. 既存の関連付けを手動で削除します。詳細については、「 AWS Systems Manager ユーザーガイド」の「関連付けの削除」を参照してください。 2. 関連付けを削除したら、Amazon EC2 GuardDuty の自動エージェント設定を無効にしてから再度有効にします。
	アカウントに SSM の関連付けが多すぎます	次の 2 つのオプションのいずれかを選択します。 • 未使用の SSM 関連付けをすべて削除します。詳細については、「 AWS Systems Manager ユーザーガイド」の「関連付けの削除」を参照してください。 • アカウントがクォータ引き上げの対象かどうかを確認します。詳細については、「」の「Systems Manager Service クォータ」を参照してくださいAWS 全般のリファレンス。
SSM 関連付けの更新に失敗しました	GuardDuty SSM の関連付けがアカウントに存在しません	GuardDuty SSM の関連付けはアカウントに存在しません。Runtime Monitoring を無効にしてから再度有効にします。
SSM 関連付けの削除に失敗しました	GuardDuty SSM の関連付けがアカウントに存在しません	SSM の関連付けがアカウントに存在しません。SSM の関連付けが意図的に削除された場合、アクションは必要ありません。

問題タイプ	発行メッセージ	トラブルシューティングのステップ
SSM インスタンス関連付けの実行に失敗しました	アーキテクチャ要件やその他の前提条件が満たされていない。	検証済みオペレーティングシステムのディストリビューションについては、「」を参照してくださいAmazon EC2 インスタンスサポートの前提条件。 それでもこの問題が解決しない場合は、次の手順が問題の特定と解決に役立ちます。 1. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。 2. ナビゲーションペインのノード管理 で、ステートマネージャー を選択します。 3. ドキュメント名プロパティでフィルタリングし、と入力しますAmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin。 4. 対応する関連付け ID を選択し、実行履歴 を表示します。 5. 実行履歴を使用して、障害を表示し、潜在的な根本原因を特定し、解決を試みます。
VPC エンドポイントの作成に失敗しました	VPC エンドポイントの作成は、共有 VPC *vpcId* ではサポートされていません	Runtime Monitoring は、組織内の共有 VPC の使用をサポートします。詳細については、「自動セキュリティエージェントで共有 VPC を使用する」を参照してください。

問題タイプ	発行メッセージ	トラブルシューティングのステップ
	自動エージェント設定で共有 VPC を使用する場合のみ 共有 VPC *vpcId* の所有者アカウント ID *111122223333* では、Runtime Monitoring、自動エージェント設定、またはその両方が有効になっていません。	共有 VPC 所有者アカウントは、少なくとも 1 つのリソースタイプ (Amazon EKS または Amazon ECS (AWS Fargate)) に対して Runtime Monitoring と自動エージェント設定を有効にする必要があります。詳細については、「Runtime Monitoring に GuardDuty固有の前提条件」を参照してください。

問題タイプ	発行メッセージ	トラブルシューティングのステップ
	プライベート DNS を有効にするには、enableDnsSupport とenableDnsHostnames VPC 属性の両方が *vpcId* に対して true に設定されている必要があります (サービス: Ec2、ステータス コード: 400、リクエスト ID: *a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*)。	次の VPC 属性が true - enableDnsSupport および enableDnsHostnames に設定されていることを確認する必要があります。詳細については、「VPC の DNS 属性」を参照してください。 https://console.aws.amazon.com/vpc/ にある Amazon VPC コンソールを使用して Amazon VPC を作成する場合は、必ず [DNS ホスト名を有効にする] および [解決を有効にする] の両方を選択してください。詳細については、「VPC 設定オプション」を参照してください。
共有 VPC エンドポイントの削除に失敗しました	共有 VPC エンドポイントの削除は、アカウント ID *111122223333* 、共有 VPC *vpcId*、所有者アカウント ID *555555555555* では許可されません。	考えられるステップ : • 共有 VPC 参加者アカウントの Runtime Monitoring ステータスを無効にしても、共有 VPC エンドポイントポリシーと所有者アカウントに存在するセキュリティグループには影響しません。 共有 VPC エンドポイントとセキュリティグループを削除するには、共有 VPC 所有者アカウントで Runtime Monitoring または自動エージェント設定ステータスを無効にする必要があります。 • 共有 VPC 参加者アカウントは、共有 VPC 所有者アカウントでホストされている共有 VPC エンドポイントとセキュリティグループを削除することはできません。

問題タイプ	発行メッセージ	トラブルシューティングのステップ
エージェントが報告しない	（意図的に空）	問題タイプはサポートを終了しました。この問題が引き続き発生し、まだ発生していない場合は、Amazon EC2 GuardDuty の自動エージェントを有効にします。 それでも問題が解決しない場合は、Runtime Monitoring を数分間無効にしてから再度有効にすることを検討してください。

Amazon ECS クラスターのカバレッジ

Amazon ECS クラスターのランタイムカバレッジには、 AWS Fargate (Fargate) および Amazon ECS コンテナインスタンス で実行されているタスクが含まれます[1]。

Fargate で実行される Amazon ECS クラスターの場合、ランタイムカバレッジはタスクレベルで評価されます。ECS クラスターのランタイムカバレッジには、Fargate (ECS のみ) の Runtime Monitoring と自動エージェント設定を有効にした後に実行を開始した Fargate タスクが含まれます。デフォルトでは、Fargate タスクはイミュータブル GuardDuty です。 は、セキュリティエージェントをインストールして、すでに実行中のタスクのコンテナをモニタリングすることはできません。このような Fargate タスクを含めるには、タスクを停止して再度開始する必要があります。関連付けられたサービスがサポートされていることを確認します。

Amazon ECS コンテナの詳細については、「キャパシティの作成」を参照してください。

内容

カバレッジ統計の確認

自分のアカウントまたはメンバーアカウントに関連付けられている Amazon ECS リソースのカバレッジ統計は、選択した 内のすべての Amazon ECS クラスターに対する正常な Amazon ECS クラスターの割合です AWS リージョン。これには、Fargate インスタンスと Amazon EC2 インスタンスの両方に関連付けられた Amazon ECS クラスターのカバレッジが含まれます。次の式はこれを次のように表します。

(正常なクラスター/すべてのクラスター)*100

考慮事項

- ECS クラスターのカバレッジ統計には、その ECS クラスターに関連付けられた Fargate タスクまたは ECS コンテナインスタンスのカバレッジステータスが含まれます。Fargate タスクのカバレッジステータスには、実行中の状態か、最近実行が終了したタスクが含まれます。
- ECS クラスターのランタイムカバレッジタブのコンテナインスタンスのカバレッジフィールドには、Amazon ECS クラスターに関連付けられたコンテナインスタンスのカバレッジステータスが表示されます。

  Amazon ECS クラスターに Fargate タスクのみが含まれている場合、カウントは 0/0 と表示されます。
- Amazon ECS クラスターが、セキュリティエージェントを持たない Amazon EC2 インスタンスに関連付けられている場合、Amazon ECS クラスターも異常カバレッジステータスになります。

  関連付けられた Amazon EC2 インスタンスのカバレッジの問題を特定してトラブルシューティングするには、Amazon EC2カバレッジ問題のトラブルシューティング」を参照してください。

いずれかのアクセス方法を選択して、アカウントのカバレッジ統計を確認してください。

Console

- にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
- ナビゲーションペインで、[Runtime Monitoring] を選択します。
- [ランタイムカバレッジ] タブを選択します。
- [ECS クラスターのランタイムカバレッジ] タブでは、[クラスターリスト] テーブルにある各 Amazon ECS クラスターのカバレッジステータス別に集計されたカバレッジ統計を表示できます。
  - [クラスターリスト] テーブルは次の列でフィルタリングできます。
    - アカウント ID
    - [クラスター名]
    - [エージェント管理タイプ]
    - [カバレッジステータス]

- いずれかの Amazon ECS クラスターのカバレッジステータスが異常 の場合、問題 列には異常ステータスの理由に関する追加情報が含まれます。

  Amazon ECS クラスターが Amazon EC2 インスタンスに関連付けられている場合は、EC2 インスタンスのランタイムカバレッジタブに移動し、クラスター名フィールドでフィルタリングして、関連する問題 を表示します。

API/CLI

- 独自の有効なディテクター ID、現在のリージョン、およびサービスエンドポイントを使用して ListCoverage API を実行します。この API を使用して、インスタンスリストをフィルタリングしたり、ソートしたりできます。
  - 以下の `CriterionKey` のオプションのいずれかを使用して例 `filter-criteria` を変更できます。
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
  - 以下のオプションで `sort-criteria` の例 `AttributeName` を変更できます。
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ECS_CLUSTER_NAME`
    - `UPDATED_AT`

      このフィールドは、関連する Amazon ECS クラスターで新しいタスクが作成されたとき、または対応するカバレッジステータスに変更があったときにのみ更新されます。
  - *`max-results`* (最大 50) を変更できます。
  - アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
"ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
```

```
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- GetCoverageStatistics API を実行して、 に基づいてカバレッジ集計統計を取得しますstatisticsType。
  - 例 statisticsType を次のオプションのいずれかに変更できます。
    - COUNT_BY_COVERAGE_STATUS – カバレッジステータス別に集計された ECS クラスターのカバレッジ統計を表します。
    - COUNT_BY_RESOURCE_TYPE – リスト内の AWS リソースのタイプに基づいて集計されたカバレッジ統計。
    - コマンドで例 filter-criteria を変更できます。CriterionKey に対して次のオプションを設定できます。
      - ACCOUNT_ID
      - ECS_CLUSTER_NAME
      - COVERAGE_STATUS
      - MANAGEMENT_TYPE
      - INSTANCE_ID
  - アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

カバレッジ問題を解決する方法の詳細については、「カバレッジ問題のトラブルシューティング」を参照してください。

カバレッジステータス変更通知の設定

Amazon ECS クラスターのカバレッジステータスは [異常] と表示される場合があります。カバレッジステータスの変化を検出するためにカバレッジステータスを定期的に監視し、ステータスが [異常] の場合はトラブルシューティングすることをお勧めします。または、Amazon EventBridge ルールを作成して、カバレッジステータスが「異常」から「正常」または「正常」に変わったときに通知を受

け取ることもできます。デフォルトでは、 はこれをアカウントのEventBridge バスに GuardDuty 発行します。

通知スキーマの例

EventBridge ルールでは、事前定義されたサンプルイベントとイベントパターンを使用して、カバレッジステータス通知を受信できます。 EventBridge ルールの作成の詳細については、「Amazon ユーザーガイド」の「ルールの作成」を参照してください。 EventBridge

さらに、次の通知スキーマの例を使用して、カスタムイベントパターンを作成します。アカウントの値を必ず置き換えてください。Amazon ECS クラスターのカバレッジステータスがから Healthyに変わったときに通知を受け取るにはUnhealthy、 が *GuardDuty Runtime Protection Unhealthy* detail-typeである必要があります。カバレッジステータスが から Unhealthyに変わったときに通知を受け取るにはHealthy、 の値を *GuardDuty Runtime Protection Healthy* detail-typeに置き換えます。

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ##### ID",
  "time": "event timestamp (string)",
  "region": "AWS #####",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
```

```
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

カバレッジ問題のトラブルシューティング

Amazon ECS クラスターのカバレッジステータスが [異常] の場合、その理由を [問題] 列で確認できます。

次のテーブルは、Fargate (Amazon ECS のみ) の問題に推奨されるトラブルシューティング手順を示しています。Amazon EC2 インスタンスカバレッジの問題については、Amazon EC2 インスタンスの カバレッジ問題のトラブルシューティング」を参照してください。

問題タイプ	追加情報	推奨されるトラブルシューティングの手順
エージェントが報告しない	エージェントが TaskDefinition - '*TASK_DEFINITION* ' のタスクを報告しない	VPC エンドポイント設定が正しいことを確認します。 組織にサービスコントロールポリシー (SCP) がある場合は、アクセスguardduty:SendSecurityTelemetry 許可が拒否されていないことを確認してください。詳細については、「組織のサービスコントロールポリシーの検証」を参照してください。
	VPC_ISSUE ; for task in TaskDefinition - ' *TASK_DEFINITION* '	追加情報の VPC の問題の詳細を確認してください。
エージェントが終了した	ExitCode: のタスクEXIT_CODE 用	追加情報で問題の詳細を表示します。

問題タイプ	追加情報	推奨されるトラブルシューティングの手順
	TaskDefinition - '*TASK_DEFINITION* '	
	理由: TaskDefinition - ' *TASK_DEFINITION* ' のタスクの *[##]*	
	ExitCode: 理由付き: のタスクのEXIT_CODE *#EXIT_CODE* TaskDefinition - '*TASK_DEFINITION* '」	

問題タイプ	追加情報	推奨されるトラブルシューティングの手順

	エージェントが終了しました: 理由: CannotPullContainerError : プルイメージマニフェストが再試行されました...	タスク実行ロールには、次の Amazon Elastic Container Registry (Amazon ECR) アクセス許可が必要です。
		
		`...`
		`"ecr:GetAuthorizationToken",`
		`"ecr:BatchCheckLayerAvailability",`
		`"ecr:GetDownloadUrlForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		
		詳細については、「ECR アクセス許可とサブネットの詳細を指定する」を参照してください。
		
		Amazon ECR アクセス許可を追加したら、タスクを再起動する必要があります。
		
		問題が解決しない場合は、「」を参照してくださいAWS Step Functions ワークフローが予期せず失敗している。

問題タイプ	追加情報	推奨されるトラブルシューティングの手順
その他またはエージェントが設定されていない	`TaskDefinition - 'TASK_DEFINITION '` のタスクにおける未確認の問題	次の質問を使用して、問題の根本原因を特定します。 • Runtime Monitoring を有効にする前にタスクが開始されましたか？ Amazon ECS では、タスクは変更できません。実行中の Fargate タスクのランタイム動作を評価するには、Runtime Monitoring がすでに有効になっていることを確認し、 のタスクを再起動 GuardDuty してコンテナサイドカーを追加します。 • このタスクは、Runtime Monitoring を有効にする前に開始されたサービスデプロイの一部ですか？ 「はい」の場合は、サービスを再起動するか、「サービスの更新」の手順に従い、`forceNewDeployment` によってサービスを更新できます。 UpdateService または を使用することもできますAWS CLI。 • ECS クラスターを Runtime Monitoring から除外した後にタスクが起動しましたか？ 事前定義された GuardDuty タグを `GuardDutyManaged -true` から `GuardDutyManaged -` に変更すると`false`、 GuardDuty は ECS クラスターのランタイムイベントを受信しません。

問題タイプ	追加情報	推奨されるトラブルシューティングの手順
		• タスクに `TaskExecutionRole` が抜けていませんか? には ECR リポジトリから GuardDuty コンテナをダウンロードするアクセス許可 GuardDuty が必要な`TaskExecutionRole` ため、 を追加する必要があります。詳細については、「ECR アクセス許可とサブネットの詳細を指定する」を参照してください。 • サービスには、古い形式の のタスクが含まれていますか`taskArn`? GuardDuty Runtime Monitoring は、古い形式の を持つタスクのカバレッジをサポートしていません`taskArn`。 Amazon ECS リソースの Amazon リソースネーム (ARNs「Amazon リソースネーム (ARNsと IDs」を参照してください。

Amazon EKS クラスターのカバレッジ

Runtime Monitoring を有効にし、EKS のセキュリティ GuardDuty エージェント (アドオン) を手動または自動エージェント設定でインストールしたら、EKS クラスターのカバレッジの評価を開始できます。

内容

- カバレッジ統計の確認
- カバレッジステータス変更通知の設定
- EKS カバレッジの問題のトラブルシューティング

カバレッジ統計の確認

自分のアカウントまたはメンバーアカウントに関連付けられた EKS クラスターのカバレッジ統計は、選択した AWS リージョンのすべての EKS クラスターに対する正常な EKS クラスターの割合です。次の式はこれを次のように表します。

(正常なクラスター/すべてのクラスター)*100

いずれかのアクセス方法を選択して、アカウントのカバレッジ統計を確認してください。

Console

- にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
- ナビゲーションペインで、[Runtime Monitoring] を選択します。
- [EKS クラスターのランタイムカバレッジ] タブを選択します。
- [EKS クラスターのランタイムカバレッジ] タブでは、[クラスターリスト] テーブルにあるカバレッジステータス別に集計されたカバレッジ統計を表示できます。
  - [クラスターリスト] テーブルは次の列でフィルタリングできます。
    - クラスター名
    - アカウント ID
    - [エージェント管理タイプ]
    - [カバレッジステータス]
    - [アドオンバージョン]
- EKS クラスターのいずれかの [カバレッジステータス] が [異常] の場合、[問題] 列には、ステータスが [異常] である理由に関する追加情報が含まれている場合があります。

API/CLI

- 独自の有効なディテクター ID、リージョン、サービスエンドポイントを使用して ListCoverage API を実行します。この API を使用して、クラスターリストをフィルタリングしたり、ソートしたりできます。
  - 以下の `CriterionKey` のオプションのいずれかを使用して例 `filter-criteria` を変更できます。
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`

    - RESOURCE_TYPE
    - COVERAGE_STATUS
    - ADDON_VERSION
    - MANAGEMENT_TYPE
  - 以下のオプションで sort-criteria の例 AttributeName を変更できます。
    - ACCOUNT_ID
    - CLUSTER_NAME
    - COVERAGE_STATUS
    - ISSUE
    - ADDON_VERSION
    - UPDATED_AT
  - *max-results* (最大 50) を変更できます。
  - アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- GetCoverageStatistics API を実行して、 に基づいてカバレッジ集計統計を取得しますstatisticsType。
  - 例 statisticsType を次のオプションのいずれかに変更できます。
    - COUNT_BY_COVERAGE_STATUS - カバレッジステータス別に集計された EKS クラスターのカバレッジ統計を表します。
    - COUNT_BY_RESOURCE_TYPE – リスト内の AWS リソースのタイプに基づいて集計されたカバレッジ統計。
    - コマンドで例 filter-criteria を変更できます。CriterionKey に対して次のオプションを設定できます。
      - ACCOUNT_ID
      - CLUSTER_NAME

    - RESOURCE_TYPE
    - COVERAGE_STATUS
    - ADDON_VERSION
    - MANAGEMENT_TYPE
- アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

EKS クラスターのカバレッジステータスが [異常] である場合は、「EKS カバレッジの問題のトラブルシューティング」を参照してください。

カバレッジステータス変更通知の設定

アカウントの EKS クラスターのカバレッジステータスが [異常] と表示されることがあります。カバレッジステータスが [異常] になったことを検出するためにカバレッジステータスを定期的にモニタリングし、ステータスが [異常] の場合はトラブルシューティングすることをお勧めします。または、カバレッジステータスが から または Healthy Unhealthyに変更された場合に通知する Amazon EventBridge ルールを作成することもできます。デフォルトでは、 はこれをアカウントのEventBridgeバスに GuardDuty 発行します。

通知スキーマの例

EventBridge ルールでは、事前定義されたサンプルイベントとイベントパターンを使用して、カバレッジステータス通知を受信できます。 EventBridge ルールの作成の詳細については、「Amazon ユーザーガイド」の「ルールの作成」を参照してください。 EventBridge

さらに、次の通知スキーマの例を使用して、カスタムイベントパターンを作成します。アカウントの値を必ず置き換えてください。Amazon EKS クラスターのカバレッジステータスが から Healthyに変わったときに通知を受け取るにはUnhealthy、 が *GuardDuty Runtime Protection Unhealthy* detail-typeである必要があります。カバレッジステータスが から Unhealthyに変わったときに通知を受け取るにはHealthy、 の値を *GuardDuty Runtime Protection Healthy* detail-typeに置き換えます。

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ##### ID",
  "time": "event timestamp (string)",
  "region": "AWS #####",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

EKS カバレッジの問題のトラブルシューティング

EKS クラスターのカバレッジステータスが の場合Unhealthy、 GuardDuty 対応するエラーはコンソールの問題列または CoverageResource データ型を使用して表示できます。

包含タグまたは除外タグを使用して EKS クラスターを選択的にモニタリングする場合、タグの同期に時間がかかることがあります。これにより、関連する EKS クラスターのカバレッジステータスに影響が及ぶ可能性があります。対応するタグ (包含または除外) を削除してから、もう一度追加してみることができます。詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS リソースのタグ付け」を参照してください。

カバレッジ問題の構造は `Issue type:Extra information` です。通常、問題にはオプションの追加情報があり、特定のクライアント側の例外や問題に関する説明が含まれる場合があります。追加

情報 に基づいて、EKS クラスターのカバレッジ問題のトラブルシューティングに推奨されるステップを次の表に示します。

問題のタイプ (プレフィックス)	追加情報	推奨されるトラブルシューティングの手順
アドオンの作成に失敗しました	アドオン`aws-guardduty-agent` は、クラスター の現在のクラスターバージョンと互換性がありません*`ClusterName`* 。指定されたアドオンはサポートされていません。	`aws-guardduty-agent` EKS アドオンのデプロイをサポートする Kubernetes バージョンのいずれかを使用していることを確認してください。詳細については、「GuardDuty セキュリティエージェントがサポートする Kubernetes バージョン」を参照してください。Kubernetes バージョンの更新については、「Amazon EKS クラスターの Kubernetes バージョンの更新」を参照してください。
アドオンの作成に失敗しました アドオンの更新に失敗しました アドオンのステータスが異常	EKS アドオンの問題 - `AddonIssueCode` : `AddonIssueMessage`	特定のアドオンの問題コードの推奨手順については、「」を参照してくださいTroubleshooting steps for Addon creation/updatation error with Addon issue code。 この問題で発生する可能性のあるアドオンの問題コードのリストについては、「」を参照してくださいAddonIssue。

問題のタイプ (プレフィックス)	追加情報	推奨されるトラブルシューティングの手順
VPC エンドポイントの作成に失敗しました	VPC エンドポイントの作成は、共有 VPC *vpcId* ではサポートされていません	Runtime Monitoring で、組織内の共有 VPC の使用がサポートされるようになりました。アカウントがすべての前提条件を満たしていることを確認します。詳細については、「共有 VPC を使用するための前提条件」を参照してください。
	自動エージェント設定で共有 VPC を使用する場合のみ 共有 VPC *vpcId* の所有者アカウント ID *111122223333* では、Runtime Monitoring、自動エージェント設定、またはその両方が有効になっていません。	共有 VPC 所有者アカウントは、少なくとも 1 つのリソースタイプ (Amazon EKS または Amazon ECS (AWS Fargate)) に対して Runtime Monitoring と自動エージェント設定を有効にする必要があります。詳細については、「Runtime Monitoring にGuardDuty固有の前提条件」を参照してください。

問題のタイプ (プレフィックス)	追加情報	推奨されるトラブルシューティングの手順
	プライベート DNS を有効にするには、enableDnsSupport とenableDnsHostnames VPC 属性の両方が *vpcId* に対して true に設定されている必要があります (サービス: Ec2、ステータス コード: 400、リクエスト ID: *a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*)。	次の VPC 属性が true - enableDnsSupport および enableDnsHostnames に設定されていることを確認する必要があります。詳細については、「VPC の DNS 属性」を参照してください。 https://console.aws.amazon.com/vpc/ にある Amazon VPC コンソールを使用して Amazon VPC を作成する場合は、必ず [DNS ホスト名を有効にする] および [解決を有効にする] の両方を選択してください。詳細については、「VPC 設定オプション」を参照してください。

問題のタイプ (プレフィックス)	追加情報	推奨されるトラブルシューティングの手順
共有 VPC エンドポイントの削除に失敗しました	共有 VPC エンドポイントの削除は、アカウント ID *111122223333* 、共有 VPC *vpcId*、所有者アカウント ID *555555555555* では許可されません。	考えられるステップ： • 共有 VPC 参加者アカウントの Runtime Monitoring ステータスを無効にしても、共有 VPC エンドポイントポリシーと所有者アカウントに存在するセキュリティグループには影響しません。 共有 VPC エンドポイントとセキュリティグループを削除するには、共有 VPC 所有者アカウントで Runtime Monitoring または自動エージェント設定ステータスを無効にする必要があります。 • 共有 VPC 参加者アカウントは、共有 VPC 所有者アカウントでホストされている共有 VPC エンドポイントとセキュリティグループを削除することはできません。

問題のタイプ (プレフィックス)	追加情報	推奨されるトラブルシューティングの手順
ローカル EKS クラスター	EKS アドオンはローカルのアウトポストクラスターではサポートされていません。	実用的ではありません。 詳細については、「AWS Outposts の Amazon EKS」を参照してください。
EKS Runtime Monitoring の有効化許可が付与されていません	(追加情報が表示される場合と表示されない場合があります)	1. この問題に関する追加情報がある場合は、根本原因を修正して次の手順に従ってください。 2. EKS Runtime Monitoring を切り替えて、オフにしてから再度オンにします。GuardDuty エージェントが、自動 GuardDuty または手動でデプロイされていることを確認します。
進行中の EKS Runtime Monitoring 有効化リソースのプロビジョニング	(追加情報が表示される場合と表示されない場合があります)	実用的ではありません。 EKS Runtime Monitoring を有効にしても、リソースプロビジョニングステップが完了するまでカバレッジステータスが `Unhealthy` として残る場合があります。カバレッジステータスは定期的に監視および更新されます。

問題のタイプ (プレフィックス)	追加情報	推奨されるトラブルシューティングの手順
その他 (その他の問題)	認証の失敗によるエラー	EKS Runtime Monitoring を切り替えて、オフにしてから再度オンにします。 GuardDuty エージェントも、 を介して自動的に、 GuardDuty または手動でデプロイされていることを確認します。

アドオンの作成または更新エラー	トラブルシューティングのステップ
EKS アドオンの問題 - `InsufficientNumberOfReplicas` : 必要な数のレプリカがないため、アドオンが異常です。	問題メッセージを使用して、根本原因を特定して修正できます。まず、クラスターを記述します。例えば、 `kubectl describe pods`を使用してポッド障害の根本原因を特定します。 根本原因を修正したら、ステップ (アドオンの作成または更新) を再試行します。
EKS アドオンの問題 - `AdmissionRequestDenied` : アドミッションウェブフックがリクエスト`"validate.kyverno.svc-fail"` を拒否しました: リソース違反`DaemonSet/amazon-guardduty/aws-guardduty-agent` のポリシー : restrict-image-registries: `autogen-validate-registries` : ...	1. Amazon EKS クラスターまたはセキュリティ管理者は、アドオンの更新をブロックしているセキュリティポリシーを確認する必要があります。 2. コントローラを無効にする (webhook) か、コントローラが Amazon EKS からのリクエストを受け付けるようにする必要があります。
EKS アドオンの問題 - `ConfigurationConflict` : 適用しようとしたときに競合が見つかりました。コンフリクト解決モー	アドオンを作成または更新するときは、`OVERWRITE` コンフリクト解決フラグを指定してください。これにより、Kubernetes API

アドオンの作成または更新エラー	トラブルシューティングのステップ
ドのため、続行できません。Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image	を使用して Kubernetes の関連リソースに直接加えられた変更が上書きされる可能性があります。 最初に「アドオンを削除」してから再インストールできます。

EKS アドオンの問題 - AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope	不足している権限を手動で eks:addon-cluster-admin ClusterRoleBinding に追加する必要があります。以下を yaml から eks:addon-cluster-admin に追加します。
	
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	
	次のコマンドを使用して、この yaml を Amazon EKS クラスターに適用できるようになります。
	
	`kubectl apply -f eks-addon-cluster-admin.yaml`

アドオンの作成または更新エラー	トラブルシューティングのステップ
EKS アドオンの問題 - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	コントローラを無効にするか、コントローラが Amazon EKS クラスターからのリクエストを受け付けるようにする必要があります。 アドオンを作成または更新する前に、GuardDuty 名前空間を作成し、 としてラベルを付けることもできますowner。

よくある質問 (FAQ)

内容

Runtime Monitoring を有効にし、 GuardDuty セキュリティエージェントをデプロイし、すべての前提条件を満たした後**Unhealthy**でも、リソースのカバレッジステータスが であるのはなぜですか？

GuardDuty セキュリティエージェントを (自動エージェント設定または手動で) デプロイしたばかりの場合、または推奨される手順に従ってカバレッジの問題をトラブルシューティングした場合、カバレッジステータスが正常になるまでに数分かかることがあります。カバレッジステータスを定期的に確認するか、カバレッジステータスが変更されたときに通知を受信するように Amazon EventBridge (EventBridge) を設定できます。

自分の に属するリソースのランタイムカバレッジステータスは誰が確認できますか AWS アカウント？

メンバーアカウントまたはスタンドアロンアカウントの場合は、自身のアカウントに関連付けられているリソースのカバレッジ統計を表示できます。組織の委任 GuardDuty 管理者アカウントとして、

アカウントと組織に属するメンバーアカウントに関連付けられたリソースのカバレッジ統計を表示できます。

CPU とメモリモニタリングの設定

Runtime Monitoring を有効にして、クラスターのカバレッジステータスが [正常] と評価されると、インサイトメトリクスを設定および表示できます。

以下のトピックは、デプロイされたエージェントがエージェントの CPU とメモリの制限に対してどのように動作するかを評価するのに役立ちます GuardDuty 。

Amazon ECS クラスターでの監視設定

Amazon CloudWatch ユーザーガイドの次の手順は、デプロイされたエージェントがエージェントの CPU とメモリの制限に対してどのように動作するかを評価するのに役立ちます GuardDuty 。

1. 「クラスターおよびサービスレベルの Amazon ECS でメトリクスの Container Insights の設定」
2. 「Amazon ECS Container Insights メトリクス」

Amazon EKS クラスターでの監視設定

GuardDuty セキュリティエージェントがデプロイされ、クラスターのカバレッジステータスが正常であることを確認したら、コンテナインサイトメトリクスを設定して表示できます。

セキュリティエージェントのパフォーマンスを評価する

1. 「Amazon ユーザーガイド」の「Amazon EKS および Kubernetes での Container Insights のセットアップ CloudWatch 」
2. 「Amazon ユーザーガイド」の「Amazon EKS および Kubernetes Container Insights メトリクス CloudWatch 」

セキュリティエージェント v1.5.0 以降でパフォーマンスを管理する

セキュリティエージェント v1.5.0 以降では、関連付けられた GuardDuty エージェントが割り当てられた制限に達していることがインサイトで示されたら、特定のパラメータを設定できます。詳細については、「EKS アドオンパラメータを設定する」を参照してください。

が GuardDuty 使用する収集済みランタイムイベントタイプ

GuardDuty セキュリティエージェントは、次のイベントタイプを収集し、 GuardDuty脅威の検出と分析のためにバックエンドに送信します。 GuardDuty これらのイベントはアクセスできません。が潜在的な脅威 GuardDuty を検出し、Runtime Monitoring の検出結果を生成した場合、対応する検出結果の詳細を表示できます。が収集したイベントタイプ GuardDuty を使用する方法の詳細については、「」を参照してくださいサービス改善のためのデータ使用をオプトアウトする。

イベントを処理する

フィールド名	説明
プロセス名	監視されたプロセスの名前。
プロセスパス	プロセスの実行可能ファイルの絶対パス。
プロセス ID	オペレーティングシステムによってプロセスに割り当てられた ID。
名前空間 PID	ホストレベルの PID 名前空間以外のセカンダリ PID 名前空間内のプロセスのプロセス ID。コンテナ内のプロセスの場合、コンテナ内で確認されるプロセス ID です。
プロセスユーザー ID	プロセスを実行したユーザーの固有 ID。
プロセス UUID。	によってプロセスに割り当てられた一意の ID GuardDuty。
プロセス GID。	プロセスグループのプロセス ID。
プロセス EGID。	プロセスグループの実効グループ ID。
プロセス EUID。	プロセスの実効ユーザー ID。
プロセスユーザー名	プロセスを実行したユーザー名。

フィールド名	説明
プロセス開始時間	プロセスが作成された時間。このフィールドは、UTC 日付文字列形式 (2023-03-22T19:37:20.168Z)です。
プロセスの実行可能ファイル SHA-256	プロセスの実行可能ファイルの SHA256 ハッシュ。
プロセススクリプトパス	実行されたスクリプトファイルのパス。
プロセス環境変数	プロセスで利用可能になった環境変数。LD_PRELOAD および LD_LIBRARY_PATH のみ収集可能です。
プロセス現在の作業ディレクトリ (PWD)	プロセスの現在の作業ディレクトリ。
親プロセス	親プロセスのプロセス詳細。親プロセスとは、監視対象のプロセスを作成したプロセスです。
コマンドライン引数 現在、このフィールドはリソースタイプに対応する特定のエージェントバージョンに制限されています。 • GuardDuty セキュリティエージェント v1.0.0 以降を搭載した Fargate (Amazon ECS のみ) 。 • GuardDuty セキュリティエージェント v1.0.0 以降の Amazon EC2 インスタンス。 • セキュリティエージェント v1.4.0 以降の Amazon EKS クラスター。 詳細については、「GuardDuty エージェントリリース履歴」を参照してください。	プロセスの実行時に提供されるコマンドライン引数。このフィールドには機密の顧客データが含まれている可能性があります。

コンテナイベント

フィールド名	説明
コンテナ名	コンテナの名前。 使用可能な場合、このフィールドには `io.kubenetes.container.name` ラベルの値が表示されます。
コンテナ UID	コンテナランタイムによって割り当てられたコンテナの固有の ID。
コンテナランタイム	コンテナの実行に使用されたコンテナランタイム (`docker` または `containerd` など)。
コンテナイメージ ID	コンテナのイメージの ID。
コンテナイメージ名	コンテナイメージの名前。

AWS Fargate (Amazon ECS のみ) タスクイベント

フィールド名	説明
タスク Amazon リソースネーム (ARN)	タスクの ARN。
[クラスター名]	Amazon ECS クラスターの名前。
[Family Name] (姓)	タスク定義のファミリー名。`family` は、タスクを起動するために使用されるタスク定義の名前として使用されます。
サービス名	タスクがサービスの一部として起動された場合の Amazon ECS サービスの名前。
起動タイプ	タスクが実行されるインフラストラクチャ。`ECSCluster` のリソースタイプの Runtime Monitoring では、起動タイプは `EC2` または `FARGATE` のどちらかになります。

フィールド名	説明
CPU	タスク定義に示されている、タスクで使用される CPU ユニットの数。

Kubernetes ポッドイベント

フィールド名	説明
ポッド ID	Kubernetes ポッドの ID。
ポッド名	Kubernetes ポッドの名前。
ポッド名前空間	Kubernetes ワークロードが属する Kubernetes 名前空間の名前。
Kubernetes クラスター名	Kubernetes クラスターの名前。

DNS イベント

フィールド名	説明
ソケットタイプ	通信セマンティクスを示すソケットのタイプ。例えば `SOCK_RAW` です。
アドレスファミリー	アドレスに関連付けられた通信プロトコルを示します。例えば、アドレスファミリー `AF_INET` は IP v4 プロトコルに使用されます。
方向 ID	接続方向の ID。
プロトコル番号	レイヤー 4 プロトコル番号。例えば UDP の場合は 17、TCP の場合は 6 です。
DNS リモートエンドポイント IP	接続のリモート IP。

フィールド名	説明
DNS リモートエンドポイントポート	接続のポート番号。
DNS ローカルエンドポイント IP	接続のローカル IP。
DNS ローカルエンドポイントポート	接続のポート番号。
DNS ペイロード	DNS クエリと応答を含む DNS パケットのペイロード。

オープンイベント

フィールド名	説明
Filepath	このイベントで開かれるファイルのパス。
Flags	読み込み専用、書き込み専用、読み込み/書き込みなどのファイルアクセスモードについて説明します。

ロードモジュールのイベント

フィールド名	説明
モジュール名	カーネルにロードされたモジュールの名前。

モプロテクトイベント

フィールド名	説明
アドレス範囲	アクセス保護が変更されたアドレス範囲。

フィールド名	説明
メモリ領域	スタックやヒープなど、プロセスのアドレス空間のリージョンを指定します。
Flags	このイベントの動作をコントロールするオプションを示します。

マウントイベント

フィールド名	説明
マウントターゲット	マウントソースがマウントされているパス。
マウントソース	マウントターゲットにマウントされているホスト上のパス。
ファイルシステムタイプ	マウントされているファイルシステムのタイプを示します。
Flags	このイベントの動作をコントロールするオプションを示します。

リンクイベント

フィールド名	説明
リンクパス	ハードリンクが作成されるパス。
ターゲットパス	ハードリンクが指すファイルのパス。

Symlink イベント

フィールド名	説明
リンクパス	Symlink リンクが作成されるパス。

フィールド名	説明
ターゲットパス	Symlink リンクが指すファイルのパス。

Dup イベント

フィールド名	説明
古いファイルディスクリプタ	開いているファイルオブジェクトを表すファイル記述子。
新規ファイルディスクリプタ	古いファイル記述子の複製である新しいファイル記述子。古いファイル記述子と新しいファイル記述子はどちらも同じ開いているファイルオブジェクトを示します。
Dup リモートエンドポイント IP	古いファイル記述子で表されるネットワークソケットのリモート IP アドレス。古いファイル記述子がネットワークソケットを示す場合にのみ適用されます。
Dup リモートエンドポイントポート	古いファイル記述子で表されるネットワークソケットのリモートポート。古いファイル記述子がネットワークソケットを示す場合にのみ適用されます。
Dup ローカルエンドポイント IP	古いファイルディスクリプタで表されるネットワークソケットのローカル IP アドレス。古いファイル記述子がネットワークソケットを示す場合にのみ適用されます。
Dup ローカルエンドポイントポート	古いファイル記述子で表されるネットワークソケットのローカルポート。古いファイル記述子がネットワークソケットを示す場合にのみ適用されます。

メモリマッピングイベント

フィールド名	説明
Filepath	メモリがマッピングされているファイルのパス。

ソケットイベント

フィールド名	説明
アドレスファミリー	アドレスに関連付けられた通信プロトコルを示します。例えば、アドレスファミリー AF_INET は IP バージョンの 4 プロトコルに使用されます。
ソケットタイプ	通信セマンティクスを示すソケットのタイプ。例えば SOCK_RAW です。
プロトコル番号	アドレスファミリー内の特定のプロトコルを指定します。通常、アドレスファミリーには単一のプロトコルがあります。例えば、アドレスファミリー AF_INET には IP プロトコルしかありません。

イベントを接続

フィールド名	説明
アドレスファミリー	アドレスに関連付けられた通信プロトコルを示します。例えば、アドレスファミリー AF_INET は IP v4 プロトコルに使用されます。
ソケットタイプ	通信セマンティクスを示すソケットのタイプ。例えば SOCK_RAW です。
プロトコル番号	アドレスファミリー内の特定のプロトコルを指定します。通常、アドレスファミリーには単一のプロトコルがあります。例えば、アドレスファミリー AF_INET には IP プロトコルしかありません。
Filepath	アドレスファミリーが AF_UNIX の場合のソケットファイルのパス。
リモートエンドポイント IP	接続のリモート IP。

フィールド名	説明
リモートエンドポイントポート	接続のポート番号。
ローカルエンドポイント IP	接続のローカル IP。
ローカルエンドポイントポート	接続のポート番号。

VM Readv イベントの処理

フィールド名	説明
Flags	このイベントの動作をコントロールするオプションを示します。
ターゲット PID	メモリを読み込んでいるプロセスのプロセス ID。
ターゲットプロセスの UUID	ターゲットプロセスの一意の ID。
ターゲットの実行可能ファイルのパス	ターゲットプロセスの実行可能ファイルの絶対パス。

VM Writev イベントの処理

フィールド名	説明
Flags	このイベントの動作をコントロールするオプションを示します。
ターゲット PID	メモリが書き込まれているプロセスのプロセス ID。
ターゲットプロセスの UUID	ターゲットプロセスの一意の ID。
ターゲットの実行可能ファイルのパス	ターゲットプロセスの実行可能ファイルの絶対パス。

Ptrace イベント

フィールド名	説明
ターゲット PID	ターゲットプロセスのプロセス ID。
ターゲットプロセスの UUID	ターゲットプロセスの一意の ID。
ターゲットの実行可能ファイルのパス	ターゲットプロセスの実行可能ファイルの絶対パス。
Flags	このイベントの動作をコントロールするオプションを示します。

バインドイベント

フィールド名	説明
アドレスファミリー	アドレスに関連付けられた通信プロトコルを示します。例えば、アドレスファミリー `AF_INET` は IP v4 プロトコルに使用されます。
ソケットタイプ	通信セマンティクスを示すソケットのタイプ。例えば `SOCK_RAW` です。
プロトコル番号	レイヤー 4 プロトコル番号。例えば UDP の場合は 17、TCP の場合は 6 です。
ローカルエンドポイント IP	接続のローカル IP。
ローカルエンドポイントポート	接続のポート番号。

リッスンイベント

フィールド名	説明
アドレスファミリー	アドレスに関連付けられた通信プロトコルを示します。例えば、アドレスファミリー AF_INET は IP v4 プロトコルに使用されます。
ソケットタイプ	通信セマンティクスを示すソケットのタイプ。例えば SOCK_RAW です。
プロトコル番号	レイヤー 4 プロトコル番号。例えば UDP の場合は 17、TCP の場合は 6 です。
ローカルエンドポイント IP	接続のローカル IP。
ローカルエンドポイントポート	接続のポート番号。

イベントの名前を変更する

フィールド名	説明
Filepath	名前が変更されたファイルへのパス。
Target	ファイルの新しいパス。

UID イベントの設定

フィールド名	説明
新しい EUID	プロセスの新しい有効なユーザー ID。
新しい UID	プロセスの新しいユーザー ID。

Chmod イベント

フィールド名	説明
Filepath	このイベントを呼び出すファイルのパス。
ファイルモード	関連付けられたファイルの更新されたアクセス許可。

Amazon ECR リポジトリホスティング GuardDuty エージェント

以下のセクションでは、 が Amazon EKS および Amazon ECS クラスターにデプロイされるセキュリティエージェントを GuardDuty ホストする Amazon Elastic Container Registry (Amazon ECR) リポジトリを一覧表示します。

内容

- EKS エージェントバージョン 1.6.0 以降のリポジトリ
- EKS エージェントバージョン 1.5.0 以前のリポジトリ
- での GuardDuty エージェントのリポジトリ AWS Fargate (Amazon ECS のみ)

EKS エージェントバージョン 1.6.0 以降のリポジトリ

次の表は、各 について、Amazon EKS アドオンエージェントバージョン (aws-guardduty-agent) 1.6.0 以降をホストする Amazon ECR リポジトリを示しています AWS リージョン。

AWS リージョン	Amazon ECR リポジトリ URI
米国西部 (オレゴン)	602401143452.dkr.ecr.us-west-2.amazonaws.com
欧州 (パリ)	602401143452.dkr.ecr.eu-west-3.amazonaws.com
アジアパシフィック (ムンバイ)	602401143452.dkr.ecr.ap-south-1.amazonaws.com

AWS リージョン	Amazon ECR リポジトリ URI
アジアパシフィック (ハイデラバード)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
カナダ (中部)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
カナダ西部 (カルガリー)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
中東 (アラブ首長国連邦)	759879836304.dkr.ecr.me-central-1.amazonaws.com
欧州 (ロンドン)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
米国西部 (北カリフォルニア)	602401143452.dkr.ecr.us-west-1.amazonaws.com
米国東部 (バージニア北部)	602401143452.dkr.ecr.us-east-1.amazonaws.com
米国東部 (オハイオ)	602401143452.dkr.ecr.us-east-2.amazonaws.com
欧州 (アイルランド)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
南米 (サンパウロ)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
欧州 (ストックホルム)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
欧州 (フランクフルト)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
欧州 (チューリッヒ)	900612956339.dkr.ecr.eu-central-2.amazonaws.com

AWS リージョン	Amazon ECR リポジトリ URI
アジアパシフィック (シンガポール)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
アジアパシフィック (シドニー)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
アジアパシフィック (ジャカルタ)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
アジアパシフィック (東京)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
アジアパシフィック (ソウル)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
アジアパシフィック (大阪)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
アジアパシフィック (香港)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
中東 (バーレーン)	759879836304.dkr.ecr.me-south-1.amazonaws.com
欧州 (ミラノ)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
欧州 (スペイン)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
アフリカ (ケープタウン)	877085696533.dkr.ecr.af-south-1.amazonaws.com

AWS リージョン	Amazon ECR リポジトリ URI
アジアパシフィック (メルボルン)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
イスラエル (テルアビブ)	066635153087.dkr.ecr.il-central-1.amazonaws.com

EKS エージェントバージョン 1.5.0 以前のリポジトリ

次の表は、各 について、Amazon EKS アドオンエージェントバージョン (aws-guardduty-agent) 1.5.0 以前の をホストする Amazon ECR リポジトリを示しています AWS リージョン。

AWS リージョン	Amazon ECR リポジトリ URI
米国西部 (オレゴン)	039403964562.dkr.ecr.us-west-2.amazonaws.com
欧州 (パリ)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
アジアパシフィック (ムンバイ)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
アジアパシフィック (ハイデラバード)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
カナダ (中部)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
中東 (アラブ首長国連邦)	601769779514.dkr.ecr.me-central-1.amazonaws.com
欧州 (ロンドン)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
米国西部 (北カリフォルニア)	373421517865.dkr.ecr.us-west-1.amazonaws.com

AWS リージョン	Amazon ECR リポジトリ URI
米国東部 (バージニア北部)	031903291036.dkr.ecr.us-east-1.amazonaws.com
米国東部 (オハイオ)	591382732059.dkr.ecr.us-east-2.amazonaws.com
欧州 (アイルランド)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
南米 (サンパウロ)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
欧州 (ストックホルム)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
欧州 (フランクフルト)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
欧州 (チューリッヒ)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
アジアパシフィック (シンガポール)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
アジアパシフィック (シドニー)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
アジアパシフィック (ジャカルタ)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
アジアパシフィック (東京)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com

AWS リージョン	Amazon ECR リポジトリ URI
アジアパシフィック (ソウル)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
アジアパシフィック (大阪)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
アジアパシフィック (香港)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
中東 (バーレーン)	541829937850.dkr.ecr.me-south-1.amazonaws.com
欧州 (ミラノ)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
欧州 (スペイン)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
アフリカ (ケープタウン)	379032919888.dkr.ecr.af-south-1.amazonaws.com
アジアパシフィック (メルボルン)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
イスラエル (テルアビブ)	292660727137.dkr.ecr.il-central-1.amazonaws.com

での GuardDuty エージェントのリポジトリ AWS Fargate (Amazon ECS のみ)

次の表は、各 の AWS Fargate (Amazon ECS のみ) の GuardDuty エージェントをホストする Amazon ECR リポジトリを示しています AWS リージョン。

AWS リージョン	Amazon ECR リポジトリ URI
米国西部 (オレゴン)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate
欧州 (パリ)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (ムンバイ)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (ハイデラバード)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate
カナダ (中部)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate
中東 (アラブ首長国連邦)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate
欧州 (ロンドン)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate
米国西部 (北カリフォルニア)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate
米国東部 (バージニア北部)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate
米国東部 (オハイオ)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate
欧州 (アイルランド)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
南米 (サンパウロ)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate

AWS リージョン	Amazon ECR リポジトリ URI
欧州 (ストックホルム)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
欧州 (フランクフルト)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
欧州 (チューリッヒ)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (シンガポール)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (シドニー)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (ジャカルタ)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (東京)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (ソウル)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (大阪)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (香港)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
中東 (バーレーン)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate

AWS リージョン	Amazon ECR リポジトリ URI
欧州 (ミラノ)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
欧州 (スペイン)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
アフリカ (ケープタウン)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate
アジアパシフィック (メルボルン)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate
イスラエル (テルアビブ)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate

GuardDuty エージェントリリース履歴

以下のセクションでは、Amazon EC2 インスタンス、Amazon ECS クラスター、および Amazon EKS クラスターにデプロイされる GuardDuty エージェントのリリースバージョンについて説明します。

GuardDuty Amazon EC2 インスタンスのセキュリティエージェント

[エージェントバージョン]	リリースノート	利用可能日
v1.2.0	OS ディストリビューション Ubuntu 20.04、Ubuntu 22.04、Debian 11、および Debian 12 をサポート カーネル 6.5 および 6.8 をサポート 一般的なパフォーマンスのチューニングと機能強化	2024 年 6 月 13 日

[エージェントバージョン]	リリースノート	利用可能日
v1.1.0	Amazon EC2 インスタンスのランタイムモニタリングで GuardDuty 自動エージェント設定をサポート EC2 インスタンスの Runtime Monitoring の一般提供を発表してリリースされた新しいセキュリティシグナルと検出結果をサポートします 一般的なパフォーマンスのチューニングと機能強化	2024 年 3 月 26 日
v1.0.2	最新の Amazon ECS AMIsをサポートします。	2024 年 2 月 21 日
v1.0.1	v1.0.2 より前にリリースされたエージェントバージョンは、2024 年 1 月 31 日以降にリリースされた Amazon ECS AMIs と互換性がありません。 一般的なパフォーマンスのチューニングと機能強化	2024 年 1 月 23 日
v1.0.0	RPM インストールの初回リリース v1.0.2 より前にリリースされたエージェントバージョンは、2024 年 1 月 31 日以降にリリースされた Amazon ECS AMIs と互換性がありません。	2023 年 11 月 26 日

RPM S3 bucket example script

パブリックキー、x86_64 RPM の署名、arm64 RPM の署名、および Amazon S3 バケットでホストされている RPM スクリプトへの対応するアクセスリンクは、以下のテンプレートから作成できます。RPM スクリプトにアクセスするには AWS リージョン、、 AWS アカウント ID、および GuardDuty エージェントバージョンの値に置き換えます。次のテンプレートには、Amazon EC2 インスタンスの最新のエージェントバージョンが含まれています。

- パブリックキー :

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/publickey.pem
```

- GuardDuty セキュリティエージェントの RPM 署名 :

  x86_64 RPM の署名

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/x86_64/amazon-guardduty-agent-1.2.0.x86_64.sig
```

  arm64 RPM の署名

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/arm64/amazon-guardduty-agent-1.2.0.arm64.sig
```

- Amazon S3 バケット内の RPM スクリプトへのアクセスリンク:

  x86_64 RPM 用アクセスリンク

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/x86_64/amazon-guardduty-agent-1.2.0.x86_64.rpm
```

  arm64 RPM 用アクセスリンク

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/arm64/amazon-guardduty-agent-1.2.0.arm64.rpm
```

Debian S3 bucket example script

パブリックキー、arm64 を使用した署名、および Amazon S3 バケットでホストされるスクリプトへの対応するアクセスリンクは、次のテンプレートから形成できます。スクリプトにアクセスするには AWS リージョン、、 AWS アカウント ID、および GuardDuty エージェントバージョン

を置き換えます。次のテンプレートには、Amazon EC2 インスタンスの最新のエージェントバージョンが含まれています。

- パブリックキー：

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/publickey.pem
```

- GuardDuty セキュリティエージェントの署名：

  amd64 の署名

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/amd64/amazon-guardduty-agent-1.2.0.amd64.sig
```

  arm64 の署名

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/arm64/amazon-guardduty-agent-1.2.0.arm64.sig
```

- Amazon S3 バケット のスクリプトへのアクセスリンク：

  amd64 のアクセスリンク

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/amd64/amazon-guardduty-agent-1.2.0.amd64.deb
```

  arm64 のアクセスリンク

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/arm64/amazon-guardduty-agent-1.2.0.arm64.deb
```

AWS リージョン	リージョン名	AWS アカウント ID
eu-west-1	欧州 (アイルランド)	694911143906
us-east-1	米国東部 (バージニア北部)	593207742271
us-east-2	米国東部 (オハイオ)	733349766148
eu-west-3	欧州 (パリ)	665651866788

us-east-2	米国東部 (オハイオ)	307168627858
eu-central-1	欧州 (フランクフルト)	323658145986
ap-northeast-2	アジアパシフィック (ソウル)	914738172881
eu-north-1	欧州 (ストックホルム)	591436053604
ap-east-1	アジアパシフィック (香港)	258348409381
me-south-1	中東 (バーレーン)	536382113932
eu-west-2	欧州 (ロンドン)	892757235363
ap-northeast-1	アジアパシフィック (東京)	533107202818
ap-southeast-1	アジアパシフィック (シンガポール)	174946120834
ap-south-1	アジアパシフィック (ムンバイ)	251508486986
ap-southeast-3	アジアパシフィック (ジャカルタ)	510637619217
sa-east-1	南米 (サンパウロ)	758426053663
ap-northeast-3	アジアパシフィック (大阪)	273192626886
eu-south-1	欧州 (ミラノ)	266869475730
af-south-1	アフリカ (ケープタウン)	197869348890
ap-southeast-2	アジアパシフィック (シドニー)	005257825471
me-central-1	中東 (アラブ首長国連邦)	000014521398
us-west-1	米国西部 (北カリフォルニア)	684579721401

ca-central-1	カナダ (中部)	354763396469
ap-south-2	アジアパシフィック (ハイデラバード)	950823858135
eu-south-2	欧州 (スペイン)	919611009337
eu-central-2	欧州 (チューリッヒ)	529164026651
ap-southeast-4	アジアパシフィック (メルボルン)	251357961535
il-central-1	イスラエル (テルアビブ)	870907303882

GuardDuty のセキュリティエージェント AWS Fargate (Amazon ECS のみ)

次の表は、Fargate GuardDuty のセキュリティエージェントのリリースバージョン履歴を示しています (Amazon ECS のみ)。

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日
v1.2.0	x86_64 (AMD64): sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93 Graviton (ARM64): sha256:91930f8446f5f95b93b8ccb18773992affa401eb3f42da89d68077a56bafa6cd	一般的なパフォーマンスのチューニングと機能強化	2024 年 5 月 31 日
v1.1.0	x86_64 (AMD64): sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c	新しいセキュリティシグナルと検出結果をサポート	2024 年 5 月 1 日

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日
	9f673f2835823957e9dcf71657 Graviton (ARM64): sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7	一般的なパフォーマンスのチューニングと機能強化	
v1.0.1	x86_64 (AMD64): sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68 Graviton (ARM64): sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7	一般的なパフォーマンスのチューニングと機能強化	2024 年 1 月 26 日
v1.0.0	x86_64 (AMD64): sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017 Graviton (ARM64): sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984	のセキュリティ GuardDuty エージェントの初回リリース AWS Fargate (Amazon ECS のみ）。	2023 年 11 月 26 日

GuardDuty Amazon EKS クラスター用の セキュリティエージェント

次の表は、Amazon EKS アドオン GuardDuty エージェント のリリースバージョン履歴を示しています。

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日	標準サポートの終了[1]
v1.6.1	x86_64 (AMD64): sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1 Graviton (ARM64): sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019	一般的なパフォーマンスのチューニングと機能強化。	2024 年 5 月 14 日	–
v1.6.0	x86_64 (AMD64): sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010 Graviton (ARM64): sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650	• EKS/EC2 リソース GuardDuty の自動エージェント設定をサポートします。 • 新しいセキュリティシグナルと検出結果をサポートします。詳細については、「GuardDuty 使用する収	2024 年 4 月 29 日	–

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日	標準サポートの終了[1]
		集済みランタイムイベントタイプ」および「Runtime Monitoring の検出結果タイプ」を参照してください。 • 一般的なパフォーマンスのチューニングと機能強化。		

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日	標準サポートの終了[1]
v1.5.0	x86_64 (AMD64): sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d Graviton (ARM64): sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6	• 一般的なパフォーマンスのチューニングと機能強化。 • の新しいイベントタイプを含むセキュリティの強化収集されたランタイムイベントタイプ。 • CPU 使用率に関するパフォーマンスの向上。	2024 年 3 月 7 日	–
v1.4.1	x86_64 (AMD64): sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c Graviton (ARM64): sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40	一般的なパフォーマンスのチューニングと機能強化。	2024 年 1 月 16 日	–

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日	標準サポートの終了[1]
v1.4.0	x86_64 (AMD64): sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f Graviton (ARM64): sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e	マニフェストマウントポイントがより良いデータ収集をサポート AppArmor マニフェストの設定 コマンドライン引数を収集する 一般的なパフォーマンスのチューニングと機能強化	2023 年 12 月 21 日	–
v1.3.1	x86_64 (AMD64): sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29 Graviton (ARM64): sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd	重要なセキュリティパッチと更新。	2023 年 10 月 23 日	–

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日	標準サポートの終了[1]
v1.3.0	x86_64 (AMD64): sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694 Graviton (ARM64): sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb	Ubuntu プラットフォームをサポートしています Kubernetes バージョン 1.28 をサポートしています 一般的なパフォーマンスの向上と安定性の向上。	2023 年 10 月 5 日	–

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日	標準サポートの終了[1]
v1.2.0	x86_64 (AMD64): sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3 Graviton (ARM64): sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa	AMD64 ベースのインスタンスに加えて、v1.2.0 では ARM64 ベースのインスタンスもサポートされるようになりました。Bottlerocket のサポートが追加、検証されました Kubernetes バージョン 1.27 をサポートしています 一般的なパフォーマンスの向上と安定性の向上。	2023 年 6 月 16 日	–

エージェントのバージョン	コンテナイメージ	リリースノート	利用可能日	標準サポートの終了[1]
v1.1.0	sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c	GuardDuty セキュリティエージェントがサポートする Kubernetes バージョンに加え、このエージェントリリースは Kubernetes バージョン 1.26 もサポートしています 一般的なパフォーマンスの向上と安定性の向上。	2023 年 5 月 2 日	2024 年 5 月 14 日
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e	Amazon EKS アドオンエージェントの初回リリース。	2023 年 3 月 30 日	2024 年 5 月 14 日

- [1] 標準サポートの終了に近づいている現在のエージェントバージョンの更新については、「」を参照してくださいセキュリティエージェントの手動更新。

リソースの無効化とクリーンアップの影響

このセクションは、Runtime Monitoring を無効にする AWS アカウント か、リソースタイプの GuardDuty 自動エージェント設定のみを無効にする場合、 に適用されます。

GuardDuty 自動エージェント設定の無効化

GuardDuty は、リソースにデプロイされているセキュリティエージェントを削除しません。ただし、 GuardDuty はセキュリティエージェントの更新の管理を停止します。

GuardDuty は、 リソースタイプからランタイムイベントを受信し続けます。使用状況統計への影響を防ぐには、リソースから GuardDuty セキュリティエージェントを削除してください。

が共有 VPC エンドポイント AWS アカウント を使用するかどうかにかかわらず、 GuardDuty VPC エンドポイントは削除されません。必要に応じて、VPC エンドポイントを手動で削除する必要があります。

Runtime Monitoring と EKS Runtime Monitoring の無効化

このセクションは、以下のシナリオで適用されます。

- EKS Runtime Monitoring を個別に有効にしたことはなく、Runtime Monitoring を無効にしました。
- Runtime Monitoring と EKS Runtime Monitoring の両方を無効にしています。EKS Runtime Monitoring の設定ステータスが不明な場合は、「」を参照してくださいEKS Runtime Monitoring 設定ステータスの確認。

> **EKS Runtime Monitoring を無効にせずに Runtime Monitoring を無効にする**
>
> このシナリオでは、ある時点で EKS Runtime Monitoring を有効にし、後で EKS Runtime Monitoring を無効にせずに Runtime Monitoring も有効にしました。
> ここで、Runtime Monitoring を無効にすると、EKS Runtime Monitoring も無効にする必要があります。無効にしないと、EKS Runtime Monitoring の使用コストが引き続き発生します。

前述のシナリオが当てはまる場合、 GuardDuty はアカウントで次のアクションを実行します。

- GuardDuty は、`GuardDutyManaged : true` タグを持つ VPC を削除します。これは、自動セキュリティエージェントを管理するために が作成した VPC GuardDuty です。
- GuardDuty は、 としてタグ付けされたセキュリティグループを削除しますGuardDutyManagedtrue。
- 少なくとも 1 つの参加者アカウントで使用されている共有 VPC の場合、 は VPC エンドポイントも共有 VPC リソースに関連付けられたセキュリティグループも削除 GuardDuty しません。

- Amazon EKS リソースの場合、 はセキュリティエージェント GuardDuty を削除します。これは、手動で管理したか、 を通じて管理したかには関係ありません GuardDuty。

  Amazon ECS リソースの場合、ECS タスクはイミュータブルであるため、そのリソースからセキュリティエージェントをアンインストール GuardDuty することはできません。これは、セキュリティエージェントの管理方法とは無関係です。手動または 経由で自動的に行います GuardDuty。Runtime Monitoring を無効にした後、新しい ECS タスクの実行が開始されると、はサイドカーコンテナをアタッチ GuardDuty しません。Fargate-ECS タスクの操作については、「」を参照してくださいRuntime Monitoring と Fargate の連携方法 (Amazon ECS のみ)。

  Amazon EC2 リソースの場合、 は、次の条件を満たす場合にのみ、Systems Manager (SSM) が管理するすべての Amazon EC2 インスタンスからセキュリティエージェントを GuardDuty アンインストールします。

  - リソースに `GuardDutyManaged : false` 除外タグが付けられていません。
  - GuardDuty には、インスタンスメタデータのタグにアクセスするためのアクセス許可が必要です。この EC2 リソースでは、インスタンスメタデータのタグへのアクセスは を許可するに設定されます。

セキュリティエージェントの手動管理を停止した場合

GuardDuty セキュリティエージェントのデプロイと管理にどのアプローチを使用するかにかかわらず、リソース内のランタイムイベントのモニタリングを停止するには、 GuardDuty セキュリティエージェントを削除する必要があります。アカウントのリソースタイプからランタイムイベントのモニタリングを停止する場合は、Amazon VPC エンドポイントを削除することもできます。

セキュリティエージェントリソースをクリーンアップするプロセス

Amazon VPC エンドポイントを削除するには

- 共有 VPC がない場合 – アカウントのリソースをモニタリングする必要がなくなった場合は、Amazon VPC エンドポイントの削除を検討してください。
- 共有 VPC を使用する場合 – 共有 VPC 所有者アカウントが、まだ使用されていた共有 VPC リソースを削除すると、共有 VPC 所有者アカウントと参加アカウントのリソースの Runtime Monitoring (および該当する場合は EKS Runtime Monitoring) カバレッジステータスが異常になる可能性があります。カバレッジステータスの詳細については、「」を参照してくださいリソースのランタイムカバレッジの評価。

詳細については、「インターフェイスエンドポイントを削除する」を参照してください。

セキュリティグループを削除するには

- 共有 VPC がない場合 – アカウントのリソースタイプをモニタリングする必要がなくなった場合は、Amazon VPC に関連付けられたセキュリティグループを削除することを検討してください。
- 共有 VPC の場合 – 共有 VPC 所有者アカウントがセキュリティグループを削除すると、共有 VPC に関連付けられたセキュリティグループを現在使用している参加者アカウント、共有 VPC 所有者アカウントおよび参加アカウントのリソースの Runtime Monitoring カバレッジステータスが異常になる可能性があります。詳細については、「リソースのランタイムカバレッジの評価」を参照してください。

詳細については、「セキュリティグループの削除」を参照してください。

EKS クラスターから GuardDuty セキュリティエージェントを削除するには

モニタリングしなくなった EKS クラスターからセキュリティエージェントを削除するには、「アドオンの削除」を参照してください。

EKS アドオンエージェントを削除しても、EKS クラスターから `amazon-guardduty` 名前空間は削除されません。`amazon-guardduty` 名前空間を削除するには、「名前空間の削除」を参照します。

`amazon-guardduty`名前空間を削除するには (EKS クラスター)

自動エージェント設定を無効にしても、EKS クラスターから `amazon-guardduty` 名前空間は自動的に削除されません。`amazon-guardduty` 名前空間を削除するには、「名前空間の削除」を参照します。

Amazon での Amazon S3 Protection GuardDuty

S3 Protection は、オブジェクトレベルの API オペレーションを含む Amazon Simple Storage Service (Amazon S3) AWS CloudTrail のデータイベントを Amazon が GuardDuty モニタリングして、Amazon S3 バケット内のデータの潜在的なセキュリティリスクを特定するのに役立ちます。

GuardDuty は AWS CloudTrail 、管理イベントと AWS CloudTrail S3 データイベントの両方をモニタリングして、Amazon S3 リソース内の潜在的な脅威を特定します。両方のデータソースでは、さまざまな種類のアクティビティについてモニタリングが行われます。S3 CloudTrail の管理イベントの例には、、、 などの Amazon S3 `ListBuckets`バケットを一覧表示または設定するオペレーションが含まれます`DeleteBucketsPutBucketReplication`。S3 CloudTrail のデータイベントの例には、`GetObject`、、、 などのオブジェクトレベルの API `ListObjects`オペレーションが含まれます`DeleteObject``PutObject`。

GuardDuty で Amazon を有効にすると AWS アカウント、 は CloudTrail 管理イベントのモニタリング GuardDuty を開始します。で S3 データイベントログを手動で有効化または設定する必要はありません AWS CloudTrail。S3 Protection 機能 (S3 CloudTrail のデータイベントをモニタリングする) は GuardDuty、この機能 AWS リージョン が Amazon 内で利用可能な任意の の任意のアカウントでいつでも有効にできます。既に を有効に AWS アカウント している では GuardDuty、30 日間の無料トライアル期間で S3 Protection を初めて有効にできます。を初めて有効に AWS アカウント する GuardDuty の場合、S3 Protection は既に有効になっており、この 30 日間の無料トライアルに含まれています。詳細については、「 GuardDuty コストの見積もり」を参照してください。

で S3 Protection を有効にすることをお勧めします GuardDuty。この機能が有効になっていない場合、 は Amazon S3 バケットを完全にモニタリングしたり、S3 バケットに保存されているデータへの疑わしいアクセスに関する検出結果を生成したり GuardDuty することはできません。

が S3 データイベント GuardDuty を使用する方法

S3 データイベント (S3 Protection) を有効にすると、 GuardDuty はすべての S3 バケットからの S3 データイベントを分析し、悪意のあるアクティビティや疑わしいアクティビティがないか監視します。詳細については、「AWS CloudTrail S3 のデータイベント」を参照してください。

認証されていないユーザーが S3 オブジェクトにアクセスする場合、その S3 オブジェクトはパブリックにアクセス可能であることを意味します。したがって、 GuardDuty はそのようなリクエストを処理しません。 は、有効な IAM (AWS Identity and Access Management) または AWS STS (AWS Security Token Service) 認証情報を使用して S3 オブジェクトに対して行われたリクエスト GuardDuty を処理します。

が S3 データイベントのモニタリングに基づいて潜在的な脅威 GuardDuty を検出すると、セキュリティ上の検出結果が生成されます。Amazon S3 バケットに対して生成 GuardDuty できる検出結果のタイプについては、「」を参照してくださいGuardDuty S3 検索タイプ。

S3 Protection を無効にすると、 は S3 バケットに保存されているデータの S3 データイベントモニタリングを GuardDuty 停止します。

スタンドアロンアカウントの S3 Protection の設定。

によって関連付けられたアカウントの場合 AWS Organizations、このプロセスはコンソール設定を使用して自動化できます。詳細については、「マルチアカウント環境での S3 Protection の設定」を参照してください。

S3 Protection を有効または無効にするには

任意のアクセス方法を選択して、スタンドアロンアカウントのために S3 Protection を設定します。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[S3 Protection] を選択します。
3. [S3 Protection] ページには、アカウントの S3 Protection の現在のステータスが表示されます。[有効にする] または [無効にする] を選択すると、いつでも S3 Protection を有効または無効にできます。
4. [確認] を選択して、選択を確定します。

API/CLI

1. 現在のリージョンの有効なディテクター ID を使用し、S3 Protection を有効または無効にするように `ENABLED` または `DISABLED` に設定された `features` オブジェクト `name` を `S3_DATA_EVENTS` として渡して updateDetector を実行します。

> **Note**
>
> アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、ListDetectors API を実行します。

2. または、 を使用することもできます AWS Command Line Interface。S3 Protection を有効にするには、次のコマンドを実行し、必ず独自の有効なディテクター ID を使用してください。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

S3 Protection を無効にするには、例の ENABLED を DISABLED に置き換えます。

マルチアカウント環境での S3 Protection の設定

マルチアカウント環境では、委任された GuardDuty 管理者アカウントのみが、組織内のメンバーアカウントの S3 Protection を設定 (有効または無効に) できます AWS 。 GuardDuty メンバーアカウントは、自分のアカウントからこの設定を変更することはできません。委任 GuardDuty 管理者アカウントは、 を使用してメンバーアカウントを管理します AWS Organizations。委任された GuardDuty 管理者アカウントは、組織内のすべてのアカウントで S3 Protection を自動的に有効にするか、新しいアカウントのみで有効にするか、組織内のアカウントなしで有効にするかを選択できます。詳細については、「AWS Organizationsを使用したアカウントの管理」を参照してください。

委任 GuardDuty 管理者アカウントの S3 Protection の設定

任意のアクセス方法を選択して、委任された GuardDuty 管理者アカウントの S3 Protection を設定します。

Console

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

   必ず管理アカウントの認証情報を使用してください。
2. ナビゲーションペインで、[S3 Protection] を選択します。
3. [S3 Protection] ページで、[編集] を選択します。

4. 次のいずれかを行います。

   [すべてのアカウントについて有効にする] の使用

   - [すべてのアカウントについて有効にする] を選択します。これにより、 AWS 組織に参加する新しい GuardDuty アカウントを含め、組織内のすべてのアクティブなアカウントに対して保護プランが有効になります。
   - [保存] を選択します。

   [アカウントを手動で設定] の使用

   - 委任された GuardDuty 管理者アカウントアカウントに対してのみ保護プランを有効にするには、アカウントを手動で設定 を選択します。
   - 委任された GuardDuty 管理者アカウント (このアカウント) セクションで 有効化 を選択します。
   - [保存] を選択します。

API/CLI

現在のリージョンの委任 GuardDuty 管理者アカウントのディテクター ID を使用して、`features` オブジェクトを として、 `S3_DATA_EVENTS` nameを `ENABLED`または `status`として渡updateDetectorして、 を実行します`DISABLED`。

または、 を使用して S3 Protection を設定することもできます AWS Command Line Interface。次のコマンドを実行し、*12abc34d567e8fa901bc2d34e56789f0* を現在のリージョンの委任 GuardDuty 管理者アカウントのディテクター ID に、*555555555555* を委任 GuardDuty 管理者アカウントの AWS アカウント ID に置き換えます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "S3_DATA_EVENTS", "Status":
 "ENABLED"}]'
```

組織内のすべてのメンバーアカウントのために S3 Protection を自動的に有効にする

Console

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

   管理者アカウントを使用してサインインします。

2. 次のいずれかを行います。

   [S3 Protection] ページの使用

   1. ナビゲーションペインで、[S3 Protection] を選択します。
   2. [すべてのアカウントについて有効にする] を選択します。このアクションにより、組織内の既存のアカウントと新しいアカウントの両方について S3 Protection が自動的に有効になります。
   3. [保存] を選択します。

   > **Note**
   >
   > メンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

   [アカウント] ページの使用

   1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
   2. [アカウント] ページで、[招待によるアカウントの追加] の前に [自動有効化] の詳細設定を選択します。
   3. [自動有効化の詳細設定を管理] ウィンドウで、[S3 Protection] の下の [すべてのアカウントについて有効にする] を選択します。
   4. [保存] を選択します。

   [すべてのアカウントについて有効にする] オプションを使用できない場合は、「メンバーアカウントで S3 Protection を選択的に有効または無効にする」を参照してください。

API/CLI

- メンバーアカウントの S3 Protection を選択的に有効または無効にするには、ユーザー独自の`###### ID` を使用して updateMemberDetectors API オペレーションを起動します。
- 次の例では、単一のメンバーアカウントで S3 Protection を有効にする方法を示しています。必ず `12abc34d567e8fa901bc2d34e56789f0` detector-idを委任 GuardDuty 管理者アカウントの 、および `111122223333` に置き換えてください。S3 Protection を無効にするには、ENABLED を DISABLED に置き換えます。

  アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

  > **Note**
  >
  > スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

すべての既存のアクティブなメンバーアカウントのために S3 Protection を有効にする

任意のアクセス方法を選択して、組織内のすべての既存のアクティブなメンバーアカウントのために S3 Protection を有効にします。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   委任 GuardDuty 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[S3 Protection] を選択します。

3. [S3 Protection] ページでは、設定の現在のステータスを表示できます。[アクティブなメンバーアカウント] セクションで、[アクション] を選択します。
4. [アクション] ドロップダウンメニューから、[すべての既存のアクティブなメンバーアカウントについて有効にする] を選択します。
5. [確認] を選択します。

API/CLI

- メンバーアカウントの S3 Protection を選択的に有効または無効にするには、ユーザー独自の`###### ID` を使用して updateMemberDetectors API オペレーションを起動します。
- 次の例では、単一のメンバーアカウントで S3 Protection を有効にする方法を示しています。必ず `12abc34d567e8fa901bc2d34e56789f0` `detector-id`を委任 GuardDuty 管理者アカウントの 、および `111122223333` に置き換えてください。S3 Protection を無効にするには、`ENABLED` を `DISABLED` に置き換えます。

  アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

新しいメンバーアカウントの S3 Protection を自動で有効にする

任意のアクセス方法を選択して、組織に参加する新しいアカウントのために S3 Protection を有効にします。

Console

委任 GuardDuty 管理者アカウントは、S3 Protection または Accounts ページを使用して、コンソールから組織内の新しいメンバーアカウントに対して を有効にできます。

新しいメンバーアカウントの S3 Protection を自動で有効にするには

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。

2. 次のいずれかを行います。

   - [S3 Protection] ページの使用:

     1. ナビゲーションペインで、[S3 Protection] を選択します。
     2. [S3 Protection] ページで、[編集] を選択します。
     3. [アカウントを手動で設定] を選択します。
     4. [新しいメンバーアカウントについて自動的に有効にする] を選択します。このステップにより、新しいアカウントが組織に参加するたびに、そのアカウントのために S3 Protection が自動的に有効になります。この設定を変更できるのは、組織の委任 GuardDuty 管理者アカウントのみです。
     5. [保存] を選択します。

   - [Accounts] (アカウント) ページを使用する場合:

     1. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
     2. [アカウント] ページで、[自動有効化] 設定を選択します。
     3. [自動有効化の詳細設定を管理] ウィンドウで、[S3 Protection] の下の [新しいアカウントについて有効にする] を選択します。
     4. [保存] を選択します。

API/CLI

- メンバーアカウントの S3 Protection を選択的に有効または無効にするには、ユーザー独自の`###### ID` を使用して UpdateOrganizationConfiguration API オペレーションを起動します。
- 次の例では、単一のメンバーアカウントで S3 Protection を有効にする方法を示しています。無効にするには、「メンバーアカウントを選択して RDS Protection を有効または無効にする」

を参照してください。組織に参加する新しいアカウント (NEW) もしくはすべてのアカウント (ALL) のために、そのリージョンで保護プランを自動的に有効または無効にするか、または組織内のどのアカウントのためにも自動的に有効または無効にしない (NONE) 詳細設定を行います。詳細については、autoEnableOrganization「メンバー」を参照してください。必要に応じて、NEW を ALL または NONE に置き換える必要がある場合があります。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

- コードが正常に実行されると、UnprocessedAccounts の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

メンバーアカウントで S3 Protection を選択的に有効または無効にする

任意のアクセス方法を選択して、メンバーアカウントのために S3 Protection を選択的に有効または無効にします。

Console

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

   委任された GuardDuty 管理者アカウントの認証情報を使用してください。

2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

   [アカウント] ページで、[S3 Protection] 列でメンバーアカウントのステータスを確認します。

3. S3 Protection を選択的に有効または無効にするには

   S3 Protection を設定するアカウントを選択します。一度に複数のアカウントを選択できます。[保護プランの編集] ドロップダウンメニューで、[S3Pro] を選択し、適切なオプションを選択します。

API/CLI

メンバーアカウントの S3 Protection を選択的に有効または無効にするには、自身のディテクター ID を使用し、updateMemberDetectors API オペレーションを実行します。次の例では、単一のメンバーアカウントで S3 Protection を有効にする方法を示しています。無効にするには、`true` を `false` に置き換えます。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> スペースで区切られたアカウント ID のリストを渡すこともできます。

コードが正常に実行されると、`UnprocessedAccounts` の空のリストが返されます。アカウントのディテクター設定を変更する際に問題が発生した場合は、そのアカウント ID と問題の概要が表示されます。

> **Note**
>
> スクリプトを使用して新しいアカウントをオンボーディングし、新しいアカウントで S3 Protection を無効にする場合は、このトピックで説明されているように、オプションの `dataSources` オブジェクトで createDetector API オペレーションを変更できます。

新しい GuardDuty アカウントの S3 Protection を自動的に無効にする

> **Important**
>
> デフォルトでは、 AWS アカウント S3 Protection はその結合 GuardDuty に対して初めて自動的に有効になります。

新しいアカウント GuardDuty で を初めて有効にする GuardDuty 管理者アカウントで、S3 Protection をデフォルトで有効にしない場合は、オプションの `features` オブジェクトで createDetector API オペレーションを変更することで無効にできます。次の例では、 を使用して AWS CLI 、S3 Protection が無効になっている新しい GuardDuty ディテクターを有効にします。

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

S3 Protection の機能

AWS CloudTrail S3 のデータイベント

データプレーンオペレーションとして知られるデータイベントは、リソース上またはリソース内で実行したリソースオペレーションに関するインサイトを提供します。それらは、多くの場合、高ボリュームのアクティビティです。

以下は、 がモニタリング GuardDuty できる S3 CloudTrail のデータイベントの例です。

- `GetObject` API オペレーション
- `PutObject` API オペレーション
- `ListObjects` API オペレーション
- `DeleteObject` API オペレーション

GuardDuty を初めて有効にすると、S3 Protection はデフォルトで有効になり、30 日間の無料トライアル期間にも含まれます。ただし、この機能はオプションであり、いつでもアカウントまたはリージョンについて有効または無効にすることを選択できます。機能としての Amazon S3 の設定の詳細については、「GuardDuty S3 保護」を参照してください。

Amazon GuardDuty の検出結果について

GuardDuty 検出結果は、ネットワーク内で検出された潜在的なセキュリティ問題を表します。GuardDuty は、 AWS 環境で予期しないアクティビティや悪意のある可能性のあるアクティビティを検出するたびに検出結果を生成します。

GuardDuty 検出結果は、 GuardDuty コンソールの「検出結果」ページで、または AWS CLI または API オペレーションを使用して表示および管理できます。検出結果の管理方法の概要については、「Amazon の検出 GuardDuty 結果の管理」を参照してください。

トピック:

検出結果の詳細

アカウントで生成される GuardDuty 検出結果に関連する詳細について説明します。

GuardDuty の検出結果の形式

検出 GuardDuty 結果タイプの形式と、 によって追跡されるさまざまな脅威の目的を理解します GuardDuty。

サンプルの検出結果

サンプルの検出結果を生成して、 GuardDuty 検出結果と関連の詳細をテストして理解してみてください。これらの検出結果は、プレフィックス [SAMPLE] でマークされます。

専用アカウントで GuardDuty の検出結果のテスト

専用の非本番環境で`guardduty-tester`スクリプトを実行して AWS アカウント 、 AWS 環境で選択した GuardDuty 結果を生成します。

検出結果タイプ

使用可能なすべての GuardDuty 検出結果をタイプ別に表示および検索します。各検出結果タイプの内容には、その検出結果の説明と修復のためのヒントと推奨事項が含まれています。

検出結果の詳細

Amazon GuardDuty コンソールでは、検出結果の概要セクションで検出結果の詳細を表示できます。検出結果の詳細は検出結果のタイプによって異なります。

検出結果にどのような情報が表示されるかを決める基本的な情報が 2 つあります。1 つ目はリソースタイプで、`Instance`、、`AccessKey`、`S3Bucket`、`S3Object`、`Kubernetes cluster`、、`ECS`

cluster、RDSDBInstanceまたは ContainerですLambda。情報の検出結果を決定する 2 つ目の詳細は [リソースロール] です。リソースロールは、アクセスキー用の Target である可能性があります。つまり、リソースが疑わしいアクティビティのターゲットであったことを意味します。インスタンスタイプの検出結果については、リソースロールが Actor である場合があります。つまり、リソースが不審なアクティビティを実行するアクターだったことを意味します。このトピックでは、検出結果の一般的に入手可能な詳細をいくつか説明します。

検出結果の概要

検出結果の概要のセクションには、次の情報を含む、検索条件の最も基本的な識別機能が含まれています。

- アカウント ID – この検出結果を生成する GuardDuty ように促したアクティビティが行われたアカウントの ID AWS 。
- カウント — このパターン GuardDuty とこの検出結果 ID に一致するアクティビティを集計した回数。
- 作成時刻 - この検出結果が初めて生成された日時。この値が [Updated at] (更新時刻) と異なる場合は、そのアクティビティが複数回発生しており、現在も進行中の問題でありことを示しています。

> **Note**
>
> GuardDuty コンソールの結果のタイムスタンプはローカルタイムゾーンに表示されますが、JSON エクスポートと CLI 出力にはタイムスタンプが UTC で表示されます。

- [Finding ID] (結果 ID) - この検出結果タイプおよびパラメータセットに対応する一意の識別子です。このパターンに一致するアクティビティが新しく出現した場合は、同じ ID に集約されます。
- [結果タイプ] - 検出結果をトリガーしたアクティビティのタイプを表す、書式設定された文字列。詳細については、「GuardDuty の検出結果の形式」を参照してください。
- リージョン — 結果が生成された AWS リージョン。サポートされるリージョンについては、「リージョンとエンドポイント」を参照してください。
- リソース ID – この検出結果を生成する GuardDuty ように促したアクティビティが行われたリソースの AWS ID。
- スキャン ID – GuardDuty Malware Protection for EC2 が有効になっている場合の検出結果に適用されます。これは、侵害された可能性のある EC2 インスタンスまたはコンテナワークロードにアタッチされた EBS ボリュームで実行されるマルウェアスキャンの識別子です。詳細については、「Malware Protection for EC2 の検出結果の詳細」を参照してください。

- 重要度 - [High] (高)、[Medium] (中)、[Low] (低) のいずれかで割り当てられた検出結果の重要度。詳細については、「GuardDuty 検出結果の重要度レベル」を参照してください。
- 更新日時 — この検出結果が最後に更新されたのは、この検出結果を生成するように促 GuardDuty したパターンに一致する新しいアクティビティです。

リソース

影響を受けるリソースは、開始アクティビティのターゲットとなった AWS リソースに関する詳細を提供します。利用可能な情報は、リソースタイプとアクションタイプによって異なります。

リソースロール — 検出結果を開始した AWS リソースのロール。値は [TARGET] または [ACTOR] で、それぞれの値は、リソースが疑わしいアクティビティの対象であったか、疑わしいアクティビティを実行したアクターであったことを表します。

リソースタイプ - 該当するリソースのタイプ。複数のリソースが関係していた場合は、複数のリソースタイプが検出結果に含まれる可能性があります。リソースタイプは、インスタンス 、AccessKey、S3Bucket、S3Object、KubernetesCluster、ECSCluster、コンテナ 、RDSDBInstance、および Lambda です。リソースタイプによって、使用可能な検出結果の詳細が異なります。リソースオプションタブを選択して、そのリソースで使用可能な詳細について説明します。

Instance

インスタンスの詳細:

> **Note**
>
> インスタンスが既に停止している場合、またはクロスリージョン API コールを行うときに別のリージョンの EC2 インスタンスから基盤となる API コールが発生した場合、インスタンスの詳細が欠落することがあります。

- インスタンス ID – 検出結果を生成する GuardDuty ように促したアクティビティに関係する EC2 インスタンスの ID。
- インスタンスタイプ - 検出結果に関連する EC2 インスタンスのタイプ。
- [起動時刻] - インスタンスが開始された日時
- Outpost ARN – の Amazon リソースネーム (ARN) AWS Outposts。 AWS Outposts インスタンスにのみ適用されます。詳細については、「AWS Outpostsとは」を参照してください。

- [セキュリティグループ名] - 関連するインスタンスに付属するセキュリティグループの名前。
- [セキュリティグループ ID] - 関係するインスタンスに付属するセキュリティグループの ID。
- [インスタンスの状態]- ターゲットインスタンスの現在の状態。
- [アベイラビリティーゾーン] - 関連するインスタンスが配置されている AWS リージョンアベイラビリティーゾーン。
- [イメージ ID] - アクティビティに関連するインスタンスの構築に使用される Amazon マシンイメージの ID。
- [イメージの説明] - アクティビティに関連するインスタンスの構築に使用される Amazon マシンイメージの ID に関する説明。
- [タグ] - このリソースにアタッチされているタグのリスト。リストの形式は `key:value` です。

AccessKey

アクセスキーの詳細:

- アクセスキー ID – 検出結果を生成する GuardDuty ように促したアクティビティに従事したユーザーのアクセスキー ID。
- プリンシパル ID – 検出結果を生成するよう促 GuardDutyしたアクティビティに従事したユーザーのプリンシパル ID。
- ユーザータイプ - 検出結果を生成する GuardDuty よう促したアクティビティにエンゲージしたユーザーのタイプ。詳細については、「CloudTrail userIdentity 要素」を参照してください。
- ユーザー名 – 検出結果を生成する GuardDuty よう促したアクティビティにエンゲージしたユーザーの名前。

S3Bucket

Amazon S3 バケットの詳細

- [名前] - 検出結果に関連するバケットの名前。
- [ARN] – 検出結果に関連するバケットの ARN。
- [所有者] - 検出結果に関連するバケットを所有するユーザーの正規ユーザー ID。正規ユーザー ID の詳細については、「AWS アカウント ID」を参照してください。
- [タイプ] - バケット検出結果のタイプで、[送信先] または [ソース] になります。
- デフォルトのサーバー側暗号化 - バケットの暗号化に関する詳細。

- バケットタグ - このリソースにアタッチされたタグのリスト。リストの形式は `key:value` です。
- [有効な許可] - 関連するバケットが公開されているかどうかを示す、バケットに関するすべての有効な許可とポリシーの評価。値は [公開] または [非公開] です。

S3Object

- S3 オブジェクトの詳細 — スキャンされた S3 オブジェクトに関する以下の情報が含まれます。
  - ARN – スキャンされた S3 オブジェクトの Amazon リソースネーム (ARN)。
  - キー — S3 バケットで作成されたときにファイルに割り当てられた名前。
  - バージョン ID – バケットのバージョニングを有効にすると、このフィールドには、スキャンされた S3 オブジェクトの最新バージョンに関連付けられたバージョン ID が表示されます。詳細については、『Amazon S3 ユーザーガイド』の「S3 バケットでのバージョニングの使用」を参照してください。
  - eTag – スキャンされた S3 オブジェクトの特定のバージョンを表します。
  - Hash – この検出結果で検出された脅威のハッシュ。
- S3 バケットの詳細 — スキャンされた Amazon S3S3 バケットに関する以下の情報が含まれます。
  - 名前 — オブジェクトを含む S3 バケットの名前を示します。
  - ARN – S3 バケットの Amazon リソースネーム (ARN)。
- 所有者 – S3 バケットの所有者の正規 ID。

EKSCluster

Kubernetes クラスターの詳細:

- 名前 — Kubernetes クラスターの名前。
- ARN — クラスターを識別する ARN。
- 作成時刻 - このクラスターが生成された日時。

> **Note**
>
> GuardDuty コンソールの結果のタイムスタンプはローカルタイムゾーンに表示されますが、JSON エクスポートと CLI 出力にはタイムスタンプが UTC で表示されます。

- VPC ID — クラスターに関連付けられている VPC ID。
- 状態 – クラスターの現在の状態。
- タグ - クラスターに適用し、クラスターの分類と整理に役立つメタデータ。各タグは、`key:value` 形式でリストされているキーとオプションの値で構成されます。キーと値の両方を定義できます。

  クラスタータグは、クラスターに関連付けられた他のリソースには伝達されません。

Kubernetes ワークロードの詳細:

- タイプ - ポッド、デプロイ、ジョブなどの Kubernetes ワークロードのタイプ。
- 名前 - Kubernetes ワークロードの名前。
- UID - Kubernetes ワークロードの固有の ID。
- 作成時刻 - このワークロードが生成された日時。
- ラベル - Kubernetes ワークロードにアタッチされたキーと値のペア。
- コンテナ - Kubernetes ワークロードの一部として実行されているコンテナの詳細。
- 名前空間 - ワークロードはこの Kubernetes 名前空間に属します。
- ボリューム - Kubernetes ワークロードが使用するボリューム。
  - ホストパス - ボリュームがマッピングされるホストマシン上の既存のファイルまたはディレクトリを示します。
  - 名前 - ボリュームの名前。
- ポッドセキュリティコンテキスト - ポッド内のすべてのコンテナの権限とアクセスコントロール設定を定義します。
- ホストネットワーク - ポッドが Kubernetes ワークロードに含まれている場合は `true` に設定します。

Kubernetes ユーザーの詳細

- グループ — 検出結果を生成したアクティビティに関与したユーザーの Kubernetes RBAC (ロールアクセスベースのコントロール) グループ。
- ID — Kubernetes ユーザーの固有の ID。
- ユーザー名 — 検出結果を生成したアクティビティに関係した Kubernetes ユーザーの名前。
- セッション名 — Kubernetes RBAC アクセス許可を持つ IAM ロールを引き受けたエンティティ。

ECSCluster

ECS クラスターの詳細

- ARN — クラスターを識別する ARN。
- 名前 - クラスターの名前。
- 状態 – クラスターの現在の状態。
- アクティブサービスの数 — ACTIVE 状態のクラスター内で実行されているサービスの数。これらのサービスは、 で表示できます。 ListServices
- 登録されたコンテナインスタンス数 — クラスターに登録されているコンテナインスタンスの数。これには、ACTIVE および DRAINING 状態の両方のコンテナインスタンスが含まれます
- 実行中のタスク数 — RUNNING 状態のクラスターのタスクの数。
- タグ - クラスターに適用し、クラスターの分類と整理に役立つメタデータ。各タグは、key:value 形式でリストされているキーとオプションの値で構成されます。キーと値の両方を定義できます。
- コンテナ – タスクに関連付けられたコンテナの詳細:
  - コンテナ名 – コンテナの名前。
  - コンテナイメージ – コンテナのイメージ。
- タスクの詳細 — クラスター内のタスクの詳細。
  - ARN – タスクの Amazon リソースネーム (ARN)。
  - 定義 ARN – タスクを作成するタスク定義の Amazon リソースネーム(ARN)。
  - バージョン– タスクのバージョンカウンター。
  - タスクの作成時刻 – タスクが作成されたときの Unix タイムスタンプ。
  - タスクの開始時刻 – タスクが開始されたときの Unix タイムスタンプ。
  - タスクの開始ユーザー – タスクの開始時に指定されたタグ。

Container

コンテナの詳細:

- コンテナランタイム — コンテナの実行に使用されたコンテナランタイム (`docker` または `containerd` など)。
- ID — コンテナインスタンスのコンテナインスタンス ID または完全な ARN エントリ。
- 名前 — コンテナの名前。

  使用可能な場合、このフィールドには `io.kubenetes.container.name` ラベルの値が表示されます。
- イメージ — コンテナインスタンスのイメージ。
- ボリュームマウント — コンテナボリュームのマウントのリスト。コンテナは、そのファイルシステムの下にボリュームをマウントできます。
- セキュリティコンテキスト — コンテナセキュリティコンテキストは、コンテナの権限とアクセス制御設定を定義します。
- プロセスの詳細 — 検出結果に関連付けられているプロセスの詳細が記述されます。

RDSDBInstance

RDSDBInstance の詳細:

> **Note**
>
> このリソースは、データベースインスタンスに関連する RDS Protection の検出結果で利用できます。

- データベースインスタンス ID — GuardDuty 検出結果に関与したデータベースインスタンスに関連付けられた識別子。
- [Engine] (エンジン) — 検出に関与したデータベースインスタンスのデータベースエンジン名。指定できる値は、Aurora MySQL 互換または Aurora PostgreSQL 互換です。
- エンジンバージョン — 検出結果に関与 GuardDutyしたデータベースエンジンのバージョン。
- データベースクラスター ID – GuardDuty 検出結果に関係するデータベースインスタンス ID を含むデータベースクラスターの識別子。

- データベースインスタンス ARN — 検出結果に関係する GuardDutyデータベースインスタンスを識別する ARN。

Lambda

Lambda 関数の詳細

- 関数名 - 検出結果に含まれた Lambda 関数の名前。
- 関数バージョン - 検出結果に含まれる Lambda 関数のバージョン。
- 関数の説明 - 検出結果に含まれた Lambda 関数の説明。
- 関数 ARN - 検出結果に含まれた Lambda 関数の Amazon リソースネーム (ARN)。
- リビジョン ID - Lambda 関数バージョンのリビジョン ID。
- ロール - 検出結果に関係する Lambda 関数の実行ロール。
- VPC 設定 - Lambda 関数に関連付けられた VPC ID、セキュリティグループ、サブネット ID を含む Amazon VPC 設定。
- VPC ID - 検出結果に含まれた Lambda 関数に関連付けられた Amazon VPC の ID。
- サブネット ID - Lambda 関数に関連付けられているサブネットの ID。
- セキュリティグループ - 関連する Lambda 関数にアタッチされたセキュリティグループ。これには、セキュリティグループ名とグループ ID が含まれます。
- タグ - このリソースにアタッチされているタグのリスト。リストの形式は `key:value` ペアです。

RDS データベース (DB) ユーザーの詳細

> **Note**
>
> このセクションは、 で RDS Protection 機能を有効にする場合の検出結果に適用されます GuardDuty。詳細については、「での RDS Protection GuardDuty」を参照してください。

この GuardDuty 検出結果は、侵害された可能性のあるデータベースの以下のユーザーと認証の詳細を提供します。

- [User] (ユーザー) - 異常なログイン試行に使用されたユーザー名

- [Application] (アプリケーション) — 異常なログイン試行に使用されたアプリケーション名
- [Database] (データベース) — 異常なログイン試行に関与したデータベースインスタンスの名前
- [SSL] — ネットワークに使用された Secure Socket Layer (SSL) のバージョン
- [認証方法] — 検出に関与したユーザーが使用した認証方法

Runtime Monitoring の検出結果の詳細

> **Note**
>
> これらの詳細は、 が の 1 つ GuardDuty を生成する場合にのみ使用できますRuntime Monitoring の検出結果タイプ。

このセクションには、プロセスの詳細や必要なコンテキストなど、ランタイムの詳細が含まれています。プロセスの詳細には、観察されたプロセスに関する情報が記述され、ランタイムのコンテキストには、潜在的に疑わしいアクティビティに関する追加情報が記述されます。

プロセスの詳細

- 名前 - プロセスの名前。
- 実行可能ファイルのパス - プロセスの実行可能ファイルの絶対パス。
- 実行可能ファイル SHA-256 - プロセスの実行可能ファイルの SHA256 ハッシュ。
- 名前空間 PID - ホストレベルの PID 名前空間以外のセカンダリ PID 名前空間内のプロセスのプロセス ID。コンテナ内のプロセスの場合、コンテナ内で確認されるプロセス ID です。
- 現在の作業ディレクトリ - プロセスの現在の作業ディレクトリ。
- プロセス ID - オペレーティングシステムによってプロセスに割り当てられた ID。
- startTime - プロセスが開始された時間。これは UTC 日付文字列形式 (`2023-03-22T19:37:20.168Z`) です。
- UUID – によってプロセスに割り当てられた一意の ID GuardDuty。
- 親 UUID - 親プロセスの固有の ID。この ID は、 によって親プロセスに割り当てられます GuardDuty。
- ユーザー - プロセスを実行したユーザー。
- ユーザー ID - プロセスを実行したユーザーの ID。

- 有効なユーザー ID - イベント発生時のプロセスの有効な実効ユーザー ID。
- 系列 - プロセスの先祖に関する情報。
  - プロセス ID - オペレーティングシステムによってプロセスに割り当てられた ID。
  - UUID – によってプロセスに割り当てられた一意の ID GuardDuty。
  - 実行可能ファイルのパス - プロセスの実行可能ファイルの絶対パス。
  - 有効なユーザー ID - イベント発生時のプロセスの有効な実効ユーザー ID。
  - 親 UUID - 親プロセスの固有の ID。この ID は、 によって親プロセスに割り当てられます GuardDuty。
  - 開始時間 - プロセスが開始された時間。
  - 名前空間 PID - ホストレベルの PID 名前空間以外のセカンダリ PID 名前空間内のプロセスのプロセス ID。コンテナ内のプロセスの場合、コンテナ内で確認されるプロセス ID です。
  - ユーザー ID - プロセスを実行したユーザーのユーザー ID。
  - 名前 - プロセスの名前。

ランタイムのコンテキスト

次のフィールドから、生成された検出結果には、その検出結果タイプに関連するフィールドのみが含まれる場合があります。

- マウントソース - コンテナによってマウントされたホスト上のパス。
- マウントターゲット - ホストディレクトリにマッピングされているコンテナ内のパス。
- ファイルシステムタイプ - マウントされたファイルシステムのタイプを示します。
- フラグ - この検出結果に関係するイベントの動作をコントロールするオプションを示します。
- プロセスの変更 - 実行時にコンテナ内でバイナリ、スクリプト、またはライブラリを作成または変更したプロセスに関する情報。
- 修正日時 - 実行時にプロセスがコンテナ内のバイナリ、スクリプト、またはライブラリを作成または変更したときのタイムスタンプ。このフィールドは、UTC 日付文字列形式 (`2023-03-22T19:37:20.168Z`)です。
- ライブラリパス - ロードされた新しいライブラリへのパス。
- LD プリロード値 - `LD_PRELOAD` 環境変数の値。
- ソケットパス - アクセスされた Docker ソケットへのパス。
- Runc バイナリパス - `runc` バイナリへのパス。
- リリースエージェントパス - `cgroup` リリースエージェントファイルへのパス。

- コマンドラインの例 — 疑わしい可能性があるアクティビティに関係するコマンドラインの例。
- ツールカテゴリ – ツールが属するカテゴリ。例としては、バックドアツール、ペネテストツール、ネットワークスキャナー、ネットワークスニッファーなどがあります。
- ツール名 – 疑わしい可能性があるツールの名前。
- スクリプトパス — 結果を生成した実行されたスクリプトへのパス。
- 脅威ファイルパス — 脅威インテリジェンスの詳細が見つかった疑わしいパス。
- サービス名 — 無効になっているセキュリティサービスの名前。

EBS ボリュームのスキャンの詳細

> **Note**
>
> このセクションは、 GuardDutyで 実行型マルウェアスキャンを有効にする場合の検出結果に適用されますGuardDuty EC2 のマルウェア保護。

EBS ボリュームスキャンは、侵害された可能性のある EC2 インスタンスまたはコンテナワークロードにアタッチされた EBS ボリュームに関する詳細を提供します。

- スキャン — マルウェアスキャンの識別子。
- スキャン開始日 — マルウェアスキャンが開始された日時。
- スキャン完了日 — 不正プログラムのスキャンの完了日時。
- 検出結果のトリガー ID — このマルウェアスキャンを開始した GuardDuty 検出結果の検出結果 ID。
- ソース — 可能な値は `Bitdefender`と ですAmazon。
- スキャン検出 — 各マルウェアスキャンの詳細と結果の全情報。
  - スキャンされたアイテム数 — スキャンされたファイルの合計数。`totalGb`、`files`、および `volumes` などの詳細を提供します。
  - 脅威が検出されたアイテム数 — スキャン中に検出された悪意のある `files` の合計数。
  - 最も重要度の高い脅威の詳細 — スキャン中に検出された、重要度が最も高い脅威の詳細と、悪意のあるファイルの数。`severity`、`threatName`、および `count` などの詳細を提供します。
  - 名前で検出された脅威 — すべての重要度レベルの脅威をグループ化するコンテナ要素。`itemCount`、`uniqueThreatNameCount`、`shortened`、および `threatNames` などの詳細を提供します。

Malware Protection for EC2 の検出結果の詳細

> **Note**
>
> このセクションは、 GuardDutyで 実行型マルウェアスキャンを有効にする場合の検出結果に適用されますGuardDuty EC2 のマルウェア保護。

Malware Protection for EC2 スキャンがマルウェアを検出すると、https://console.aws.amazon.com/guardduty/ コンソールの検出結果ページで対応する検出結果を選択することで、スキャンの詳細を表示できます。Malware Protection for EC2 の検出結果の重要度は、検出結果の GuardDuty重要度によって異なります。

> **Note**
>
> `GuardDutyFindingDetected` タグは、スナップショットにマルウェアが含まれていると指定します。

次の情報は、詳細パネルの「検出された脅威」セクションでご覧になれます。

- 名前 — 検出によってファイルをグループ化することによって取得された脅威の名前。
- 重要度 — 検出された脅威の重要度。
- ハッシュ – ファイルの SHA-256 ハッシュ。
- ファイルパス — EBS ボリューム内の悪意のあるファイルの場所。
- ファイル名 — 脅威が検出されたファイルの名前。
- ボリューム ARN — スキャンされた EBS ボリュームの ARN。

次の情報は、詳細パネルの「マルウェアスキャンの詳細」のセクションでご覧になれます。

- スキャン — 不正プログラムスキャンのスキャン ID。
- スキャン開始日 — スキャンが開始された日時。
- スキャン完了日 — スキャンの完了日時。
- スキャンされたファイル — スキャンされたファイルとディレクトリの合計数。
- スキャンされた合計 GB — プロセス中にスキャンされたストレージの容量。

- トリガー検出結果 ID — このマルウェアスキャンを開始した検出結果の検出 GuardDuty 結果 ID。
- 次の情報は、詳細パネルの「ボリュームの詳細」のセクションでご覧になれます。
  - ボリューム ARN — ボリュームの Amazon リソースネーム (ARN)。
  - SnapshotARN — EBS ボリュームのスナップショットの ARN。
  - ステータス — `Running`、`Skipped`、および `Completed` などのボリュームのスキャン状態。
  - 暗号化タイプ — ボリュームの暗号化に使用される暗号化のタイプ。例えば `CMCMK` です。
  - デバイス名 - デバイスの名前。例えば `/dev/xvda` です。

Malware Protection for S3 の検出結果の詳細

で S3 の GuardDuty と Malware Protection の両方を有効にすると、次のマルウェアスキャンの詳細を使用できます AWS アカウント。

- 脅威 — マルウェアスキャン中に検出された脅威のリスト。

  検出結果に含めることができる脅威の数については、「」を参照してくださいMalware Protection for S3 のクォータ。
- 項目パス – ネストされた項目パスのリストと、スキャンされた S3 オブジェクトのハッシュの詳細。
  - ネストされた項目パス — 脅威が検出されたスキャンされた S3 オブジェクトの項目パス。

    このフィールドの値は、最上位オブジェクトがアーカイブであり、アーカイブ内で脅威が検出された場合にのみ使用できます。
  - Hash – この検出結果で検出された脅威のハッシュ。
- ソース — 可能な値は `Bitdefender`および ですAmazon。

アクション

検出結果の [Action] (アクション) は、その検出をトリガーしたアクティビティのタイプに関する詳細を示します。利用可能な情報は、アクションタイプによって異なります。

[アクションタイプ] - 検出結果アクティビティのタイプ。この値は、NETWORK_CONNECTION、PORT_PROBE、DNS_REQUEST、AWS_API_CALL、RDS_LOGIN_ATT のいずれかになります。利用可能な情報は、アクションタイプによって異なります。

- NETWORK_CONNECTION - ネットワークトラフィックが識別済み EC2 インスタンスとリモートホスト間で交わされたことを示します。このアクションタイプには、次の追加情報が含まれています。
  - 接続方向 — 検出結果を生成する GuardDuty ように促したアクティビティで観測されたネットワーク接続方向。これには、次のいずれかの値を指定できます。
    - インバウンド - リモートホストがアカウントの識別済み EC2 インスタンスのローカルポートへの接続を開始したことを示します。
    - アウトバウンド - 識別済み EC2 インスタンスがリモートホストへの接続を開始したことを示します。
    - UNKNOWN – が接続の方向を特定 GuardDuty できなかったことを示します。
  - プロトコル — 検出結果を生成する GuardDuty 原因となったアクティビティで観察されたネットワーク接続プロトコル。
  - ローカル IP (ローカル IP) - 検出結果をトリガーしたトラフィックの元の送信元 IP アドレス。この情報を使用して、トラフィックが通過する中間レイヤーの IP アドレスと、検出結果をトリガーしたトラフィックの元の送信元 IP アドレスを区別します。例えば、EKS ポッドが実行されているインスタンスの IP アドレスではなく、EKS ポッドの IP アドレスです。
  - [ブロック] - ターゲットポートがブロックされているかどうかを示します。
- PORT_PROBE - リモートホストが複数のオープンポートで識別済みの EC2 インスタンスを調査したことを示します。このアクションタイプには、次の追加情報が含まれています。
  - ローカル IP - 検出結果をトリガーしたトラフィックの元の送信元 IP アドレス。この情報を使用して、トラフィックが通過する中間レイヤーの IP アドレスと、検出結果をトリガーしたトラフィックの元の送信元 IP アドレスを区別します。例えば、EKS ポッドが実行されているインスタンスの IP アドレスではなく、EKS ポッドの IP アドレスです。
  - [ブロック] - ターゲットポートがブロックされているかどうかを示します。
- DNS_REQUEST - 識別済みの EC2 インスタンスがドメイン名を照会したことを示します。このアクションタイプには、次の追加情報が含まれています。
  - プロトコル — 検出結果を生成する GuardDuty 原因となったアクティビティで観察されたネットワーク接続プロトコル。
  - [ブロック] - ターゲットポートがブロックされているかどうかを示します。
- AWS_API_CALL - AWS API が呼び出されたことを示します。このアクションタイプには、次の追加情報が含まれています。
  - API – 呼び出され、この検出結果を生成する GuardDuty ように求められた API オペレーションの名前。

> **Note**
>
> これらのオペレーションは、 AWS CloudTrailによってキャプチャされる API 以外のイベントを含めることもできます。詳細については、「 でキャプチャされた API 以外のイベント CloudTrail」を参照してください。

  - [ユーザーエージェント] – API リクエストを実行したユーザーエージェント。この値は、呼び出しが 、 AWS サービス AWS Management Console、 AWS SDKs、または のいずれから行われたかを示します AWS CLI。
  - エラーコード - API コールの失敗によって検出結果がトリガーされた場合、そのコールに対してエラーコードが表示されます。
  - サービス名 - 検出結果をトリガーした API コールを実行しようとしたサービスの DNS 名。
- RDS_LOGIN_ATTEMPT — 侵害された可能性のあるデータベースに、リモート IP アドレスからログインが試行されたことを示します。
  - [IP アドレス] — 疑わしいログイン試行に使用されたリモート IP アドレス。

アクターまたはターゲット

[リソースロール] が TARGET の場合には、検出結果に [アクター] セクションが表示されます。これは、リソースが疑わしいアクティビティの対象であったことを示します。また、[Actor] (アクター) セクションには、リソースを対象としたエンティティの詳細が含められます。

[リソースロール] が ACTOR の場合には、検出結果に [ターゲット] セクションが表示されます。これは、リソースがリモートホストに対する不審なアクティビティに関与していたことを示します。また、このセクションには、リソースのターゲットになった IP またはドメインに関する情報が含められます。

[アクター] セクションまたは [ターゲット] セクションには、次の情報を含めることができます。

- 孤立 – リモート API 発信者の AWS アカウントが GuardDuty 環境に関連しているかどうかに関する詳細。この値が `true` の場合、API コール実行者は何らかの形でアカウントに関連しています。`false` の場合、API コール実行者は環境外です。
- リモートアカウント ID – 最終ネットワークでリソースにアクセスするために使用されたアウトバウンド IP アドレスを所有するアカウント ID。
- IP アドレス – 検出結果を生成する GuardDuty よう促したアクティビティに関係する IP アドレス。

- Location – 検出結果の生成 GuardDuty を促したアクティビティに関係する IP アドレスの場所情報。
- 組織 – 検出結果を生成する GuardDuty よう促したアクティビティに関連する IP アドレスの ISP 組織情報。
- ポート — 検出結果の生成 GuardDuty を促したアクティビティに関係するポート番号。
- ドメイン – 検出結果を生成する GuardDuty よう促したアクティビティに関係するドメイン。
- サフィックス付きのドメイン — 結果を生成する GuardDuty 原因となった可能性のあるアクティビティに関係する 2 番目と最上位のドメイン。最上位ドメインと第 2 レベルのドメインのリストについては、「パブリックサフィックスリスト」を参照してください。

追加情報

すべての検出結果には [追加情報] セクションがあり、次のような情報が含まれます。

- 脅威リスト名 – 検出結果を生成する GuardDuty よう促したアクティビティに関係する IP アドレスまたはドメイン名を含む脅威リストの名前。
- サンプル - サンプル検出結果であるかどうかを示す true または false の値。
- アーカイブ - 検出結果がアーカイブ済みかどうかを示す true または false の値。
- [異常] - 履歴で確認されていないアクティビティの詳細 これらには、異常な (以前に確認されていない) ユーザー、場所、時間、バケット、ログイン動作、または ASN Org などが含まれます。
- 異常なプロトコル — 検出結果を生成する GuardDuty 原因となったアクティビティに関連するネットワーク接続プロトコル。
- エージェント詳細 - AWS アカウントの EKS クラスターに現在導入されているセキュリティエージェントに関する詳細。これは EKS Runtime Monitoring の検出結果タイプにのみ適用されます。
  - エージェントバージョン – GuardDuty セキュリティエージェントのバージョン。
  - エージェント ID – GuardDuty セキュリティエージェントの一意の識別子。

証拠

脅威インテリジェンスに基づく検出結果には [証拠] セクションがあり、次のような情報が含まれます。

- 脅威インテリジェンスの詳細 — 認識された `Threat name`が表示される脅威リストの名前。
- 脅威名 – 脅威に関連付けられているマルウェアファミリーまたはその他の識別子の名前。

- 脅威ファイル SHA256 – 検出結果を生成したファイルの SHA256。

異常な動作

で終わる検出結果タイプは、検出結果が異常検出機械学習 (ML) GuardDuty モデルによって生成されたAnomalousBehaviorことを示します。機械学習モデルは、アカウントへのすべての API リクエストを評価し、相手が使用するタクティクスに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。

API リクエストのどの要素がリクエストを呼び出した CloudTrail ユーザー ID に対して異常であるかに関する詳細は、検出結果の詳細で確認できます。ID は CloudTrail userIdentity Element によって定義され、指定できる値は `Root`、`IAMUser`、`AssumedRole`、`FederatedUser`、`AWSAccount`、または ですAWSService。

API アクティビティに関連付けられているすべての GuardDuty 検出結果の詳細に加えて、AnomalousBehavior検出結果には、次のセクションで概説する追加の詳細があります。これらの詳細はコンソールで表示でき、検出結果の JSON でも確認できます。

- 異常な API - 検出結果に関連付けられたプライマリ API リクエストに近いユーザーアイデンティティが原因の API リクエストのリスト。このペインでは、次の方法で API イベントの詳細をさらに分類します。
  - 最初にリストされている API はプライマリ API です。プライマリ API は、観測された最も高いリスクアクティビティに関連付けられた API リクエストです。これは、発見をトリガーし、検出結果タイプの攻撃ステージと相関する API です。これは、コンソールの [アクション] セクションおよび検出結果の JSON で詳述されている API でもあります。
  - リストされている他の API は、プライマリ API の近くで観察されるリストされたユーザーアインデンティティからの追加の異常 API です。リストに API が 1 つしかない場合、機械学習モデルはそのユーザーアイデンティティからの追加の API リクエストを異常として識別しませんでした。
  - API のリストは、API が正常に呼び出されたかどうかに基づいて分類され、API が正常に呼び出されなかった場合は、エラーレスポンスが受信されたことを意味します。受信したエラーレスポンスのタイプは、それぞれ正常に呼び出されなかった API の上に一覧表示されます。考えられるエラーレスポンスのタイプは、`access denied`、`access denied exception`、`auth failure`、`instance limit exceeded`、`invalid permission - duplicate`、`invalid permission - not found`、および `operation not permitted` です。

- API は、関連するサービスによって分類されます。

> **Note**
>
> その他のコンテキストについては、[Historical APIs] (過去の API) を選択し、上位 API の詳細を確認します。通常は、ユーザーアイデンティティとアカウント内のユーザーすべての両方で表示される最大 20 個の API です。API は、[めったにない(月に 1 回未満)]、[頻繁でない(月に数回)]、または [頻繁(毎日から毎週)] でマークされ、アカウント内で使用されている頻度によって異なります。

- [Unusual Behavior (Account)] (異常な動作 (アカウント)) - このセクションでは、アカウントでプロファイリングされた動作に関する詳細について説明します。このパネルで追跡される情報は次のとおりです。
  - [ASN Org] (ASN 組織) - 異常な API コールが行われた ASN 組織
  - [ユーザー名] - 異常な API コールを行ったユーザーの名前。
  - ユーザーエージェント - 異常な API コールを行うために使用されるユーザーエージェント。ユーザーエージェントは、`aws-cli` または `Botocore` などのコールを行うために使用されるメソッドです。
  - [ユーザータイプ] - 異常な API コールを行ったユーザーの名前。可能な値は、`AWS_SERVICE`、`ASSUMED_ROLE`、`IAM_USER` または `ROLE` です。
  - バケット — アクセスされている S3 バケットの名前。
- [Unusual Behavior (User Identity)] (異常な動作 (ユーザー ID)) - このセクションでは、検出に関与したユーザーアイデンティティのプロファイリングされた動作の詳細について説明します。動作が履歴として識別されない場合、 GuardDuty ML モデルでは、トレーニング期間内にこの方法でこの API コールを行ったユーザー ID が以前に確認されていないことを意味します。ユーザーアイデンティティ に関する詳細については、次を参照してください。
  - [ASN 組織] - 異常な API コールが行われた元の ASN 組織。
  - ユーザーエージェント - 異常な API コールを行うために使用されるユーザーエージェント。ユーザーエージェントは、`aws-cli` または `Botocore` などのコールを行うために使用されるメソッドです。
  - バケット — アクセスされている S3 バケットの名前。
- [Unusual Behavior (Bucket)] (異常な動作 (バケット)) - このセクションでは、検出結果に関連する、S3 バケットのプロファイリングされた動作に関する詳細について説明します。動作が履歴として識別されない場合、 GuardDuty ML モデルはトレーニング期間内にこの方法でこのバケット

に対して行われた API コールを以前に確認していないことを意味します。このセクションで追跡される情報は次のとおりです。

- [ASN 組織] - 異常な API コールが行われた元の ASN 組織。
- [ユーザー名] - 異常な API コールを行ったユーザーの名前。
- ユーザーエージェント - 異常な API コールを行うために使用されるユーザーエージェント。ユーザーエージェントは、`aws-cli` または `Botocore` などのコールを行うために使用されるメソッドです。
- [ユーザータイプ] - 異常な API コールを行ったユーザーの名前。可能な値は、`AWS_SERVICE`、`ASSUMED_ROLE`、`IAM_USER` または `ROLE` です。

> **Note**
>
> 過去の動作の詳細については、[異常な動作 (アカウント)]、[ユーザー ID]、または [バケット] セクションのいずれかで [過去の動作] を選択し、アカウント内での使用頻度に応じて、[頻度が低い (月に 1 回未満)]、[頻繁でない (月に数回)]、または [頻度が高い (毎日から毎週)] の各カテゴリーのアカウントで、想定される動作の詳細を表示します。

- 異常な動作 (データベース) - このセクションでは、検出結果に関連するデータベースインスタンスの、プロファイリングされた動作に関する詳細について説明します。動作が履歴として識別されない場合は、 GuardDuty ML モデルがトレーニング期間内にこの方法でこのデータベースインスタンスへのログイン試行を以前に確認していないことを意味します。検出結果パネルで追跡されるこのセクションの情報は次のとおりです。
  - [User name] (ユーザー名) - 異常なログイン試行に使用されたユーザー名
  - [ASN Org] (ASN 組織) - 異常なログイン試行が行われた ASN 組織
  - [Application name] (アプリケーション名) — 異常なログイン試行に使用されたアプリケーション名
  - [データベース名] — 異常なログイン試行に関与したデータベースインスタンス名

> **Note**
>
> [履歴動作] セクションでは、関連するデータベースの [ユーザー名]、[ASN 組織]、[アプリケーション名]、[データベース名] について、以前に確認した内容について詳しく説明しています。固有の値にはそれぞれ、ログインが成功した際にその値が確認された回数を示すカウントが関連付けられています。

- 異常動作 (アカウント Kubernetes クラスター、Kubernetes 名前空間、 Kubernetes ユーザー名) - このセクションでは、検出結果に関連する、Kubernetes クラスターと名前空間の、プロファイリングされた動作に関する詳細を説明します。動作が履歴として識別されない場合、 GuardDuty ML モデルがこのアカウント、クラスター、名前空間、またはユーザー名をこの方法で以前に確認していないことを意味します。検出結果パネルで追跡されるこのセクションの情報は次のとおりです。
  - ユーザー名 — 検出結果に関連付けられた Kubernetes API を呼び出したユーザー。
  - 偽装されたユーザー名 – `username` に偽装されているユーザー。
  - 名前空間 — アクションが発生した Amazon EKS クラスター内の Kubernetes 名前空間。
  - ユーザーエージェント — Kubernetes API コールに関連付けられたユーザーエージェント。ユーザーエージェントは、`kubectl` などのコールを行うために使用されるメソッドです。
  - API — Amazon EKS クラスター内で `username` によって呼び出される Kubernetes API。
  - ASN 情報 — この呼び出しを行うユーザーの IP アドレスに関連付けられた、組織や ISP などの ASN 情報。
  - 曜日 — Kubernetes API コールが行われた曜日。
  - アクセス権限 [1] — `username` が Kubernetes API を使用できるかどうかのアクセスの確認を受ける Kubernetes の動詞とリソース。
  - サービスアカウント名[1] – ワークロードに ID を提供する Kubernetes ワークロードに関連付けられたサービスアカウント。
  - レジストリ[1] — Kubernetes ワークロードにデプロイした、コンテナイメージに関連付けられたコンテナレジストリ。
  - イメージ[1] — Kubernetes ワークロードにデプロイされた、関連するタグやダイジェストを含まないコンテナイメージ。
  - Image Prefix Config[1] — イメージを使用するコンテナの、`hostNetwork` または `privileged` などのコンテナとワークロードセキュリティ設定が有効になっているイメージプレフィックス。
  - サブジェクト名[1] — `RoleBinding` や `ClusterRoleBinding` 内の参照ロールにバインドされている `user`、`group`、`serviceAccountName` などのサブジェクト。
  - ロール名[1] — ロールまたは `roleBinding` API の作成や変更に関係するロールの名前。

S3 ボリュームベースの異常

このセクションでは、S3 ボリュームベースの異常についてのコンテキスト情報について詳しく説明します。ボリュームベースの検出結果 (Exfiltration:S3/AnomalousBehavior) は、ユーザーの S3 バケットに対する異常な数の S3 API コールをモニタリングし、データ漏えいの可能性を示します。以下の S3 の API 呼び出しは、ボリュームベースの異常検出のために監視されます。

- GetObject
- CopyObject.Read
- SelectObjectContent

以下のメトリクスは、IAM エンティティが S3 バケットにアクセスするときの通常の動作のベースラインを構築するのに役立ちます。データの流出を検出するために、ボリュームベースの異常検出結果は通常の行動ベースラインに対してすべてのアクティビティを評価します。次のメトリクスを表示するには、[異常な動作]、[確認されたボリューム (ユーザーアイデンティティ)]、および [確認されたボリューム (バケット)] セクションで [過去の動作] を選択します。

- 過去 24 時間に、影響を受ける S3 バケットに関連付けられた IAM ユーザーまたは IAM ロール (どちらが発行されたかによって異なる) によって呼び出された s3-api-name API コールの数。
- 過去 24 時間に、すべての S3 バケットに関連付けられた IAM ユーザーまたは IAM ロール (どちらが発行されたかによって異なる) によって呼び出された s3-api-name API コールの数。
- 過去 24 時間に、影響を受ける S3 バケットに関連付けられた IAM ユーザーまたは IAM ロール (どちらが発行されたかによって異なる) によって呼び出された s3-api-name API コールの数。

RDS ログインアクティビティベースの異常

このセクションは、異常なアクターが行ったログイン試行回数の詳細について説明するものであり、ログイン試行の結果ごとにグループ分けされています。RDS Protection の検出結果タイプ はログインイベントをモニタリングして successfulLoginCount、failedLoginCount、incompleteConnectionCount などの異常なパターンがないかを確認し、異常な動作を特定します。

- successfulLoginCount – このカウンターは、異常なアクターによってデータベースインスタンスに対して行われた正常な接続 (ログイン属性の正しい組み合わせ) の合計を表します。ログイン属性には、ユーザー名、パスワード、データベース名が含まれます。
- failedLoginCount – このカウンターは、データベースインスタンスへの接続を確立するために失敗した (失敗した) ログイン試行の合計を表します。これは、ユーザー名、パスワード、データベース名など、ログイン情報の組み合わせの属性が 1 つ以上、正しくなかったことを示します。
- incompleteConnectionCount – このカウンターは、成功または失敗として分類できない接続試行の数を表します。これらの接続は、データベースが応答する前に閉じられています。例えば、データベースポートは接続されているものの情報がデータベースに送信されないポートスキャンや、ログインが成功または失敗して完了する前に接続が中止された場合などです。

GuardDuty の検出結果の形式

GuardDuty は AWS の環境内で不審な動作や予期しない動作を検出すると、検出結果を生成します。検出結果は、GuardDuty で検出した潜在的なセキュリティ問題に関する詳細を含む通知です。[finding details] (結果の詳細) には、何が起こったのか、不審なアクティビティに関与している AWS リソース、このアクティビティの発生日時やその他の情報が含まれます。

検出結果の詳細で最も役立つ情報の 1 つは、[finding type] (結果タイプ) です。検出結果タイプの目的は、潜在的なセキュリティ問題について簡潔でわかりやすい説明を提供することです。例えば、GuardDuty の Recon:EC2/PortProbeUnprotectedPort 検出結果タイプは、AWS 環境の EC2 インスタンスに保護されていないポートがあり、これを攻撃者が見つけようとしていることを迅速に知らせます。

GuardDuty では、次のフォーマットを使って、生成するさまざまな検出結果タイプに名前を付けます。

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

このフォーマットの各部分は、検出結果タイプの特徴を表します。これらの特徴には、次のような説明があります。

- ThreatPurpose - 攻撃型または潜在的な攻撃型の脅威の主な目的についての説明です。GuardDuty 脅威の目的の一覧表については、次のセクションを参照してください。
- ResourceTypeAffected - この検出結果でどの AWS リソースが攻撃対象の候補として特定されたかを示します。現在、GuardDuty は EC2、S3、IAM、および EKS のリソースに関する検出結果を生成できます。
- ThreatFamilyName - GuardDuty で検出された全体的な脅威または潜在的な悪意のあるアクティビティの説明です。例えば、NetworkPortUnusual の値は、GuardDuty の検出結果で識別された EC2 インスタンスに、識別された特定のリモートポートでの通信履歴がないことを示します。
- DetectionMechanism - どの GuardDuty が検出結果を検出した方法を説明します。これは、一般的な検出結果タイプの変動や、GuardDuty が特定のメカニズムを使用して検出した検出結果を示すために使用できます。例えば、Backdoor:EC2/DenialOfService.Tcp は、TCP 上でサービス拒否 (DoS) が検出されたことを示します。UDP バリアントは Backdoor:EC2/DenialOfService.Udp です。

  .Custom の値は、GuardDuty がカスタム脅威リストに基づいて検出結果を検出したことを示し、.Reputation は、GuardDuty がドメインレピュテーションスコアモデルを使用して検出結果を検出したことを示します。

- Artifact - 悪意のあるアクティビティで使用されたツールが所有する特定のリソースを示します。例えば、検出結果タイプ CryptoCurrency:EC2/BitcoinTool.B!DNS の DNS は、EC2 インスタンスがビットコインに関連する既知のドメインと通信していることを示します。

脅威の目的

GuardDuty において、[threat purpose] (脅威の目的) は、攻撃型または潜在的な攻撃の段階など脅威の主な目的について説明します。例えば、バックドアなどの脅威の目的は、攻撃型であると示します。ただし、MITRE ATT&CK 戦術と一致する [Impact] (影響) などの脅威の目的があります。MITRE ATT&CK 戦術は、攻撃者の攻撃サイクルにおける異なるフェーズを示します。現行の GuardDutyリリースの発売で、ThreatPurpose は次の値に設定できます。

Backdoor

この値は、攻撃者が AWS リソースに侵入し、そのリソースを変更したので、ホームのコマンドアンドコントロール (C&C) サーバーに連絡でき、悪意のあるアクティビティを仕掛ける命令を受け取ることを示します。

Behavior

この値は、GuardDutyは特定の AWS リソースの確立されたベースラインとは異なるアクティビティやアクティビティパターンを検出したことを示します。

CredentialAccess

この値は、GuardDuty がユーザーの環境からアカウント ID やパスワードなどの認証情報を盗むために攻撃者が使用する可能性のあるアクティビティパターンを検出したことを示します。この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

Cryptocurrency

この値は、GuardDuty がユーザーの環境の AWS リソースが、(ビットコインなどの) 暗号通貨に関連付けられたソフトウェアをホストしています。

DefenseEvasion

この値は、ユーザーの環境に侵入している間、GuardDuty は攻撃者が検出を回避するために使用する可能性のあるアクティビティまたはアクティビティパターンを検出したことを示します。この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

Discovery

この値は、GuardDuty がシステムおよび内部ネットワークに関する知識を拡張するために使用する可能性のあるアクティビティまたはアクティビティパターンを検出したことを示します。この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

実行

この値は、GuardDuty が、攻撃者が悪意のあるコードを実行してネットワークを探索したり、データを盗んだりする可能性があることを検出したことを示します。この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

Exfiltration

この値は、GuardDuty がネットワークからデータを盗もうとするときに攻撃者が使用する可能性のあるアクティビティまたはアクティビティパターンを検出したことを示します。この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

Impact

この値は、GuardDuty がアクティビティまたはアクティビティパターンを検出することにより、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ることを示しています。この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

InitialAccess

この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

Pentest

AWS リソースの所有者や承認された担当者は、オープンなセキュリティグループや安全性の低いアクセスキーなどの脆弱性を見つけるために、AWS アプリケーションに対して意図的にテストを実行する場合があります。これらの侵入テストは、攻撃者が気づく前に脆弱なリソースを特定してロックダウンする目的で実行されます。ただし、承認済みペンテスターが使用する一部のツールは一般的なものであるため、不正なユーザーや攻撃者がこのテストに便乗して利用する場合があります。GuardDuty は、このようなアクティビティの真の意図は特定できませんが、[Pentest] (侵入テスト) 値により、GuardDuty がこのようなアクティビティを検出し、および既知の侵入テストツールで生成したアクティビティと類似しユーザーのネットワークへの悪意のある調査を示します。

Persistence

この値は、GuardDuty が初期アクセスルートが切断された場合でも、攻撃者がシステムへのアクセスを維持するために使用する可能性のあるアクティビティまたはアクティビティパターンを検出したことを示します。例えば、既存のユーザーの侵入して得た認証情報を介してアクセスした

後に、新しい IAM ユーザーを作成することが含まれます。既存のユーザーの認証情報が削除されると、攻撃者はオリジナルイベントの一部として検出されなかった新しいユーザーへのアクセスを保持します。この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

Policy

この値は、AWS アカウント がセキュリティに関して推奨されたベストプラクティスに反する動作を行っていることを示します。

PrivilegeEscalation

この値は、ユーザーの AWS 環境下の関連プリンシパルが、攻撃者にネットワークへのより高いレベルの許可を取得するために使用する可能性のあることを通知します。この脅威の目的は、MITRE ATT&CK 戦術に基づいています。

Recon

この値は、GuardDuty がネットワークの偵察を実行するときに、攻撃者がアクセスを拡大したり、リソースを利用したりする方法を決定するために使用する可能性のあるアクティビティまたはアクティビティパターンを検出したことを示します。例えば、このアクティビティは、AWS ポートを調べたり、ユーザーやデータベーステーブルなどをリスト化により、環境の脆弱性のスコープアウトを含めることができます。

Stealth

この値は、攻撃者が積極的にアクションを隠そうとしていることを示します。例えば、匿名化したプロキシサーバーを使用し、アクティビティの本質の判断を非常に難しくしています。

Trojan

この値は、悪意のあるアクティビティを密かに実行するトロイの木馬プログラムが攻撃に使用されていることを示します。このソフトウェアは合法的なプログラムを装う場合があります。ユーザーは、このソフトウェアを誤って実行することがあります。脆弱性を特定して自動的に実行されることもあります。

UnauthorizedAccess

この値は、承認されていない個人による不審なアクティビティまたは不審なアクティビティパターンが GuardDuty で検出されたことを示します。

でのサンプルの検出結果の生成 GuardDuty

Amazon を使用してサンプル検出結果を生成 GuardDuty し、 が生成 GuardDuty できるさまざまな検出結果タイプを視覚化して理解するのに役立ちます。サンプル検出結果を生成すると、 GuardDuty

は、サポートされている検出結果タイプごとに 1 つのサンプル検出結果を現在の検出結果リストに入力します。

生成されるサンプルは、プレースホルダーの値が入力された近似値です。これらのサンプルは、環境の実際の検出結果とは異なるように見えますが、イベント EventBridge やフィルターなど GuardDuty、 のさまざまな設定をテストするために使用できます。検出結果タイプで使用できる値のリストについては、「 検出結果タイプ表」を参照してください。

GuardDuty コンソールまたは API を使用したサンプル検出結果の生成

任意のアクセス方法を選択して、サンプルの検出結果を生成します。

> **Note**
>
> コンソールメソッドは、各検出結果タイプのうちの 1 つを生成します。1 つのサンプル検出結果を生成できるのは、API 経由のみです。

Console

サンプル検出結果を生成するには、次の手順を使用します。このプロセスでは、検出結果タイプごとに 1 つのサンプル GuardDuty 検出結果が生成されます。

1. https://console.aws.amazon.com/guardduty/ で GuardDuty 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. [Settings] (設定) ページの [Sample findings] (結果のサンプル) で、[Generate sample findings] (結果サンプルの生成) を選択します。
4. ナビゲーションペインで [Findings] (結果) を選択します。[Current findings] (最近の結果) ページに [SAMPLE] とプレフィックスされたサンプル検出結果が表示されます。

API/CLI

CreateSampleFindings API を使用して、任意の検出結果タイプに一致する単一のサンプル GuardDuty 検出結果を生成できます。検出結果タイプに使用可能な値は検出結果タイプ表に一覧表示されます。

これは、検出結果に基づく CloudWatch イベントルールまたはオートメーションのテストに役立ちます。次の例は、 AWS CLIを使用して Backdoor:EC2/DenialOfService.Tcp タイプの単一サンプル検出結果を生成する方法を示しています。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

これらのメソッドによって生成されたサンプル検出結果のタイトルは、常にコンソール内で [SAMPLE] で始まります。サンプルの検出結果には、検出結果の JSON の詳細の additionalInfo セクションに値 "sample": true があります。

環境 AWS アカウント 内で分離された専用の でシミュレートされたアクティビティに基づいて一般的な検出結果を生成するには、「」を参照してください専用アカウントで GuardDuty の検出結果のテスト。

専用アカウントで GuardDuty の検出結果のテスト

このドキュメントを使用して、この目的のために特別に使用する AWS アカウント で GuardDuty 検出結果を生成するテスタースクリプトを実行します。これらのステップは、特定の GuardDuty 検出結果タイプを理解して学習したい場合に実行できます。このエクスペリエンスは、 の生成とは異なりますサンプルの検出結果。検出結果のテストエクスペリエンスの詳細については、 GuardDuty「」を参照してください考慮事項。

内容

考慮事項

先に進む前に、次の点を考慮してください。

- GuardDuty では、テスタースクリプトを専用の非本番環境 AWS アカウント または分離された環境にデプロイすることをお勧めします。テスタースクリプトを実行すると、 GuardDuty はこのアカウントに特定の AWS リソースをデプロイします。これは、これらのシミュレートされた検出結果を特定するのにも役立ちます。
- テスタースクリプトは、さまざまな AWS リソースの組み合わせで 100 を超える GuardDuty 検出結果を生成します。現在、これにはすべての が含まれているわけではありません検出結果タイプ。このテスタースクリプトで生成できる検出結果タイプのリストについては、「」を参照してくださいGuardDuty テスタースクリプトが生成できる検出結果。
- テスタースクリプトは、専用アカウント GuardDuty の設定ステータスを検証します。このアカウント GuardDuty が有効になっていない場合、スクリプトは の実行時に有効にするよう要求しますステップ 3 - テスタースクリプトを実行する。テスタースクリプトは、検出結果の生成に必要な特定の保護プランを有効にするアクセス許可をリクエストします。

  を初めて有効に GuardDuty する

  が特定のリージョンで初めて専用アカウントで有効 GuardDuty になると、アカウントは自動的に 30 日間の無料トライアルに登録されます。

  GuardDuty には、オプションの保護プランが用意されています。を有効にすると GuardDuty、特定の保護プランも有効になり、 GuardDuty 30 日間の無料トライアルに含まれます。詳細については、「 GuardDuty 30 日間の無料トライアルの使用」を参照してください。

  GuardDuty テスタースクリプトを実行する前に、 アカウントで が既に有効になっている

  GuardDuty が既に有効になっている場合、テスタースクリプトはパラメータに基づいて、検出結果の生成に必要な特定の保護プランやその他のアカウントレベルの設定の設定ステータスをチェックします。

  このテスタースクリプトを実行すると、リージョンの専用アカウントで特定の保護プランが初めて有効になる場合があります。これにより、その保護プランの 30 日間の無料トライアルが開始されます。各保護プランに関連する無料トライアルについては、「」を参照してくださいGuardDuty 30 日間の無料トライアルの使用。
- テスタースクリプトが終了すると、専用アカウントは元の保護プランの設定と設定に復元されます。

GuardDuty テスタースクリプトが生成できる検出結果

現在、テスタースクリプトは、Amazon EC2、Amazon EKS、Amazon S3、IAM、および EKS 監査ログに関連する次の検出結果タイプを生成します。

- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Udp
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- PenTest:IAMUser/KaliLinux
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

- UnauthorizedAccess:IAMUser/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- PenTest:S3/KaliLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation

- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

ステップ 1 - 前提条件

テスト環境を準備するには、次の項目が必要です。

- Git – 使用するオペレーティングシステムに基づいて git コマンドラインツールをインストールします。これは、`amazon-guardduty-tester`リポジトリ のクローンを作成するために必要です。
- AWS Command Line Interface – コマンドラインシェルのコマンド AWS のサービス を使用して とやり取りできるオープンソースツール。詳細については、「 ユーザーガイド」の AWS CLI「 の開始方法AWS Command Line Interface 」を参照してください。
- AWS Systems Manager – を使用してマネージドノードで Session Manager セッションを開始するには、ローカルマシンに Session Manager プラグインをインストール AWS CLI する必要があります。詳細については、「 ユーザーガイド」の「 用の Session Manager プラグイン AWS CLIのインストールAWS Systems Manager 」を参照してください。
- Node Package Manager (NPM) — NPM をインストールして、すべての依存関係をインストールします。
- Docker – Docker がインストールされている必要があります。インストール手順については、Docker のウェブサイトを参照してください。

  Docker がインストールされていることを確認するには、次のコマンドを実行し、次のような出力があることを確認します。

  ```
  $ docker --version
  Docker version 19.03.1
  ```

- で Kali Linux イメージをサブスクライブしますAWS Marketplace。

ステップ 2 - AWS リソースをデプロイする

このセクションでは、主要な概念と、特定の AWS リソースを専用アカウントにデプロイする手順のリストを示します。

概念

次のリストは、リソースのデプロイに役立つコマンドに関連する主要な概念を示しています。

- AWS Cloud Development Kit (AWS CDK) – CDK は、コードでクラウドインフラストラクチャを定義し、 を通じてプロビジョニングするためのオープンソースのソフトウェア開発フレームワークです AWS CloudFormation。CDK は、コンストラクトと呼ばれる再利用可能なクラウドコンポーネントを定義するために、いくつかのプログラミング言語をサポートしています。これらをスタックとアプリケーションにまとめて構成できます。その後、CDK アプリケーションを にデプロイ AWS CloudFormation して、 リソースをプロビジョニングまたは更新できます。詳細については、「 AWS Cloud Development Kit (AWS CDK) デベロッパーガイド」の「 とは AWS CDK」を参照してください。
- ブートストラップ — AWS 環境で を使用するための準備プロセスです AWS CDK。CDK スタックを AWS 環境にデプロイする前に、まず環境をブートストラップする必要があります。によって使用される環境内の特定の AWS リソースをプロビジョニングするこのプロセスは、次のセクション - で実行する手順の一部 AWS CDK ですAWS リソースをデプロイするステップ。

  ブートストラップの仕組みの詳細については、「 AWS Cloud Development Kit (AWS CDK) デベロッパーガイド」の「ブートストラップ」を参照してください。

AWS リソースをデプロイするステップ

リソースのデプロイを開始するには、次の手順を実行します。

1. 専用アカウントリージョン変数が `bin/cdk-gd-tester.ts` ファイルで手動で設定されていない限り、 AWS CLI デフォルトのアカウントとリージョンを設定します。詳細については、「 AWS Cloud Development Kit (AWS CDK) デベロッパーガイド」の「環境」を参照してください。
2. リソースをデプロイするには、次のコマンドを実行します。

```
git clone https://github.com/awslabs/amazon-guardduty-tester && cd amazon-guardduty-
tester
npm install
cdk bootstrap
```

```
cdk deploy
```

最後のコマンド (cdk deploy) は、ユーザーに代わって AWS CloudFormation スタックを作成します。このスタックの名前は ですGuardDutyTesterStack。

このスクリプトの一部として、 は新しいリソース GuardDuty を作成して、アカウントで結果を生成します GuardDuty。また、Amazon EC2 インスタンスに次のタグキーと値のペアも追加されます。

```
CreatedBy:GuardDuty Test Script
```

Amazon EC2 インスタンスには、EKS ノードと ECS クラスターをホストする EC2 インスタンスも含まれます。

> **インスタンスのタイプ**
>
> GuardDuty はt3.micro、Amazon EKS ノードグループに対する例外を除き、すべてのリソースに対して を作成します。EKS には少なくとも 2 つのコアが必要なため、EKS ノードにはt3.mediumインスタンスタイプがあります。インスタンスタイプの詳細については、「Amazon EC2 インスタンスタイプガイド」の「使用可能なサイズ」を参照してください。 Amazon EC2

ステップ 3 - テスタースクリプトを実行する

これは、最初にテストドライバーでセッションを開始し、次にスクリプトを実行して特定のリソースの組み合わせで GuardDuty 結果を生成する必要がある 2 ステップのプロセスです。

パート A - テストドライバーでセッションを開始する

1. リソースがデプロイされたら、リージョンコードを現在のターミナルセッションの変数に保存します。次のコマンドを使用して、*us-east-1* をリソースをデプロイしたリージョンコードに置き換えます。

   ```
   $ REGION=us-east-1
   ```

2. テスタースクリプトは AWS Systems Manager (SSM) を介してのみ使用できます。テスターホストインスタンスでインタラクティブシェルを起動するには、ホスト をクエリしますInstanceId。

3. 次のコマンドを使用して、テスタースクリプトのセッションを開始します。

```
aws ssm start-session
  --region $REGION
  --document-name AWS-StartInteractiveCommand
  --parameters command="cd /home/ssm-user/py_tester && bash -l"
  --target $(aws ec2 describe-instances
    --region $REGION
    --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
    --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
    --output text)
```

パート B - 結果の生成

テスタースクリプトは、入力に基づいて検出結果を生成する bash スクリプトを動的に構築する Python ベースのプログラムです。1 つ以上の AWS リソースタイプ、保護プラン、 GuardDuty 脅威の目的 (戦術) 、、基礎データソースまたは に基づいて結果を柔軟に生成できますthe section called “GuardDuty テスタースクリプトが生成できる検出結果”。

次のコマンド例を参照として使用し、1 つ以上のコマンドを実行して、探索する検出結果を生成します。

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

有効なパラメータの詳細については、次のヘルプコマンドを実行します。

```
python3 guardduty_tester.py --help
```

パート C - 生成された結果を確認する

任意の方法を選択して、アカウントで生成された結果を表示します。

GuardDuty console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで 調査結果を選択します。
3. 結果テーブルから、詳細を表示する結果を選択します。これにより、結果の詳細パネルが開きます。詳細については、「Amazon GuardDuty の検出結果について」を参照してください。
4. これらの結果をフィルタリングする場合は、リソースタグのキーと値を使用します。例えば、Amazon EC2 インスタンスに対して生成された結果をフィルタリングするには、インスタンスタグキー とインスタンスタグキー に `CreatedBy` : `GuardDuty Test Script` タグキー: 値ペアを使用します。

API

- ListFindings を実行して、特定のディテクター ID の検出結果を表示します。検出結果をフィルタリングするパラメータを指定できます。

  アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

AWS CLI

- 次の AWS CLI コマンドを実行して生成された結果を表示し、*us-east-1* および *12abc34d567e8fa901bc2d34EXAMPLE* を適切な値に置き換えます。

  ```
  aws guardduty list-findings --region us-east-1 --detector-
  id 12abc34d567e8fa901bc2d34EXAMPLE
  ```

  アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

  結果のフィルタリングに使用できるパラメータの詳細については、 AWS CLI コマンドリファレンスの「list-findings」を参照してください。

ステップ 4 - AWS テストリソースをクリーンアップする

中に行われたアカウントレベルの設定やその他の設定ステータスの更新は、テスタースクリプトの終了時に元の状態ステップ 3 - テスタースクリプトを実行するに戻ります。

テスタースクリプトを実行したら、 AWS テストリソースをクリーンアップすることを選択できます。これを行うには、次のいずれかの方法を使用します。

- 次のコマンドを実行します。

```
cdk destroy
```

- という名前の AWS CloudFormation スタックを削除しますGuardDutyTesterStack。ステップの詳細については、「コンソールでのスタックの削除 AWS CloudFormation」を参照してください。

よくある問題に対するトラブルシューティング

GuardDuty は一般的な問題を特定し、トラブルシューティング手順を推奨しています。

- `Cloud assembly schema version mismatch` – AWS CDK CLI を、必要なクラウドアセンブリバージョンと互換性のあるバージョン、または利用可能な最新バージョンに更新します。詳細については、「 AWS CDK CLI の互換性」を参照してください。
- `Docker permission denied` – 専用アカウントがコマンドを実行できるように、専用アカウントユーザーを docker-users に追加します。ステップの詳細については、「Docker アクセス拒否」を参照してください。
- `Your requested instance type is not supported in your requested Availability Zone` – 一部のアベイラビリティーゾーンは、特定のインスタンスタイプをサポートしていません。優先インスタンスタイプをサポートするアベイラビリティーゾーンを特定し、 AWS リソースのデプロイを再試行するには、次の手順を実行します。

  1. 任意の方法を選択して、インスタンスタイプをサポートするアベイラビリティーゾーンを決定します。

     Console

     優先インスタンスタイプをサポートするアベイラビリティーゾーンを特定するには

     1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。

2. ページの右上隅にある AWS リージョンセレクターを使用して、インスタンスを起動するリージョンを選択します。
3. ナビゲーションペインのインスタンス で、インスタンスタイプ を選択します。
4. インスタンスタイプ テーブルから、優先インスタンスタイプを選択します。
5. ネットワーク で、アベイラビリティーゾーン にリストされているリージョンを表示します。

   この情報に基づいて、リソースをデプロイできる新しいリージョンを選択する必要がある場合があります。

AWS CLI

次のコマンドを実行して、アベイラビリティーゾーンのリストを表示します。希望するインスタンスタイプとリージョン (*us-east-1*) を必ず指定してください。

```
aws ec2 describe-instance-type-offerings --location-type availability-zone  --
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --
output table
```

このコマンドの詳細については、「 コマンドリファレンスdescribe-instance-type-offerings」の「」を参照してください。 AWS CLI

このコマンドを実行するときにエラーが発生した場合は、最新バージョンの を使用していることを確認してください AWS CLI。詳細については、「AWS Command Line Interface ユーザーガイド」の「トラブルシューティング」を参照してください。

2. AWS リソースを再度デプロイし、希望するインスタンスタイプをサポートするアベイラビリティーゾーンを指定します。

   AWS リソースのデプロイを再試行するには

   1. bin/cdk-gd-tester.ts ファイルでデフォルトのリージョンを設定します。
   2. アベイラビリティーゾーンを指定するには、 amazon-guardduty-tester/lib/common/network/vpc.ts ファイルを開きます。
   3. このファイルで、 をインスタンスタイプのアベイラビリティーゾーンを指定する必要がある availabilityZones: ['*us-east-1a*', '*us-east-1c*'], maxAzs: 2,に置き換えます。
   4. の残りのステップに進みますAWS リソースをデプロイするステップ。

GuardDuty 検出結果の重要度レベル

各 GuardDuty 検出結果には、セキュリティエンジニアが判断したネットワークに対する潜在的なリスクを反映した重要度レベルと値が割り当てられます。重要度の値の範囲は 1.0 ~ 8.9 です。値が大きいほど、セキュリティリスクが高いことを示します。検出結果で強調表示されている潜在的なセキュリティ問題への対応を判断するために、 はこの範囲を、高、中、低の重要度レベルに分類 GuardDuty します。

> **Note**
>
> 0 の値と 9.0 ~ 10.0 の範囲の値は将来使用するために現在予約されています。

現在定義されている検出結果の GuardDuty重要度レベルと値、およびそれぞれの一般的な推奨事項を次に示します。

重要度レベル	値の範囲
[High] (高)	7.0 ~ 8.9
高の重要度は、問題になっているリソース (EC2 インスタンスや IAM ユーザーサインイン認証情報) が侵害され、不正な目的で活発に使用されていることを示します。 重要度が [High] (高) の検出結果のセキュリティの問題は、優先事項として処理し、リソースのそれ以上の不正使用を防ぐために直ちに修復を行うことをお勧めします。例えば、EC2 インスタンスをクリーンアップまたは終了するか、IAM 認証情報を更新します。詳細については、「Remediation Steps」(修復のステップ) を参照してください。	
[Medium] (中)	4.0 ~ 6.9
[Medium] (中) の重要度は、通常観察される動作から逸脱する不審なアクティビティを示し、場合によってはリソースが侵害されていることを示します。 できるだけ早く、関連するリソースを調査することをお勧めします。修復のステップはリソースと検出結果のタイプによって異なりますが、通常、アクティビティが許可されており、ユースケースに沿っていることを確認する必要があります。原因を特定できない場合やアクティビティが許可されたことを確認できない場合は、リソースが侵害されたとみなし、「Remediation Steps」(修復のステップ) に従ってリソースを保護する必要があります。	

重要度レベル	値の範囲
次に、重要度が [Medium] (中) の検出結果を確認する場合に考慮する事項を示します。 • 未承認のユーザーがインストールした新しいソフトウェアでリソースの動作が変更されていないか確認してください。例えば、通常より高いトラフィックが許可されている場合や、新しいポートの通信が有効化されている場合などがあります。 • 許可されているユーザーがコントロールパネルの設定を変更しているかどうかを確認します (セキュリティグループの設定の変更など)。 • 該当するリソースでアンチウィルススキャンを実行し、未承認のソフトウェアを検出します。 • 該当する IAM ロール、ユーザー、グループ、または認証情報セットにアタッチされている許可を検証します。次のアクセス許可を変更または更新する必要がある場合があります。	
[Low] (低)	1.0 ~ 3.9
「低」の重要度は、ネットワークが侵害されなかった不審なアクティビティが試行されたことを示します (ポートスキャンや侵入の失敗など)。 すぐに推奨されるアクションはありませんが、この情報は、誰かがネットワークの弱点を探していることを示している可能性があるので、念のためメモしてください。	

GuardDuty 結果の集約

すべての検出結果は動的です。つまり、 が同じセキュリティ問題に関連する新しいアクティビティ GuardDuty を検出すると、新しい検出結果を生成する代わりに、元の検出結果を新しい情報で更新します。この動作により、同様のレポートを複数確認しなくても現在の問題を識別することが可能となり、認識済みのセキュリティの問題が重複してノイズになることを減らせます。

例えば、`UnauthorizedAccess:EC2/SSHBruteForce` の検出結果の場合、インスタンスへの複数のアクセスの試行が同じ検出結果 ID に集約され、検出結果の詳細のカウント数が増加します。これは、その検出結果が、インスタンスの SSH ポートがそのタイプのアクティビティに対して適切に保護されていないことを示す単一のセキュリティの問題を示しているためです。ただし、 が環境内の新しいインスタンスをターゲットとする SSH アクセスアクティビティ GuardDuty を検出すると、一意の検出結果 ID を持つ新しい検出結果が作成され、新しいリソースに関連するセキュリティ上の問題があることを警告します。

検出結果が集計されると、そのアクティビティの最新のオカレンスの情報で更新されます。つまり、上記の例ではインスタンスが新しいアクターからのブルートフォースの試みのターゲットになった場

合、検出結果の詳細は最も新しいソースのリモート IP を反映して更新され、古い情報は置き換えられることになります。個々のアクティビティの試行に関する詳細情報は、 または VPC フローログで CloudTrail引き続き利用できます。

既存の検出結果を集約するのではなく、新しい検出結果を生成する GuardDuty ようにアラートする基準は、検出結果のタイプによって異なります。各検出結果タイプの集約の条件は、ご利用のアカウントの個別のセキュリティの問題を明確にするために、当社のセキュリティエンジニアによって決定されます。

結果の検索と分析 GuardDuty

以下の手順に従って、 GuardDuty 結果を表示および分析します。

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. [Findings] (結果) を選択し、特定の検出結果を選択して詳細を表示します。

   各検出結果の詳細は、検出結果タイプ、関連リソース、アクティビティの性質によって異なります。使用可能な検出結果フィールドの詳細については、「検出結果の詳細」を参照してください。
3. (オプション) 検出結果をアーカイブする場合は、検出結果のリストから検出結果を選択し、[Actions] (アクション) メニューを選択します。その後、[Archive] (アーカイブ) を選択します。

   アーカイブされた検出結果は、[Current] (最新) のドロップダウンから [Archived] (アーカイブ済み) を選択すると表示されます。

   現在、 GuardDuty メンバーアカウントの GuardDuty ユーザーは結果をアーカイブできません。

   > **Important**
   >
   > 上記の手順を使用して検出結果を手動でアーカイブする場合は、この検索後に発生した検出結果 (アーカイブ完了後に生成された検出結果) はすべて、現在の検出結果のリストに追加されます。現在のリストにこの検出結果を表示しない場合は、自動アーカイブすることができます。詳細については、「抑制ルール」を参照してください。
4. (オプション) 検出結果をダウンロードするには、検出結果のリストから検出結果を選択し、[Actions] (アクション) メニューを選択します。その後、[Export] (エクスポート) を選択します。検出結果を [Export] (エクスポート) すると、完全な JSON ドキュメントが表示されます。

> **Note**
>
> 場合によっては、 は、特定の検出結果が生成された後に誤検出である GuardDuty ことを認識します。 は、検出結果の JSON に信頼度フィールド GuardDuty を提供し、その値をゼロに設定します。これにより GuardDuty 、このような検出結果を安全に無視できることがわかります。

検出結果タイプ

新しく追加または廃止された GuardDuty 検出結果タイプなど、検出結果タイプに対する重要な変更については、「」を参照してくださいAmazon のドキュメント履歴 GuardDuty。

現在廃止された検出結果タイプの詳細については、「廃止された検出結果タイプ」を参照してください。

GuardDuty EC2 の検出結果タイプ

次の検出結果は Amazon EC2 リソースに固有であり、常に `Instance` のリソースタイプを有しています。検出結果の重要度と詳細は、EC2 インスタンスが不審なアクティビティの対象であるか、不審なアクティビティを実行するアクターであるかを示すリソースロールによって異なります。

ここにリストされている検出結果には、検出結果タイプの生成に使用されるデータソースとモデルが含まれます。データソースとモデルの詳細については、「基礎データソース」を参照してください。

> **Note**
>
> インスタンスが既に終了している場合、または基盤となる API コールが、異なるリージョンに EC2 インスタンスを生じるクロスリージョン API コールの一部である場合、インスタンスの詳細がEC2 インスタンスの検出結果から欠落することがあります。

すべての EC2 の検出結果について、問題のリソースを調べて正常に動作しているかどうかを確認することをお勧めします。アクティビティが認可されると、そのリソースに対する誤検出の通知を防ぐため、抑制ルールや信頼できる IP リストを使用できます。予期しないアクティビティについては、セキュリティのベストプラクティスとしてインスタンスが侵害されていると仮定し、侵害された可能性のある Amazon EC2 インスタンスの修復 で説明されている対策をとることをお勧めします。

トピック

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts

- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce

- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

EC2 インスタンスは、既知の C&C サーバーに関連付けられる IP をクエリしています。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化したインスタンスが既知の C&C サーバーに関連付けられた IP をクエリしていることを知らせるものです。リスト化したインスタンスは侵害されている可能性があります。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータです。

ボットネットとは、一般的なタイプのマルウェアに感染し制御されたインターネットコネクテッドデバイス (PC、サーバー、モバイルデバイス、IoT デバイスなど) のコレクションです。通常、ボットネットは、マルウェアの配布や盗用された情報 (クレジットカード番号など) の収集に使用されます。ボットネットの目的と構造によっては、C&C サーバーから分散型サービス拒否 (DDoS) 攻撃を開始するためのコマンドが発行されることもあります。

> **Note**
>
> クエリされた IP が log4j 関連の場合、関連付けられた検出結果のフィールドには次の値が含まれます。
>
> - service.additionalInfothreatListName .= Amazon
> - service.additionalInfo.threatName = Log4j Related

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Backdoor:EC2/C&CActivity.B!DNS

EC2 インスタンスが、既知の C&C サーバーに関連付けられるドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境のリスト化したインスタンスが既知の C&C サーバーに関連付けられているドメインをクエリしていることを知らせるものです。リスト化したインスタンスは侵害されている可能性があります。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータです。

ボットネットとは、一般的なタイプのマルウェアに感染し制御されたインターネットコネクテッドデバイス (PC、サーバー、モバイルデバイス、IoT デバイスなど) のコレクションです。通常、ボットネットは、マルウェアの配布や盗用された情報 (クレジットカード番号など) の収集に使用されます。ボットネットの目的と構造によっては、C&C サーバーから分散型サービス拒否 (DDoS) 攻撃を開始するためのコマンドが発行されることもあります。

> **Note**
>
> クエリされたドメイン名が log4j 関連の場合、関連付けられた検出結果のフィールドには次の値が含まれます。
>
> - service.additionalInfothreatListName .= Amazon
> - service.additionalInfo.threatName = Log4j Related

> **Note**
>
> がこの検出結果タイプ GuardDuty を生成する方法をテストするには、テストドメインに対してインスタンスから DNS リクエストを行います (digLinux の場合は 、Windows nslookup の場合は を使用) guarddutyc2activityb.com。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Backdoor:EC2/DenialOfService.Dns

EC2 インスタンスが、DNS プロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、大量のアウトバウンド DNS トラフィックを生成しているリスト化した EC2 インスタンスが AWS 環境にあることを知らせるものです。これは、リストされたインスタンスが侵害され、DNS プロトコルを使用した denial-of-service (DoS) 攻撃の実行に利用されていることを示している可能性があります。 DoS

> **Note**
>
> この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Backdoor:EC2/DenialOfService.Tcp

EC2 インスタンスが TCP プロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、大量のアウトバウンド TCP トラフィックを生成しているリスト化した EC2 インスタンスが AWS 環境にあることを知らせるものです。これは、インスタンスが侵害され、TCP プロトコルを使用した denial-of-service (DoS) 攻撃の実行に利用されていることを示している可能性があります。

> **Note**
>
> この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Backdoor:EC2/DenialOfService.Udp

EC2 インスタンスが UDP プロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、大量のアウトバウンド UDP トラフィックを生成しているリスト化した EC2 インスタンスが AWS 環境にあることを知らせるものです。これは、リストされたインスタンスが侵害され、UDP プロトコルを使用した denial-of-service (DoS) 攻撃の実行に利用されていることを示している可能性があります。

> **Note**
>
> この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

EC2 インスタンスが、TCP ポートで UDP プロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、TCP 通信に通常使用されるポートを対象とした大量のアウトバウンド UDP トラフィックを生成している EC2 インスタンスが AWS 環境にあることを知らせるものです。これは、リストされたインスタンスが侵害され、TCP ポートで UDP プロトコルを使用して (DoS) 攻撃を実行する denial-of-serviceために使用されていることを示している可能性があります。

> **Note**
>
> この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Backdoor:EC2/DenialOfService.UnusualProtocol

EC2 インスタンスが、異常なプロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、ご利用の AWS 環境にリストされている EC2 インスタンスが、Internet Group Management Protocol などの EC2 インスタンスでは通常使用されない異常なプロトコルタイプから大量のアウトバウンドトラフィックを生成していることを知らせるものです。これは、インスタンスが侵害され、異常なプロトコルを使用した denial-of-service (DoS) 攻撃の実行に利用されていることを示している可能性があります。この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Backdoor:EC2/Spambot

EC2 インスタンスがポート 25 でリモートホストと通信して異常な動作を示しています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがポート 25 でリモートホストと通信していることを知らせるものです。この EC2 インスタンスにはポート 25 での通信履歴が以前にないため、この動作は通常と異なります。従来、ポート 25 はメールサーバーで SMTP 通信のために使用されています。この検出結果は、EC2 インスタンスが侵害されており、スパムの送信に利用されている可能性があることを示しています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Behavior:EC2/NetworkPortUnusual

EC2 インスタンスが通常と異なるサーバーポートでリモートホストと通信しています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、確立されたベースラインから逸脱して動いていることを知らせるものです。この EC2 インスタンスには、このリモートポートでの通信履歴がありません。

> **Note**
>
> EC2 インスタンスがポート 389 またはポート 1389 で通信した場合、関連する検出の重要度は [High] (高) に変更され、検出結果フィールドには次の値が含まれます。
>
> - service.additionalInfo.context = Possible log4j callback

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Behavior:EC2/TrafficVolumeUnusual

EC2 インスタンスがリモートホストに対して通常と異なる大量のネットワークトラフィックを生成しています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、確立されたベースラインから逸脱して動いていることを知らせるものです。この EC2 インスタンスでは、このリモートホストに対してこれほど大量のトラフィックを送信した履歴がありません。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

CryptoCurrency:EC2/BitcoinTool.B

EC2 インスタンスが暗号通貨関連のアクティビティに関連付けられている IP アドレスをクエリしています。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスでビットコインやその他の暗号通貨関連アクティビティに紐づけられた IP アドレスがクエリされていることを知らせるものです。ビットコインは、他の通貨、製品、サービスと交換できる国際的な暗号通貨およびデジタル決済システムです。ビットコインはビットコインマイニングの報酬であり、脅威アクターを高度に追及します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスがを使用する場合、またはこのインスタンスがブロックチェーンのアクティビティに関与している場合は、この検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `CryptoCurrency:EC2/BitcoinTool.B` という値を使用します。2 つ目のフィルター条件では、ブロックチェーンのアクティビティに関係するインスタンスの [Instance ID] (インスタンス ID) を使用します。抑制ルールの作成の詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

CryptoCurrency:EC2/BitcoinTool.B!DNS

EC2 インスタンスが暗号通貨関連のアクティビティに関連付けられているドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスで、ビットコイン、またはその他の暗号通貨関連アクティビティに紐づけたドメインがクエリされていることを知らせるものです。ビットコインは、他の通貨、製品、サービスと交換できる国際的な暗号通貨およびデジタル決済システムです。ビットコインはビットコインマイニングの報酬であり、脅威アクターを高度に追及します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスがを使用する場合、またはこのインスタンスがブロックチェーンのアクティビティに関与している場合は、この検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `CryptoCurrency:EC2/BitcoinTool.B!DNS` という値を使用します。2 つ目のフィルター条件では、ブロックチェーンのアクティビティに関係するインスタンスの [Instance ID] (インスタンス ID) を使用します。抑制ルールの作成の詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

DefenseEvasion:EC2/UnusualDNSResolver

Amazon EC2 インスタンスでは、例外的なパブリック DNS リゾルバーと通信しています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した Amazon EC2 インスタンスが、ベースラインの動作から逸脱して動いていることを知らせるものです。この EC2 インスタンスには、このパブリック DNS リゾルバーに対する最近の通信履歴がありません。 GuardDuty コンソールの検出結果の詳細パネルの Unusual フィールドには、クエリされた DNS リゾルバーに関する情報が表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

DefenseEvasion:EC2/UnusualDoHActivity

Amazon EC2 インスタンスが、例外的な DNS over HTTPS (DoH) 通信を実行しています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境内のリスト化した Amazon EC2 インスタンスが、確立されたベースラインから逸脱して動いていることを知らせるものです。この EC2 インスタンスには、このパブリック DoH サーバーとの DNS over HTTPS (DoH) 通信の最近の履歴はありません。検出結果の詳細の [例外的] フィールドには、問い合わせた DoH サーバーに関する情報が表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

DefenseEvasion:EC2/UnusualDoTActivity

Amazon EC2 インスタンスが、例外的な DNS over TLS (DoT) 通信を実行しています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、確立されたベースラインから逸脱して動いていることを知らせるものです。この EC2 インスタンスには、このパブリック DoT サーバーとの DNS over TLS (DoT) 通信の最近の履歴はありません。検出結果詳細パネルの [例外的] フィールドには、問い合わせた DoT サーバーに関する情報が表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Impact:EC2/AbusedDomainRequest.Reputation

EC2 インスタンスが、既知の悪用されたドメインに関連付けられた評価の低いドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- データソース; DNS ログ

この検出結果は、AWS 環境内にリストされている Amazon EC2 インスタンスが、既知の悪用されたドメインまたは IP アドレスに関連付けられたレピュテーションの低いドメイン名をクエリしていることを知らせるものです。悪用したドメインの例としては、動的 DNS プロバイダーだけでなく、無料のサブドメイン登録を提供する最上位のドメイン名 (TLD) と第 2 位のドメイン名 (2LD) があります。脅威アクターは、無料または低コストでドメインを登録するこれらのサービスを使用する傾向があります。このカテゴリの評価の低いドメインは、レジストラのパーキング IP アドレスを決定する有効期限切れドメインであり、アクティブになっていない可能性があります。パーキング IP は、レジストラがどのサービスにもリンクされていないドメインのトラフィックを管理する場所です。脅威アクターが一般的にこれらのレジストラのサービスまたは C&C のサービス、マルウェア配布に使用するため、リストされた Amazon EC2 インスタンスは侵害される可能性があります。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Impact:EC2/BitcoinDomainRequest.Reputation

EC2 インスタンスが、暗号通貨関連のアクティビティに関連付けられている評判の低いドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境のリスト化した Amazon EC2 インスタンスで、ビットコイン、またはその他の暗号通貨関連アクティビティに紐づけた評判の低いドメイン名がクエリされていることを知らせるものです。ビットコインは、他の通貨、製品、サービスと交換できる国際的な暗号通貨およびデジタル決済システムです。ビットコインはビットコインマイニングの報酬であり、脅威アクターを高度に追及します。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスがを使用する場合、またはこのインスタンスがブロックチェーンのアクティビティに関与している場合は、この検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `Impact:EC2/BitcoinDomainRequest.Reputation` という値を使用します。2 つ目のフィルター条件では、ブロックチェーンのアクティビティに関係するインスタンスの [Instance ID] (インスタンス ID) を使用します。抑制ルールの作成の詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Impact:EC2/MaliciousDomainRequest.Reputation

EC2 インスタンスが、悪意のある既知のドメインに関連付けられた評判の低いドメインをクエリしています。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境内にリストされている Amazon EC2 インスタンスが、悪意のある既知のドメインまたは IP アドレスに関連付けられたレピュテーションの低いドメイン名をクエリしていることを知らせるものです。例えば、ドメインを既知のシンクホール IP アドレスに関連付けることができます。シンクホールドメインは、以前に脅威アクターに制御されたドメインであり、ドメインへのリクエストは、インスタンスが侵害されていることを示している場合があります。これらのドメインは、悪意のある既知のキャンペーンやドメイン生成アルゴリズムと相関している可能性もあります。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Impact:EC2/PortSweep

EC2 インスタンスが、多数の IP アドレスのポートを調査しています。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、AWS 環境にリスト化した EC2 インスタンスが、多数のパブリックにルーティング可能な IP アドレス上のポートを調査していることを知らせるものです。このアクティビティタイ

プは、通常脆弱性ホストを見つけて悪用するのに使われます。 GuardDuty コンソールの検出結果の詳細パネルには、最新のリモート IP アドレスのみが表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Impact:EC2/SuspiciousDomainRequest.Reputation

EC2 インスタンスが、年齢や低人気により、本質的に疑わしい、低評判のドメイン名をクエリしています。

デフォルトの重要度: [Low] (低)

- データソース; DNS ログ

この検出結果は、AWS 環境のリスト化した Amazon EC2 インスタンスが悪意があると疑われたり、過去に悪意のあるドメインだったため評判の低いドメイン名をクエリしていることを知らせるものですが、当社の評判モデルは、既知の脅威と明確に関連付けることができませんでした。これらのドメインは通常、新たに観察されるか、または少量のトラフィックを受信します。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Impact:EC2/WinRMBruteForce

EC2 インスタンスがアウトバウンドの Windows リモート管理総当たり攻撃を実行しています。

デフォルトの重要度: [Low] (低)*

> **Note**
>
> EC2 インスタンスが総当たり攻撃の対象である場合、この検出結果の重要度は「低」です。EC2 インスタンスが総当たり攻撃の動作主体である場合、この検出結果の重要度は「高」です。

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、Windows ベースのシステム上の Windows リモート管理サービスへのアクセスを目的とした Windows リモート管理 (WinRM) 総当たり攻撃を実行していることを知らせるものです。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Recon:EC2/PortProbeEMRUnprotectedPort

EC2 インスタンスの保護されていない EMR 関連のポートを悪意のある既知のホストが探しています。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、 AWS環境のクラスターの一部であるリスト化した EC2 インスタンスの EMR 関連の機密ポートが、セキュリティグループ、アクセスコントロールリスト (ACL)、または Linux IPTables などのオンホストファイアウォールによってブロックされていないことを知らせるものです。この検出結果は、インターネット上の既知のスキャナーがこのポートを積極的に調査していることも知らせるものです。ポート 8088 (YARN ウェブ UI ポート) など、この検出結果をトリガーできるポートは、リモートコード実行で使用される可能性があります。

修復のレコメンデーション

インターネットからクラスター上のポートへのオープンアクセスをブロックし、それらのポートへのアクセスを必要とする特定の IP アドレスのみにアクセスを制限する必要があります。詳細については、「Security Groups for EMR Clusters」(EMR クラスターのセキュリティグループ) を参照してください。

Recon:EC2/PortProbeUnprotectedPort

EC2 インスタンスの保護されていないポートを悪意のある既知のホストが探しています。

デフォルトの重要度: [Low] (低)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Low] (低) です。ただし、調査対象のポートが Elasticsearch (9200 または 9300) で使用されている場合、検出結果の重要度は High になります。

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスのポートが、セキュリティグループ、アクセスコントロールリスト (ACL)、Linux IPTables など、ホスト上のファイアウォールでブロックされておらず、インターネットの既知のスキャナーが積極的に調査していることを知らせるものです。

識別された保護されていないポートが 22 または 3389 であり、それらのポートを使用してインスタンスに接続している場合は、それらのポートへのアクセスを自社ネットワークの IP アドレス空間の IP アドレスのみに許可することで公開を制限することができます。Linux でポート 22 へのアクセスを制限するには、「Linux インスタンス用の受信トラフィックの認可」を参照してください。Windows でポート 3389 へのアクセスを制限するには、「Windows インスタンス用の受信トラフィックの認可」を参照してください。

GuardDuty は、ポート 443 および 80 に対してこの検出結果を生成しません。

修復のレコメンデーション

インスタンスがウェブサーバーをホストしている場合など、インスタンスが意図的に公開されている場合があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `Recon:EC2/PortProbeUnprotectedPort` という値を使用します。2 番目のフィルター条件は、要塞ホストとして機能する 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可能な条件に応じて、[Instance image ID] (インスタンスイメージ ID) 属性または [Tag] (タグ) 値の属性のいずれかを使用できます。抑制ルールの作成の詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Recon:EC2/Portscan

EC2 インスタンスがリモートホストにアウトバウンドポートスキャンを実行しています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが短時間にに複数のポートに接続しようとして、ポートスキャン攻撃を行っている可能性があることを知らせるものです。ポートスキャン攻撃の目的は、オープンポートを見つけ、マシンで実行されているサービスを発見してそのオペレーティングシステムを特定することです。

修復のレコメンデーション

この検出結果は、ご利用の環境の EC2 インスタンスに脆弱性評価アプリケーションがデプロイされており、それらのアプリケーションがポートをスキャンして、誤ってオープンポート設定になっているものをアラートするので、誤検出される可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `Recon:EC2/Portscan` という値を使用します。2 番目のフィルター条件は、これらの脆弱性評価ツールをホストする 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可能な条件に応じて、[Instance image ID] (インスタンスイメージ

ID) 属性または [Tag] (タグ) 値の属性のいずれかを使用できます。抑制ルールの作成の詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/BlackholeTraffic

EC2 インスタンスが既知のブラックホールであるリモートホストの IP アドレスに通信しようとしています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがブラックホール (あるいはシンクホール) の IP アドレスと通信しようとしているため、侵害されている可能性があることを知らせるものです。ブラックホールとは、送受信トラフィックが密かに破棄されるネットワークの場所を指し、意図した受信者にデータが届いていないことは送信元に知らされません。ブラックホール IP アドレスは、稼働していないホストマシンやホストが割り当てられていないアドレスを指定します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/BlackholeTraffic!DNS

EC2 インスタンスがブラックホールの IP アドレスにリダイレクトされるドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- データソース; DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがブラックホール IP アドレスにリダイレクトされるドメイン名をクエリしているため、侵害されている可能性があることを知らせるもの

です。ブラックホールとは、送受信トラフィックが密かに破棄されるネットワークの場所を指し、意図した受信者にデータが届いていないことは送信元に知らされません。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/DGADomainRequest.B

EC2 インスタンスがアルゴリズムを使用して生成されたドメインをクエリしています。このようなドメインは、マルウェアによって悪用されることが多く、EC2 インスタンスが侵害されている場合があります。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがドメイン生成アルゴリズム (DGA) のドメインをクエリしようとしていることを知らせるものです。EC2 インスタンスは侵害されている可能性があります。

DGA は、大量のドメイン名を定期的に生成してコマンドアンドコントロール (C&C) サーバーとのランデブーポイントとするために使用されます。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータであり、一般的なタイプのマルウェアに感染して制御されたインターネットのコネクテッドデバイスのコレクションです。ランデブーポイントの候補数が多いと、感染されたコンピュータは毎日これらのドメイン名の一部にアクセスしてアップデートやコマンドを受け取ろうとするため、ボットネットを効果的にシャットダウンすることが困難となります。

> **Note**
>
> この検出結果は、アドバンストな経験則を使用したドメイン名分析に基づいており、脅威インテリジェンスフィードでは検出されない新しい DGA ドメインを識別する可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/DGADomainRequest.C!DNS

EC2 インスタンスがアルゴリズムを使用して生成されたドメインをクエリしています。このようなドメインは、マルウェアによって悪用されることが多く、EC2 インスタンスが侵害されている場合があります。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがドメイン生成アルゴリズム (DGA) のドメインをクエリしようとしていることを知らせるものです。EC2 インスタンスは侵害されている可能性があります。

DGA は、大量のドメイン名を定期的に生成してコマンドアンドコントロール (C&C) サーバーとのランデブーポイントとするために使用されます。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータであり、一般的なタイプのマルウェアに感染して制御されたインターネットのコネクテッドデバイスのコレクションです。ランデブーポイントの候補数が多いと、感染されたコンピュータは毎日これらのドメイン名の一部にアクセスしてアップデートやコマンドを受け取ろうとするため、ボットネットを効果的にシャットダウンすることが困難となります。

> **Note**
>
> この検出結果は、 の脅威インテリジェンスフィードの既知の DGA GuardDutyドメインに基づいています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/DNSDataExfiltration

EC2 インスタンスが DNS クエリを使用してデータを密かに抽出しようとしています。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、アウトバウンドデータ転送用の DNS クエリを使用しているマルウェアであることを知らせるものです。このタイプのデータ転送は、侵害されたインスタンスを示し、データの漏洩につながる可能性があります 通常、DNS トラフィックはファイアウォールでブロックされません。例えば、侵害された EC2 インスタンスのマルウェアは、データ (クレジットカード番号など) を DNS クエリ内にエンコードし、それを攻撃者が制御するリモート DNS サーバーに送信できます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/DriveBySourceTraffic!DNS

EC2 インスタンスがドライブバイダウンロード攻撃の既知の攻撃元であるリモートホストのドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、自動ダウンロード攻撃の既知のソースであるリモートホストのドメイン名をクエリしているため、リスト化した AWS 環境の EC2 インスタンスが侵害された可能性があることを知らせるものです。これらは、インターネットから意図せずにダウンロードされるコンピュータソフトウェアであり、ウイルス、スパイウェア、マルウェアの自動インストールをトリガーする場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/DropPoint

EC2 インスタンスが、マルウェアによって収集された認証情報やその他の盗難されたデータを保持していることが認識されているリモートホストの IP アドレスに通信しようとしています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスで、マルウェアが取り込んだ認証情報やその他の盗難されたデータを保持して、リモートホストの IP アドレスに通信しようとしていることを知らせるものです。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/DropPoint!DNS

EC2 インスタンスが、マルウェアによって収集された認証情報やその他の盗難されたデータを保持していることが認識されているリモートホストのドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- データソース; DNS ログ

この検出結果は、AWS 環境の EC2 インスタンスで、マルウェアが取り込んだ認証情報やその他の盗難されたデータを保持するリモートホストのドメイン名をクエリしていることを知らせるものです。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Trojan:EC2/PhishingDomainRequest!DNS

EC2 インスタンスがフィッシング攻撃に関与しているドメインをクエリしています。EC2 インスタンスは侵害されている可能性があります。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境の EC2 インスタンスがフィッシング攻撃に関与しているドメインをクエリしようとしていることを知らせるものです。フィッシングドメインは、個人を特定できる情報、銀行やクレジットカードの詳細情報とパスワードなど、ユーザーが機密データを提供するように仕向ける、正当な機関になりすました人物によって設定されます。EC2 インスタンスがフィッシングウェブサイトに保存されている機密データを検索しようとしたり、フィッシングウェブサイトを設定しようとしたりする可能性があります。EC2 インスタンスは侵害されている可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

EC2 インスタンスがカスタム脅威リストの IP アドレスに接続しています。

デフォルトの重要度: [Medium] (中)

- データソース: VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスが、ユーザーがアップロードした脅威リストに含まれている IP アドレスを使用してアウトバウンド通信していることを知らせるものです。GuardDuty で、脅威リストは既知の悪意のある IP アドレスで構成されます。 GuardDuty は、アップロードされた脅威リストに基づいて結果を生成します。この検出結果を生成するために使用された脅威リストは、検出結果の詳細に表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

UnauthorizedAccess:EC2/MetadataDNSRebind

EC2 インスタンスが、インスタンスメタデータサービスに解決する DNS 検索を実行しています。

デフォルトの重要度: [High] (高)

- データソース; DNS ログ

この検出結果は、AWS 環境の EC2 インスタンスが、EC2 メタデータ IP アドレス (169.254.169.254) を決定するドメインをクエリしていることを知らせるものです。この種類の DNS クエリは、インスタンスが DNS リバイディング技術の対象であることを示している可能性があります。この手法は、インスタンスに関連付けらた IAM 認証情報など、EC2 インスタンスからメタデータを取得するために使用できます。

DNS リバインディングには、EC2 インスタンスで実行されているアプリケーションをだまして URL から返されるデータをロードすることが含まれます。URL のドメイン名は EC2 メタデータ IP アドレス (169.254.169.254) に解決されます。これにより、アプリケーションは EC2 メタデータにアクセスし、攻撃者がそのメタデータを使用できるようにする可能性があります。

EC2 インスタンスが URL の追加を許可する脆弱なアプリケーションを実行している場合や、EC2 インスタンスで実行されているウェブブラウザで、誰かが URL にアクセスする場合のみ、DNS リバインディングを使用して EC2 メタデータにアクセスできます。

修復のレコメンデーション

この検出結果に応じて、EC2 インスタンスで実行されている脆弱性アプリケーションがあるか、誰が検出結果で識別したドメインへアクセスするためブラウザを使用しているかを評価する必要があります。根本的な原因が脆弱なアプリケーションである場合は、脆弱性を修復する必要があります。ユーザーが識別したドメインを閲覧した場合、ドメインをブロックするか、ユーザーがそのドメインにアクセスできないようにします。この検出結果が上記のいずれかのケースに関連していると判断した場合は、EC2 インスタンスに関連付けられたセッションを取り消す必要があります。

一部の AWS のお客様は、メタデータ IP アドレスを信頼できる DNS サーバーのドメイン名に意図的にマッピングします。ご利用の環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `UnauthorizedAccess:EC2/MetaDataDNSRebind` という値を使用します。2 つ目のフィルター条件では、DNS リクエストのドメインを使用します。値はメタデータの IP アドレス (169.254.169.254) にマッピングしたドメインと一致する必要があります。抑制ルールの作成の詳細については、「抑制ルール」を参照してください。

UnauthorizedAccess:EC2/RDPBruteForce

EC2 インスタンスが RDP ブルートフォース攻撃に巻き込まれています。

デフォルトの重要度: [Low] (低)*

> **Note**
>
> EC2 インスタンスが総当たり攻撃の対象である場合、この検出結果の重要度は「低」です。EC2 インスタンスが総当たり攻撃の動作主体である場合、この検出結果の重要度は「高」です。

- データソース: VPC フローログ

この検出結果は、 AWS 環境の EC2 インスタンスが、Windows ベースのシステムで RDP サービスへのパスワードを取得することを目的としたブルートフォース攻撃に関与していることを知らせるものです。これは、AWS リソースへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

インスタンスのリソースロールが ACTOR の場合は、インスタンスが RDP 総当たり攻撃の実行に利用されたことを示しています。このインスタンスに Target としてリストされた IP アドレスと通信する合理的な理由がない限りは、インスタンスが侵害されたと仮定し、侵害された可能性のある Amazon EC2 インスタンスの修復 でリストされたアクションを取ることをお勧めします。

インスタンスの [Resource Role] (リソースロール) が TARGET である場合は、セキュリティグループ、ACL、ファイアウォールのいずれかを使用して RDP ポートを信頼できる IP のみ保護することで、この検出結果を修復できます。詳細については、「EC2 インスタンスの保護のヒント (Linux)」を参照してください。

UnauthorizedAccess:EC2/SSHBruteForce

EC2 インスタンスが SSH ブルートフォース攻撃に巻き込まれています。

デフォルトの重要度: [Low] (低)*

> **Note**
>
> 総当たり攻撃が EC2 インスタンスのいずれかを標的にしている場合、この検出結果の重要度は「低」です。EC2 インスタンスが総当たり攻撃の動作主体である場合、この検出結果の重要度は「高」です。

- データソース: VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスが、Linux ベースのシステムで SSH サービスへのパスワードを取得目的の総当たり攻撃に関与したことを知らせるものです。これは、AWS リソースへの未承認のアクセスを示している場合があります。

> **Note**
>
> この検出結果は、ポート 22 のモニタリングトラフィックを通じてのみ生成されます。SSH サービスが他のポートを使用するように設定されている場合には、この検出結果は生成されません。

修復のレコメンデーション

総当たり攻撃の対象が要塞ホストである場合、これはご利用の AWS 環境の想定内の動作を示している可能性があります。このような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `UnauthorizedAccess:EC2/SSHBruteForce` という値を使用します。2 番目のフィルター条件は、要塞ホストとして機能する 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可能な条件に応じて、[Instance image ID] (インスタンスイメージ ID) 属性または [Tag] (タグ) 値の属性のいずれかを使用できます。抑制ルールの作成の詳細については、「抑制ルール」を参照してください。

このアクティビティがご利用の環境で想定外であり、インスタンスの [Resource Role] (リソースロール) が `TARGET` である場合は、セキュリティグループ、ACL、ファイアウォールのいずれかを使用して SSH ポートを信頼できる IP のみ保護することで、この検出結果を修復できます。詳細については、「EC2 インスタンスの保護のヒント (Linux)」を参照してください。

インスタンスの [Resource Role] (リソースロール) が `ACTOR` の場合は、インスタンスが SSH 総当たり攻撃の実行に利用されたことを示しています。このインスタンスに `Target` としてリストされた IP アドレスと通信する合理的な理由がない限りは、インスタンスが侵害されたと仮定し、侵害された可能性のある Amazon EC2 インスタンスの修復 でリストされたアクションを取ることをお勧めします。

UnauthorizedAccess:EC2/TorClient

EC2 インスタンスが Tor Guard または Authority ノードに接続しています。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスが TorGuard または 権限ノードに接続中であることを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。Tor Guards および Authority ノードは、Tor ネットワークへの初期ゲートウェイとして動作します。このトラフィックは、この EC2 インスタンスが侵害され、Tor ネットワーク上のクライアントとして動作していることを示している場合があります。この検出結果は、攻撃者が真のアイデンティティを隠して、AWS リソースへの不正アクセスを示している場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

UnauthorizedAccess:EC2/TorRelay

EC2 インスタンスが Tor リレーとして Tor ネットワークに接続しています。

デフォルトの重要度: [High] (高)

- データソース: VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスが Tor リレーとして動作していることを示す方法で、Tor ネットワークに接続中であることを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。ある Tor リレーから別の Tor リレーにクライアントの不正なトラフィックを転送することで、通信の匿名性を高めます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

GuardDuty IAM 検出結果タイプ

次の検出結果は、IAM エンティティとアクセスキーに特有であり、常に `AccessKey` の [Resource Type] (リソースタイプ) です。検出結果の重要度と詳細は、検出結果タイプによって異なります。

ここにリストされている検出結果には、検出結果タイプの生成に使用されるデータソースとモデルが含まれます。詳細については、「基礎データソース」を参照してください。

すべての IAM 関連の検出結果について、問題のエンティティを検証し、その許可が最小特権のベストプラクティスに従っていることを確認することをお勧めします。このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。検出結果の修正についての詳細は、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

トピック

- CredentialAccess:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/AnomalousBehavior

- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

AWS 環境へのアクセスに使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティで近

似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者がユーザーの環境のパスワード、ユーザー名、およびアクセスキーを収集しようすると、攻撃の認証情報アクセスステージに一般的に関連しています。このカテゴリの API は、`GetPasswordData`、`GetSecretValue`、`GenerateDbAuthToken` です。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

DefenseEvasion:IAMUser/AnomalousBehavior

防御対策を回避するために使用された API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティで近似の一連の関連 API リクエストが含まれる場合があります。観察された API は、攻撃者が自分のトラックをカバーし、検出を回避しようとしている防御回避戦術に一般的に関連しています。このカテゴリの API は通常、削除、無効化、停止オペレーションです (`DeleteFlowLogs`、`DisableAlarmActions`、`StopLogging` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Discovery:IAMUser/AnomalousBehavior

リソースの検出に一般的に使用される API が、異常な方法で呼び出されました。

デフォルトの重要度: [Low] (低)

- データソース: CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティで近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者が情報を収集して AWS 、環境がより広範な攻撃の影響を受けやすいかどうかを判断する場合に、攻撃の検出段階に一般的に関連します。このカテゴリの API は、get、describe、または list オペレーションです (`DescribeInstances`、`GetRolePolicy`、または `ListAccessKeys` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Exfiltration:IAMUser/AnomalousBehavior

AWS 環境からデータを収集するために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [High] (高)

- データソース: CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティで近似の一連の関連 API リクエストが含まれる場合があります。観測された API は、侵入戦術に一般的に関連していて、そこでは攻撃者がネットワークからデータを収集しようとしています。この検出結果タイプの API は管理 (コントロールプレーン)オペレーションのみであり、通常は、S3、スナップショット、およびデータベースに関連しています (`PutBucketReplication`、`CreateSnapshot`、`RestoreDBInstanceFromDBSnapshot` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Impact:IAMUser/AnomalousBehavior

AWS 環境内のデータまたはプロセスを改ざんするために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [High] (高)

- データソース: CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティで近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者がオペレーションを中断し、ユーザーのアカウント内のデータを操作、中断、または破壊しようとするインパクト戦術に一般的に関連しています。この検出結果タイプの API は、通常、delete、update、または put オペレーションです (`DeleteSecurityGroup`、`UpdateUser`、`PutBucketPolicy` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

InitialAccess:IAMUser/AnomalousBehavior

AWS 環境への不正アクセスを得るために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティで近似の一連の関連 API リクエストが含まれる場合があります。攻撃者がユーザーの環境へのアクセスを確立しようとすると、観察される API は、攻撃の初期アクセス段階に一般的に関連しています。このカテゴリの API は、通常 get トークン、またはセッションオペレーションです (`GetFederationToken`、`StartSession`、`GetAuthorizationToken` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

PenTest:IAMUser/KaliLinux

API が Kali Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、Kali Linux を実行しているマシンが、 環境のリストされた AWS アカウントに属する認証情報を使用して API コールを行っていることを知らせるものです。Kali Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。また、攻撃者はこのツールを使用して EC2 設定の弱点を見つけ、AWS 環境への不正アクセスを行います。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

PenTest:IAMUser/ParrotLinux

API が Parrot Security Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、Parrot Security Linux を実行しているマシンが、 環境のリストされた AWS アカウントに属する認証情報を使用して API コールを行っていることを知らせるものです。Parrot Security Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。また、攻撃者はこのツールを使用して EC2 設定の弱点を見つけ、 AWS 環境への不正アクセスを行います。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

PenTest:IAMUser/PentooLinux

API が Pentoo Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、Pentoo Linux を実行しているマシンが、環境内のリストされている AWS アカウントに属する認証情報を使用して API コールを行っていることを知らせるものです。Pentoo Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。また、攻撃者はこのツールを使用して EC2 設定の弱点を見つけ、 AWS 環境への不正アクセスを行います。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Persistence:IAMUser/AnomalousBehavior

AWS 環境への不正アクセスを維持するために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティで近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者がユーザーの環境へのアクセスを獲得し、そのアクセスを維持しようとするパーシスタンス戦術に一般的に関連しています。このカテゴリの API は、通常、create、インimport、または modify オペレーションです (`CreateAccessKey`、`ImportKeyPair`、`ModifyInstanceAttribute` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用する

テクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Policy:IAMUser/RootCredentialUsage

API がルートユーザーサインイン認証情報を使用して呼び出されました。

デフォルトの重要度: [Low] (低)

- データソース: CloudTrail 管理イベントまたは CloudTrail データイベント

この検出結果は、ユーザーの環境のリスト化された AWS アカウント のルートユーザーサインイン認証情報が AWS サービスへのリクエストに使用されていることを知らせるものです。ユーザーは、ルートユーザーのサインイン認証情報を使用して AWS サービスにアクセスしないことをお勧めします。代わりに、 AWS Security Token Service (STS) からの最小特権の一時的な認証情報を使用して AWS サービスにアクセスする必要があります。 AWS STS がサポートされていない状況では、IAM ユーザー認証情報をお勧めします。詳細については、「IAM ベストプラクティス」を参照してください。

> **Note**
>
> アカウントで S3 脅威検出が有効になっている場合、この検出結果は、 AWS アカウント アのルートユーザーサインイン認証情報を使用して S3 リソースで S3 データプレーンオペレーションを実行しようとした場合に応答して生成される可能性があります。使用された API コールは、検出結果の詳細でリスト化されます。S3 脅威検出が有効になっていない場合、この検出結果はイベントログ API によってのみトリガーされます。S3 脅威検出の詳細については、「S3 Protection 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

PrivilegeEscalation:IAMUser/AnomalousBehavior

AWS 環境への高レベルのアクセス許可を取得するために一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、アカウント内で異常な API リクエストが観察されたことを知らせるものです。この検出結果には、単一の API、または単一のユーザーアイデンティティで近似の一連の関連 API リクエストが含まれる場合があります。観察される API は、攻撃者が環境へのより高いレベルの許可を取得しようとする特権エスカレーション戦術に一般的に関連しています。このカテゴリの API は、通常、IAM ポリシー、ロール、ユーザーを変更するオペレーションを含みます (`AssociateIamInstanceProfile`、`AddUserToGroup`、`PutUserPolicy` など)。

この API リクエストは、 の異常検出機械学習 (ML) GuardDutyモデルによって異常として識別されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API など、API リクエストのさまざまな要因を追跡します。リクエストしたユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細 」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Recon:IAMUser/MaliciousIPCaller

API が悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、ユーザーの環境内のアカウントの AWS リソースをリスト化または記述できる API オペレーションが、脅威リストの IP アドレスから呼び出されたことを知らせるものです。攻撃者は、盗まれた認証情報を使用して、より貴重な認証情報を見つけたり、既に持っている認証情報の機能を特定したりするために、 AWS リソースのこの種の偵察を実行する場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Recon:IAMUser/MaliciousIPCaller.Custom

API が悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、ユーザーの環境のアカウントの AWS リソースをリスト化または説明できる API オペレーションがカスタム脅威リストの IP アドレスから呼び出されたことを知らせるものです。使用された脅威リストは、検出結果の詳細に表示されます。攻撃者は、盗まれた認証情報を使用して、より貴重な認証情報を見つけたり、既に持っている認証情報の機能を特定したりするために、 AWS リソースのこの種の偵察を実行する可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Recon:IAMUser/TorIPCaller

API が Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、ユーザーの環境のアカウントの AWS リソースをリスト化または説明できる API オペレーションが Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。Tor は匿

名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。攻撃者は真のアイデンティティを隠すために Tor を使用します。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail ログ記録が無効になりました。

デフォルトの重要度: [Low] (低)

- データソース: CloudTrail 管理イベント

この検出結果は、 AWS 環境内の CloudTrail 証跡が無効になったことを知らせるものです。これにより、悪意ある目的でユーザーの AWS リソースへアクセスしている間、活動の痕跡を消してトラックを隠してログ記録を無効化しようとします。この検出結果は、証跡情報の削除または更新が成功することによってトリガーされる場合があります。この検出結果は、 に関連付けられている証跡から口グを保存する S3 バケットが正常に削除されたことでトリガーすることもできます GuardDuty。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Stealth:IAMUser/PasswordPolicyChange

アカウントのパスワードポリシーが弱化されています。

デフォルトの重要度: [Low] (低)*

> **Note**
>
> この検出結果の重要度は、パスワードポリシーに加えられた変更の重要度に応じて、[Low] (低)、[Medium] (中)、[High] (高) になります。

- データソース: CloudTrail 管理イベント

AWS アカウントパスワードポリシーは、 AWS 環境内のリストされたアカウントで弱まりました。例えば、アカウントの削除、必要な文字数を減らすような更新、記号や数字を不要とする更新、パスワードの有効期限を延長するような更新が行われています。この検出結果は、 AWS アカウントのパスワードポリシーを更新または削除しようとしてトリガーすることもできます。 AWS アカウントパスワードポリシーは、IAM ユーザーに設定できるパスワードの種類を管理するルールを定義します。パスワードポリシーが弱化されると、覚えやすいパスワードや推測しやすいパスワードの作成が可能になり、セキュリティ上のリスクが生じます。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

世界中でコンソールに対する複数の正常なログインが確認されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、世界各地から同時に同じ IAM ユーザーによるコンソールへの複数の正常なログインが確認されたことを知らせるものです。このような異常でリスクの高いアクセス場所パターンは、AWS リソースへの不正アクセスの可能性を示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

インスタンス起動ロールを通じて EC2 インスタンス専用に作成された認証情報は、AWS内の別のアカウントから使用されています。

デフォルトの重要度: [High] (高)*

> **Note**
>
> この検出結果のデフォルトの重要度は [High] (高) です。ただし、API が AWS 環境に関連付けられたアカウントによって呼び出された場合、重要度は Medium になります。

- データソース: CloudTrail 管理イベントまたは S3 データイベント

この検出結果は、EC2 インスタンス認証情報を使用して、関連付けられた EC2 インスタンスが実行されているアカウントとは異なる AWS アカウントが所有する IP アドレスから APIs を呼び出すときに通知します。

AWS では、一時的な認証情報を作成したエンティティ (AWS アプリケーション、EC2、Lambda など) の外部に再配布することはお勧めしません。ただし、承認されたユーザーは EC2 インスタンスから認証情報をエクスポートして正当な API コールを行うことができます。`remoteAccountDetails.Affiliated` フィールドが の場合`True`、API は AWS 環境に関連付けられたアカウントから呼び出されました。攻撃の可能性を排除してアクティビティが正当であることを確認するには、これらの認証情報を割り当てる先の IAM ユーザーに問い合わせてみます。

> **Note**
>
> がリモートアカウントからの継続的なアクティビティ GuardDuty を観察すると、その機械学習 (ML) モデルはこれを予想される動作として識別します。したがって、 GuardDuty は、そのリモートアカウントからのアクティビティに関するこの検出結果の生成を停止します。GuardDuty は、他のリモートアカウントからの新しい動作に関する検出結果を引き続き生成し、時間の経過とともに動作が変化するにつれて、学習したリモートアカウントを再評価します。

修復のレコメンデーション

この検出結果に応じて、次のワークフローを使用して、一連のアクションを決定できます。

1. `service.action.awsApiCallAction.remoteAccountDetails.accountId` フィールドから関係するリモートアカウントを特定します。

2. 次に、そのアカウントが `service.action.awsApiCallAction.remoteAccountDetails.affiliated`フィールドから環境 GuardDutyに関連付けられているかどうかを確認します。
3. アカウントが連携している場合は、リモートアカウントの所有者と EC2 インスタンスの認証情報の所有者に問い合わせて、調査してください。
4. アカウントが関連付けられていない場合、まず、アカウントが組織に関連付けられているがマルチアカウント設定の一部 GuardDutyではないか、アカウントで GuardDuty まだ有効になっていないかを評価します。それ以外の場合は、EC2 認証情報の所有者に問い合わせて、リモートアカウントがこれらの認証情報を使用するユースケースがあるかどうかを判断します。
5. 認証情報の所有者がリモートアカウントを認識しない場合は、 AWS内で動作する脅威アクターによって認証情報が侵害された可能性があります。ご利用の環境を保護するために、侵害された可能性のある Amazon EC2 インスタンスの修復 で推奨されているステップを実行する必要があります。

   さらに、 AWS Trust and Safety チームに不正使用レポートを送信して、リモートアカウントの調査を開始できます。 AWS Trust and Safety にレポートを送信するときは、検出結果の完全な JSON の詳細を含めます。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

インスタンス作成ロールで EC2 インスタンス専用に作成された認証情報が外部 IP アドレスから使用されています。

デフォルトの重要度: [High] (高)

- データソース: CloudTrail 管理イベントまたは S3 データイベント

この検出結果は、 以外のホスト AWS が AWS 、環境の EC2 インスタンスで作成された一時的な AWS 認証情報を使用して AWS API オペレーションを実行しようとしたことを知らせるものです。リストされている EC2 インスタンスが侵害されている可能性があり、このインスタンスの一時的な認証情報が の外部にあるリモートホストに流出した可能性があります AWS。 AWS は、一時的な認証情報を作成したエンティティ (AWS アプリケーション、EC2、Lambda など) の外部に再配布することはお勧めしません。ただし、承認されたユーザーは EC2 インスタンスから認証情報をエクスポートして正当な API コールを行うことができます。潜在的な攻撃を除外し、アクティビティの正当性を検証するには、検出結果においてリモート IP からのインスタンスの認証情報の使用が想定されるかどうかを検証します。

> **Note**
>
> がリモートアカウントからの継続的なアクティビティ GuardDuty を観察すると、その機械学習 (ML) モデルはこれを予想される動作として識別します。したがって、 GuardDuty は、そのリモートアカウントからのアクティビティに関するこの検出結果の生成を停止します。GuardDuty は、他のリモートアカウントからの新しい動作に関する検出結果を引き続き生成し、時間の経過とともに動作が変化するにつれて、学習したリモートアカウントを再評価します。

修復のレコメンデーション

この検出結果が生成されるのは、VPC インターネットゲートウェイ (IGW) からではなく、オンプレミスのゲートウェイから排出され、インターネットトラフィックがルーティングされるように、ネットワークが構成されている場合です。AWS Outposts や VPC VPN 接続などの一般的な構成では、このようにトラフィックがルーティングされる可能性があります これが予期した動作である場合は、抑制ルールを使用して、2 つのフィルター条件で構成されるルールを作成することをお勧めします。1 つ目の条件では、[finding type] (結果タイプ) に `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` を使用します。2 番目のフィルター条件は、オンプレミスインターネットゲートウェイの IP アドレスまたは CIDR 範囲を持つ [API caller IPv4 Address] (API 発信者の IPv4 アドレス) です。抑制ルールの作成の詳細については、「抑制ルール」を参照してください。

> **Note**
>
> が外部ソースからの継続的なアクティビティ GuardDuty を観察した場合、その機械学習モデルはこれを予想される動作として識別し、そのソースからのアクティビティについてこの検出結果の生成を停止します。 GuardDuty は他のソースからの新しい動作の検出結果を引き続き生成し、時間の経過とともに動作が変化するにつれて学習したソースを再評価します。

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。「侵害された可能性のある AWS 認証情報の修正」を参照してください。

UnauthorizedAccess:IAMUser/MaliciousIPCaller

API が悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、API オペレーション (EC2 インスタンスの起動、新しい IAM ユーザーの作成、AWS 権限の変更など) が悪意のある既知の IP アドレスから呼び出されたことを知らせるものです。これは、環境内の AWS リソースへの不正アクセスを示している可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

API がカスタム脅威リストにある IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、API オペレーション (EC2 インスタンスの起動、新しい IAM ユーザーの作成、AWS 権限の変更など) が、アップロードした脅威リストに含まれている IP アドレスから呼び出されたことを知らせるものです。 では、脅威リストは悪意のある既知の IP アドレスで構成されます。これは、環境内の AWS リソースへの不正アクセスを示している可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

UnauthorizedAccess:IAMUser/TorIPCaller

API が Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース: CloudTrail 管理イベント

この検出結果は、API オペレーション (EC2 インスタンスの起動、新しい IAM ユーザーの作成、AWS 権限の変更などの試行など) が Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、攻撃者が真のアイデンティティを隠しているという意図により、 AWS リソースへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

EKS 監査ログの検出結果タイプ

次の検出結果は Kubernetes リソースに固有であり、resource_type は `EKSCluster` です。検出結果の重要度と詳細は、検出結果タイプによって異なります。

すべての Kubernetes タイプの検出結果については、問題のリソースを調べて、アクティビティが想定されたものであるのか、または悪意あるアクティビティである可能性があるのかを判断することをお勧めします。 GuardDuty 検出結果によって識別された侵害された Kubernetes リソースの修正に関するガイダンスについては、「」を参照してくださいEKS 監査ログのモニタリング検出結果の修正。

> **Note**
>
> これらの結果を生成する原因となるアクティビティが想定される場合は、今後アラートが発生しないように 抑制ルール を追加することを検討してください。

トピック

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Kubernetes バージョン 1.14 以前は、`system:unauthenticated`グループは`system:basic-user`ClusterRolesデフォルトで `system:discovery`および に関連付けられていました。この関連付けは、匿名ユーザーからの意図しないアクセスを許可する場合があります。クラスターの更新では、これらの許可は取り消されません。クラスターをバージョン 1.14 以降に更新した場合でも、これらの許可は引き続き有効になっている可能性があります。これらの許可の関連付けを `system:unauthenticated` グループから解除することをお勧めします。これらのアクセス許可を取り消す方法については、「Amazon EKS ユーザーガイド」の「Amazon EKS 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。

CredentialAccess:Kubernetes/MaliciousIPCaller

Kubernetes クラスターの認証情報またはシークレットにアクセスするために一般的に使用される API が悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが悪意のある既知のアクティビティと関連した IP アドレスから呼び出されたことを知らせるものです。観察された API は、攻撃者が Kubernetes クラスターのパスワード、ユーザー名、およびアクセスキーの収集を試みている認証情報アクセス戦術に一般的に関連付けられています。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが である場合は`system:anonymous`、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の手順に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消すことを許可された理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Kubernetes クラスターの認証情報またはシークレットにアクセスするために一般的に使用される API が、カスタム脅威リストの IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが、アップロード済みの脅威リストに含まれている IP アドレスから呼び出されたことを知らせるものです。この検出結果に関連する脅威リストは、検出結果の詳細の [Additional Information] (追加情報) セクションにリストされています。観察された API は、攻撃者が Kubernetes クラスターのパスワード、ユーザー名、およびアクセスキーの収集を試みている認証情報アクセス戦術に一般的に関連付けられています。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが である場合は`system:anonymous`、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の手順に従って、匿名ユーザーが API の呼び出しとアクセス許可の取り消しを許可された理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Kubernetes クラスターの認証情報またはシークレットにアクセスするために一般的に使用される API が、認証されていないユーザーによって呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが `system:anonymous` ユーザーによって正常に呼び出されたことを知らせるものです。`system:anonymous` によって実行された API コールは認証されていません。観察された API は、攻撃者が Kubernetes クラスターのパスワード、ユーザー名、およびア

クセスキーの収集を試みている認証情報アクセス戦術に一般的に関連付けられています。このアクティビティは、検出結果で報告された API アクションで匿名アクセスまたは非認証アクセスが許可され、他のアクションで許可される可能性があることを示します。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります。

修復のレコメンデーション

クラスター上の `system:anonymous` ユーザーに付与されている許可を調べて、すべての許可が必要であることを確認する必要があります。誤って、または悪意を持って許可が付与された場合は、ユーザーのアクセスを取り消し、クラスターに対して攻撃者が加えた変更を元に戻す必要があります。詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS 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。

詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

CredentialAccess:Kubernetes/TorIPCaller

Kubernetes クラスターの認証情報またはシークレットにアクセスするために一般的に使用される API が、Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API が Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。観察された API は、攻撃者が Kubernetes クラスターのパスワード、ユーザー名、およびアクセスキーの収集を試みている認証情報アクセス戦術に一般的に関連付けられています。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、攻撃者が真のアイデンティティを隠す意図を持った、Kubernetes クラスターのリソースへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが である場合は`system:anonymous`、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消すことを許可された理由を調べます。ユーザーが認証されたユーザーである場合は、

そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

DefenseEvasion:Kubernetes/MaliciousIPCaller

防御対策を回避するために一般的に使用される API が、悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが悪意のある既知のアクティビティと関連した IP アドレスから呼び出されたことを知らせるものです。観察された API は一般に、攻撃者が検出を回避するためにアクションの隠ぺいを試みている防御回避戦術に関連付けられています。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが `system:anonymous` である場合は、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消すことを許可された理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

防御対策を回避するために一般的に使用される API が、カスタム脅威リストにある IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが、アップロード済みの脅威リストに含まれている IP アドレスから呼び出されたことを知らせるものです。この検出結果に関連する脅威リストは、検出結果の詳細の [Additional Information] (追加情報) セクションにリストされています。観察された API は一般に、攻撃者が検出を回避するためにアクションの隠ぺいを試みている防御回避戦術に関連付けられています。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが `system:anonymous` である場合は、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API を呼び出すことを許可された理由を調べ、必要に応じてアクセス許可を取り消します。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

防御対策を回避するために一般的に使用される API が、認証されていないユーザーによって呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが `system:anonymous` ユーザーによって正常に呼び出されたことを知らせるものです。`system:anonymous` によって実行された API コールは認証されていません。観察された API は一般に、攻撃者が検出を回避するためにアクションの隠ぺいを試みている防御回避戦術に関連付けられています。このアクティビティは、検出結果で報告された API アクションで匿名アクセスまたは非認証アクセスが許可され、他のアクションで許可される可能性があることを示します。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります。

修復のレコメンデーション

クラスター上の `system:anonymous` ユーザーに付与されている許可を調べて、すべての許可が必要であることを確認する必要があります。誤って、または悪意を持って許可が付与された場合は、

ユーザーのアクセスを取り消し、クラスターに対して攻撃者が加えた変更を元に戻す必要があります。詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS 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。

詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

DefenseEvasion:Kubernetes/TorIPCaller

防御対策を回避するために一般的に使用される API が、Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API が Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。観察された API は一般に、攻撃者が検出を回避するためにアクションの隠ぺいを試みている防御回避戦術に関連付けられています。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、攻撃者が真のアイデンティティを隠す意図を持った、Kubernetes クラスターへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

`KubernetesUserDetails` セクションの結果で報告されたユーザーが `system:anonymous` である場合は、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消すことを許可された理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Discovery:Kubernetes/MaliciousIPCaller

Kubernetes クラスター内のリソースを見つけるために一般的に使用される API が、ある IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが悪意のある既知のアクティビティと関連した IP アドレスから呼び出されたことを知らせるものです。観察される API は、攻撃の検出段階で一般的に使用されます。攻撃者は、情報を収集して、Kubernetes クラスターがより広範な攻撃の影響を受けやすいかどうかを判断します。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが である場合は`system:anonymous`、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しとアクセス許可の取り消しを許可された理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Discovery:Kubernetes/MaliciousIPCaller.Custom

Kubernetes クラスターのリソースを見つけるために一般的に使用される API が、カスタム脅威リストにある IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、API が、アップロード済みの脅威リストに含まれている IP アドレスから呼び出されたことを知らせるものです。この検出結果に関連する脅威リストは、検出結果の詳細の [Additional Information] (追加情報) セクションにリストされています。観察される API は、攻撃の検出段階で一般的に使用されます。攻撃者は、情報を収集して、Kubernetes クラスターがより広範な攻撃の影響を受けやすいかどうかを判断します。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが である場合は`system:anonymous`、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しとアクセス許可の取り消しを許可

された理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Discovery:Kubernetes/SuccessfulAnonymousAccess

Kubernetes クラスターのリソースを見つけるために一般的に使用される API が、認証されていないユーザーによって呼び出されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが `system:anonymous` ユーザーによって正常に呼び出されたことを知らせるものです。`system:anonymous` によって実行された API コールは認証されていません。攻撃者が Kubernetes クラスターで情報を収集しているときに観測された API は、攻撃の検出段階に一般的に関連しています。このアクティビティは、検出結果で報告された API アクションで匿名アクセスまたは非認証アクセスが許可され、他のアクションで許可される可能性があることを示します。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります。

修復のレコメンデーション

クラスター上の `system:anonymous` ユーザーに付与されている許可を調べて、すべての許可が必要であることを確認する必要があります。誤って、または悪意を持って許可が付与された場合は、ユーザーのアクセスを取り消し、クラスターに対して攻撃者が加えた変更を元に戻す必要があります。詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS 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。

詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Discovery:Kubernetes/TorIPCaller

Kubernetes クラスターのリソースを見つけるために一般的に使用される API が、Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、API が Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。観察される API は、攻撃の検出段階で一般的に使用されます。攻撃者は、情報を収集して、Kubernetes クラスターがより広範な攻撃の影響を受けやすいかどうかを判断します。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、攻撃者が真のアイデンティティを隠す意図を持った、Kubernetes クラスターへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが `system:anonymous` である場合は、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが APIand の呼び出しを許可され、必要に応じてアクセス許可を取り消す理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Execution:Kubernetes/ExecInKubeSystemPod

`kube-system` 名前空間内のポッド内でコマンドが実行されました

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、コマンドが `kube-system` 名前空間内のポッドで Kubernetes exec API を使用して実行されたことを示すものです。`kube-system` 名前空間はデフォルトの名前空間であり、主に `kube-dns` や `kube-proxy` などのシステムレベルのコンポーネントに使用されます。`kube-system` 名前空間のポッドまたはコンテナ内でコマンドを実行することは非常にまれであり、疑わしいアクティビティを示している可能性があります。

修復のレコメンデーション

このコマンドの実行が想定されていない場合は、コマンドの実行に使用されたユーザーアイデンティティの認証情報が侵害される可能性があります。ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Impact:Kubernetes/MaliciousIPCaller

Kubernetes クラスターのリソースを改ざんするために一般的に使用される API が、悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが悪意のある既知のアクティビティと関連した IP アドレスから呼び出されたことを知らせるものです。観測された API は、攻撃者が AWS 環境内のデータを操作、中断、または破壊しようとしている影響戦術に一般的に関連しています。

修復のレコメンデーション

`KubernetesUserDetails` セクションの結果で報告されたユーザーが `system:anonymous` である場合は、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消した理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Impact:Kubernetes/MaliciousIPCaller.Custom

Kubernetes クラスターのリソースを改ざんするために一般的に使用される API が、カスタム脅威リストにある IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが、アップロード済みの脅威リストに含まれている IP アドレスから呼び出されたことを知らせるものです。この検出結果に関連する脅威リストは、検出結果の詳細の [Additional Information] (追加情報) セクションにリストされています。観測された API は、攻撃者が AWS 環境内のデータを操作、中断、または破壊しようとしている影響戦術に一般的に関連しています。

修復のレコメンデーション

`KubernetesUserDetails` セクションの結果で報告されたユーザーが `system:anonymous` である場合は、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消した理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Impact:Kubernetes/SuccessfulAnonymousAccess

Kubernetes クラスターのリソースを改ざんするために一般的に使用される API が、認証されていないユーザーによって呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが `system:anonymous` ユーザーによって正常に呼び出されたことを知らせるものです。`system:anonymous` によって実行された API コールは認証されていません。観測された API は、攻撃者がクラスターのリソースを改ざんしているときの攻撃の影響段階に一般的に関連しています。このアクティビティは、検出結果で報告された API アクションで匿名アクセスまたは非認証アクセスが許可され、他のアクションで許可される可能性があることを示します。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります。

修復のレコメンデーション

クラスター上の `system:anonymous` ユーザーに付与されている許可を調べて、すべての許可が必要であることを確認する必要があります。誤って、または悪意を持って許可が付与された場合は、

ユーザーのアクセスを取り消し、クラスターに対して攻撃者が加えた変更を元に戻す必要があります。詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS 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。

詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Impact:Kubernetes/TorIPCaller

Kubernetes クラスターのリソースを改ざんするために一般的に使用される API が、Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API が Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。観測された API は、インパクト戦術に一般的に関連していて、ここでは攻撃者が AWS 環境内部でデータを操作、割り込み、または破壊しようとしています。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、攻撃者が真のアイデンティティを隠す意図を持った、Kubernetes クラスターへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

`KubernetesUserDetails` セクションの検出結果で報告されたユーザーが である場合は`system:anonymous`、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消すことを許可された理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Persistence:Kubernetes/ContainerWithSensitiveMount

機密性の高い外部ホストパスが内部でマウントされた状態でコンテナが起動されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、volumeMounts セクションに書き込みアクセス権を持つ機密ホストパスを含む設定でコンテナが起動されたことを知らせるものです。これにより、機密性の高いホストパスがコンテナ内からアクセスおよび書き込み可能になります。この手法は、攻撃者がホストのファイルシステムにアクセスするために一般的に使用されます。

修復のレコメンデーション

このコンテナの起動が想定されていない場合、コンテナの起動に使用されたユーザーアイデンティティの認証情報が侵害される可能性があります。ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

このコンテナの起動が想定されている場合は、resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix フィールドに基づくフィルター基準で構成される抑制ルールを使用することをお勧めします。フィルター基準では、imagePrefix フィールドは検出結果で指定された imagePrefix と同じである必要があります。抑制ルールの作成の詳細については、「Suppression rules」(抑制ルール) を参照してください。

Persistence:Kubernetes/MaliciousIPCaller

Kubernetes クラスターへの永続アクセスを取得するために一般的に使用される API が、悪意のある既知の IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが悪意のある既知のアクティビティと関連した IP アドレスから呼び出されたことを知らせるものです。観察される API は、攻撃者がユーザーの Kubernetes クラスターへのアクセス権を取得し、そのアクセスを維持しようとする永続化戦術に一般的に関連しています。

修復のレコメンデーション

KubernetesUserDetails セクションの結果で報告されたユーザーが である場合 はsystem:anonymous、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消した理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Persistence:Kubernetes/MaliciousIPCaller.Custom

Kubernetes クラスターへの永続アクセスを取得するために一般的に使用される API が、カスタム脅威リストにある IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが、アップロード済みの脅威リストに含まれている IP アドレスから呼び出されたことを知らせるものです。この検出結果に関連する脅威リストは、検出結果の詳細の [Additional Information] (追加情報) セクションにリストされています。観察される API は、攻撃者がユーザーの Kubernetes クラスターへのアクセス権を取得し、そのアクセスを維持しようとする永続化戦術に一般的に関連しています。

修復のレコメンデーション

KubernetesUserDetails セクションの結果で報告されたユーザーが である場合 はsystem:anonymous、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消した理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Persistence:Kubernetes/SuccessfulAnonymousAccess

Kubernetes クラスターへの高レベルの許可を取得するために一般的に使用される API が、認証されていないユーザーによって呼び出されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、API オペレーションが `system:anonymous` ユーザーによって正常に呼び出されたことを知らせるものです。`system:anonymous` によって実行された API コールは認証されていません。観察される API は、攻撃者がユーザーのクラスターへのアクセス権を取得し、そのアクセスを維持しようとする永続化戦術に一般的に関連しています。このアクティビティは、検出結果で報告された API アクションで匿名アクセスまたは非認証アクセスが許可され、他のアクションで許可される可能性があることを示します。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります。

修復のレコメンデーション

クラスター上の `system:anonymous` ユーザーに付与されている許可を調べて、すべての許可が必要であることを確認する必要があります。誤って、または悪意を持って許可が付与された場合は、ユーザーのアクセスを取り消し、クラスターに対して攻撃者が加えた変更を元に戻す必要があります。詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS 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。

詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Persistence:Kubernetes/TorIPCaller

Kubernetes クラスターへの永続アクセスを取得するために一般的に使用される API が、Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、API が Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。観察される API は、攻撃者がユーザーの Kubernetes クラスターへのアクセス権を取得し、そのアク

セスを維持しようとする永続化戦術に一般的に関連しています。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、攻撃者の真のアイデンティティを隠す目的で、 AWS リソースへの不正アクセスを示している可能性があります。

修復のレコメンデーション

`KubernetesUserDetails` セクションの結果で報告されたユーザーが である場合は`system:anonymous`、Amazon EKS ユーザーガイドの「Amazon EKS のセキュリティのベストプラクティス」の指示に従って、匿名ユーザーが API の呼び出しを許可され、必要に応じてアクセス許可を取り消した理由を調べます。ユーザーが認証されたユーザーである場合は、そのアクティビティが正当なものであるのか、または悪意のあるものであるのかを調査します。アクティビティが悪意のあるものである場合は、ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

デフォルトのサービスアカウントには、Kubernetes クラスターに対する管理者権限が付与されています。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、Kubernetes クラスター内の名前空間のデフォルトのサービスアカウントに管理者権限が付与されたことを知らせるものです。Kubernetes は、クラスター内のすべての名前空間のためにデフォルトのサービスアカウントを作成します。別のサービスアカウントに明示的に関連付けられていないポッドに、デフォルトのサービスアカウントをアイデンティティとして自動的に割り当てます。デフォルトのサービスアカウントに管理者権限がある場合、ポッドが誤って管理者権限で起動される可能性があります。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります。

修復のレコメンデーション

ポッドに許可を付与するためにデフォルトのサービスアカウントを使用しないでください。代わりに、ワークロードごとに専用のサービスアカウントを作成し、必要に応じてそのアカウントに許可を付与する必要があります。この問題を解決するには、すべてのポッドとワークロードの専用サービス

アカウントを作成し、ポッドとワークロードを更新して、デフォルトのサービスアカウントから専用アカウントに移行する必要があります。その後、デフォルトのサービスアカウントから管理者許可を削除する必要があります。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Policy:Kubernetes/AnonymousAccessGranted

system:anonymous ユーザーには、Kubernetes クラスターに対する API 許可が付与されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、Kubernetes クラスター上のユーザーが、ユーザー `system:anonymous` をロールにバインドするために `ClusterRoleBinding` または `RoleBinding` を正常に作成したことを知らせるものです。これにより、ロールで許可された API オペレーションへの認証されていないアクセスを有効にします。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります

修復のレコメンデーション

クラスター上の `system:anonymous` ユーザーまたは `system:unauthenticated` グループに付与されている許可を調べて、不要な匿名アクセスを取り消す必要があります。詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS 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。悪意を持って許可が付与された場合は、その許可を付与したユーザーのアクセスを取り消し、クラスターに対して攻撃者が加えた変更を元に戻す必要があります。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Policy:Kubernetes/ExposedDashboard

Kubernetes クラスターのダッシュボードがインターネットに公開されました

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、クラスターの Kubernetes ダッシュボードがロードバランサーサービスによってインターネットに公開されたことを知らせるものです。ダッシュボードが公開されると、クラスターの管理インターフェイスがインターネットからアクセス可能になり、攻撃者は認証およびアクセスコントロールの存在する可能性のあるギャップを悪用できます。

修復のレコメンデーション

Kubernetes ダッシュボードで強力な認証および認可が強制されているようにする必要があります。また、ネットワークアクセスコントロールを実装して、特定の IP アドレスからダッシュボードへのアクセスを制限する必要があります。

詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Policy:Kubernetes/KubeflowDashboardExposed

Kubernetes クラスターの Kubeflow ダッシュボードがインターネットに公開されました

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、クラスターの Kubeflow ダッシュボードがロードバランサーサービスによってインターネットに公開されたことを知らせるものです。Kubeflow ダッシュボードが公開されると、Kubeflow 環境の管理インターフェイスがインターネットからアクセス可能になり、攻撃者は認証およびアクセスコントロールの存在する可能性のあるギャップを悪用できます。

修復のレコメンデーション

Kubeflow ダッシュボードで強力な認証および認可が強制されているようにする必要があります。また、ネットワークアクセスコントロールを実装して、特定の IP アドレスからダッシュボードへのアクセスを制限する必要があります。

詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

PrivilegeEscalation:Kubernetes/PrivilegedContainer

ルートレベルのアクセス権を持つ特権コンテナが Kubernetes クラスターで起動されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、特権コンテナが、クラスター内の特権コンテナを起動するためにこれまで使用されたことのないイメージを使用して Kubernetes クラスターで起動されたことを知らせるものです。特権コンテナには、ホストへのルートレベルのアクセス権があります。攻撃者は、特権のエスカレーション戦術として特権コンテナを起動して、ホストにアクセスして侵害することができます。

修復のレコメンデーション

このコンテナの起動が想定されていない場合、コンテナの起動に使用されたユーザーアイデンティティの認証情報が侵害される可能性があります。ユーザーのアクセスを取り消し、攻撃者がクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

一般的にシークレットへのアクセスに使用される Kubernetes API が、異常な方法で呼び出されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、機密のクラスターシークレットを取得する異常な API オペレーションが、クラスター内の Kubernetes ユーザーによって呼び出されたことを知らせるものです。観察された API は一般的に、認証情報アクセス戦略と関連付けられ、特権エスカレーションやクラスター内でさらにアクセスされる可能性があります。この動作が予期されない場合は、設定ミスまたは AWS 認証情報が侵害されている可能性があります。

観察された API は、異常検出機械学習 (ML) GuardDuty モデルによって異常として識別されました。ML モデルは、EKS クラスター内のユーザー API アクティビティをすべて評価し、権限のないユーザーによって使用されたテクニックに関連する異常なイベントを特定します。ML モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用ユーザーエージェント、ユーザーが操作した名前空間など、API 操作の複数の要因を追跡します。異常な API リクエストの詳細は、GuardDuty コンソールの検出結果の詳細パネルで確認できます。

修復のレコメンデーション

クラスターの Kubernetes ユーザーに付与された許可を調べて、すべての許可が必要であることを確認してください。誤って、または悪意を持って許可が付与された場合は、ユーザーのアクセスを取り消し、クラスターに対し認証されていないユーザーが加えたすべての変更を元に戻してください。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

AWS 認証情報が侵害されている場合は、「」を参照してください侵害された可能性のある AWS 認証情報の修正。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Kubernetes クラスターで過度に許可されたロールまたは機密性の高い名前空間 ClusterRoleBinding に対する RoleBinding または が作成または変更されました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、 または に RoleBinding または ClusterRoleBinding が含まれる ClusterRoles `admin`場合`cluster-admin`、重要度は High になります。

- 機能: EKS 監査ログ

この検出結果は、Kubernetes クラスター内のユーザーが、`RoleBinding` または `ClusterRoleBinding` を作成して、管理者権限または機密性の高い名前空間を持つロールにユーザーをバインドしたことを知らせるものです。この動作が想定されていない場合は、設定ミスまたは AWS 認証情報が侵害されている可能性があります。

観察された API は、異常検出機械学習 (ML) GuardDuty モデルによって異常として識別されました。ML モデルは EKS クラスター内のすべてのユーザー API アクティビティを評価します。この ML モデルは、権限のないユーザーが使用したテクニックに関連する異常なイベントも特定します。また、ML モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用ユーザーエージェント、ユーザーが操作した名前空間など、API 操作の複数の要因を追跡します。異常な API リクエストの詳細は、 GuardDuty コンソールの検出結果の詳細パネルで確認できます。

修復のレコメンデーション

Kubernetes ユーザーに付与された権限を確認してください。これらの権限は、RoleBinding および ClusterRoleBinding に関係するロールとサブジェクトで定義されます。誤って、または悪意を持って許可が付与された場合は、ユーザーのアクセスを取り消し、クラスターに対し認証されていないユーザーが加えたすべての変更を元に戻してください。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

AWS 認証情報が侵害されている場合は、「」を参照してください侵害された可能性のある AWS 認証情報の修正。

Execution:Kubernetes/AnomalousBehavior.ExecInPod

ポッド内で異常な方法によるコマンドが実行されました。

デフォルトの重要度: [Medium] (中)

- 機能: EKS 監査ログ

この検出結果は、Kubernetes exec API を使用してポッド内でコマンドが実行されたことを知らせるものです。Kubernetes exec API を使用すると、ポッド内で任意のコマンドを実行できます。この動作がユーザー、名前空間、またはポッドで想定されていない場合は、設定ミスまたは AWS 認証情報が侵害されている可能性があります。

観察された API は、異常検出機械学習 (ML) GuardDuty モデルによって異常として識別されました。ML モデルは EKS クラスター内のすべてのユーザー API アクティビティを評価します。この ML モデルは、権限のないユーザーが使用したテクニックに関連する異常なイベントも特定します。また、ML モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用ユーザーエージェント、ユーザーが操作した名前空間など、API 操作の複数の要因を追跡します。異常な API リクエストの詳細は、 GuardDuty コンソールの検出結果の詳細パネルで確認できます。

修復のレコメンデーション

このコマンドの実行が想定されていない場合は、コマンドの実行に使用されたユーザーアイデンティティの認証情報が侵害されている可能性があります。ユーザーのアクセスを取り消し、認証されていないユーザーがクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

AWS 認証情報が侵害されている場合は、「」を参照してください侵害された可能性のある AWS 認証情報の修正。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

ワークロードが特権コンテナを使用して異常な方法で起動されました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果は、ワークロードが Amazon EKS クラスター内の特権コンテナを使用して起動されたこと知らせるものです。特権コンテナには、ホストへのルートレベルのアクセス権があります。認証されていないユーザーは、特権のエスカレーション戦術として特権コンテナを起動して、ホストに最初にアクセスして侵害することができます。

観察されたコンテナの作成または変更は、異常検出機械学習 (ML) モデルによって GuardDuty 異常として識別されました。ML モデルは EKS クラスター内のすべてのユーザー API およびコンテナイメージアクティビティを評価します。この ML モデルは、権限のないユーザーが使用したテクニックに関連する異常なイベントも特定します。また、ML モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用ユーザーエージェント、アカウントで観察されたコンテナイメージ、ユーザーが操作した名前空間など、API 操作の複数の要因を追跡します。異常な API リクエストの詳細は、 GuardDuty コンソールの検出結果の詳細パネルで確認できます。

修復のレコメンデーション

このコンテナの起動が想定されていない場合、コンテナの起動に使用されたユーザーアイデンティティの認証情報が侵害されている可能性があります。ユーザーのアクセスを取り消し、認証されていないユーザーがクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

AWS 認証情報が侵害されている場合は、「」を参照してください侵害された可能性のある AWS 認証情報の修正。

このコンテナの起動が想定されている場合は、`resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` フィールドに基づくフィルター基準を使用した抑制ルールを使用することをお勧めします。フィルター基準では、`imagePrefix` フィールドの値が検出結果で指定した `imagePrefix` フィールドの値と同じである必要があります。詳細については、「抑制ルール」を参照してください。

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount

ワークロードが異常な方法でデプロイされ、機密性の高いホストパスがワークロード内でマウントされました。

デフォルトの重要度: [High] (高)

- 機能: EKS 監査ログ

この検出結果により、volumeMounts セクションに機密ホストパスを含むコンテナを使用してワークロードが起動されたことが分かります。これにより、機密性の高いホストパスがコンテナ内からアクセスおよび書き込み可能となる場合があります。この手法は、認証されていないユーザーがホストのファイルシステムにアクセスするために一般的に使用されます。

観察されたコンテナの作成または変更は、異常検出機械学習 (ML) モデルによって GuardDuty 異常として識別されました。ML モデルは EKS クラスター内のすべてのユーザー API およびコンテナイメージアクティビティを評価します。この ML モデルは、権限のないユーザーが使用したテクニックに関連する異常なイベントも特定します。また、ML モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用ユーザーエージェント、アカウントで観察されたコンテナイメージ、ユーザーが操作した名前空間など、API 操作の複数の要因を追跡します。異常な API リクエストの詳細は、 GuardDuty コンソールの検出結果の詳細パネルで確認できます。

修復のレコメンデーション

このコンテナの起動が想定されていない場合、コンテナの起動に使用されたユーザーアイデンティティの認証情報が侵害されている可能性があります。ユーザーのアクセスを取り消し、認証されていないユーザーがクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

AWS 認証情報が侵害されている場合は、「」を参照してください侵害された可能性のある AWS 認証情報の修正。

このコンテナの起動が想定されている場合は、resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix フィールドに基づくフィルター基準を使用した抑制ルールを使用することをお勧めします。フィルター基準では、imagePrefix フィールドの値が検出結果で指定した imagePrefix フィールドの値と同じである必要があります。詳細については、「抑制ルール」を参照してください。

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

ワークロードが異常な方法で起動されました。

デフォルトの重要度: [Low] (低)*

> **Note**
>
> デフォルトの重大度は [Low] (低) です。ただし、ワークロードに疑わしいイメージ名 (既知のペンテストツールなど)や、起動時に疑わしいコマンドを実行しているコンテナ (リバースシェルコマンドなど) が含まれている場合、この検出結果タイプの重要度は [Midium] (中) と見なされます。

- 機能: EKS 監査ログ

この検出結果は、Kubernetes ワークロードが Amazon EKS クラスター内で、API アクティビティ、新しいコンテナイメージ、危険なワークロード設定などの異常な方法で作成または変更されたこと知らせるものです。承認されていないユーザーは、任意のコードを実行する手法としてコンテナを起動し、最初にホストにアクセスして、侵害する可能性があります。

観察されたコンテナの作成または変更は、異常検出機械学習 (ML) モデルによって GuardDuty 異常として識別されました。ML モデルは EKS クラスター内のすべてのユーザー API およびコンテナイメージアクティビティを評価します。この ML モデルは、権限のないユーザーが使用したテクニックに関連する異常なイベントも特定します。また、ML モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用ユーザーエージェント、アカウントで観察されたコンテナイメージ、ユーザーが操作した名前空間など、API 操作の複数の要因を追跡します。異常な API リクエストの詳細は、 GuardDuty コンソールの検出結果の詳細パネルで確認できます。

修復のレコメンデーション

このコンテナの起動が想定されていない場合、コンテナの起動に使用されたユーザーアイデンティティの認証情報が侵害されている可能性があります。ユーザーのアクセスを取り消し、認証されていないユーザーがクラスターに加えた変更を元に戻します。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

AWS 認証情報が侵害されている場合は、「」を参照してください侵害された可能性のある AWS 認証情報の修正。

このコンテナの起動が想定されている場合は、`resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` フィールドに基づくフィルター基準を使用した抑制ルールを使用することをお勧めします。フィルター基準では、`imagePrefix` フィールドの値が検出結果で指定した `imagePrefix` フィールドの値と同じである必要があります。詳細については、「抑制ルール」を参照してください。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

許可の高いロール または が異常な方法で作成または変更 ClusterRole されました。

デフォルトの重要度: [Low] (低)

- 機能: EKS 監査ログ

この検出結果は、過剰な権限を使用した `Role` または `ClusterRole` を作成する異常な API オペレーションが、Amazon EKS クラスター内の Kubernetes ユーザーによって呼び出されたこと知らせるものです。アクターは、強力な権限を持つロール作成を利用することで、組み込み型の管理者に似せたロールの使用を避け、検出を回避する可能性があります。過剰な権限により、権限エスカレーションやリモートコードが実行され、名前空間やクラスターが制御される可能性があります。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります。

観察された API は、異常検出機械学習 (ML) GuardDuty モデルによって異常として識別されました。ML モデルは、Amazon EKS クラスター内のユーザー API アクティビティをすべて評価し、権限のないユーザーによって使用された手法に関連する異常なイベントを特定します。また、ML モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用ユーザーエージェント、アカウントで観察されたコンテナイメージ、ユーザーが操作した名前空間など、API 操作の複数の要因を追跡します。異常な API リクエストの詳細は、 GuardDuty コンソールの検出結果の詳細パネルで確認できます。

修復のレコメンデーション

`Role` または `ClusterRole` で定義されている権限を調べ、すべての権限が必要であることを確認し、最小特権の原則に従ってください。誤って、または悪意を持って許可が付与された場合は、ユーザーのアクセスを取り消し、クラスターに対し認証されていないユーザーが加えたすべての変更を元に戻してください。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

AWS 認証情報が侵害されている場合は、「」を参照してください侵害された可能性のある AWS 認証情報の修正。

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

ユーザーが異常な方法でアクセス許可を確認しました。

デフォルトの重要度: [Low] (低)

- 機能: EKS 監査ログ

この検出結果は、Kubernetes クラスター内のユーザーが、特権エスカレーションやリモートコード実行につながる可能性がある既知の強力な権限が許可されているかどうかの確認に成功したこと知らせるものです。例えば、ユーザーの権限を確認するのに使用される一般的なコマンドは、`kubectl auth can-i` です。この動作が想定されていない場合は、設定ミスがあるか、または認証情報が侵害されている可能性があります。

観察された API は、異常検出機械学習 (ML) GuardDuty モデルによって異常として識別されました。ML モデルは、Amazon EKS クラスター内のユーザー API アクティビティをすべて評価し、権限のないユーザーによって使用された手法に関連する異常なイベントを特定します。また、ML モデルは、リクエストを行ったユーザー、リクエストが行われた場所、確認された許可、ユーザーが操作した名前空間など、API 操作の複数の要因を追跡します。異常な API リクエストの詳細は、GuardDuty コンソールの検出結果の詳細パネルで確認できます。

修復のレコメンデーション

Kubernetes ユーザーに付与された権限を調べて、すべての権限が必要であることを確認してください。誤って、または悪意を持って許可が付与された場合は、ユーザーのアクセスを取り消し、クラスターに対し認証されていないユーザーが加えたすべての変更を元に戻してください。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

AWS 認証情報が侵害されている場合は、「」を参照してください侵害された可能性のある AWS 認証情報の修正。

Lambda Protection の検出結果タイプ

このセクションでは、AWS Lambda リソースに固有であり、`Lambda` としてリストされている `resourceType` を持つ検出結果タイプについて説明します。すべての Lambda の検出結果につい

て、問題のリソースを調べて正常に動作しているかどうかを確認することをお勧めします。アクティビティが認可されると、そのリソースに対する誤検出の通知を防ぐため、抑制ルールや信頼できる IP および脅威リストを使用できます。

アクティビティが予想されていなかった場合、セキュリティのベストプラクティスは、Lambda が侵害されている可能性があると想定し、修復のレコメンデーションに従うことです。

トピック

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Lambda 関数は、既知のコマンドとコントロールサーバーに関連付けられる IP アドレスをクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Lambda Network Activity Monitoring

この検出結果は、AWS 環境のリスト化した Lambda 関数が既知のコマンドとコントロール (C&C) サーバーに関連付けられた IP アドレスをクエリしていることを知らせるものです。生成された検出結果に関連する Lambda 関数が危険にさらされている可能性があります。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータです。

ボットネットとは、一般的なタイプのマルウェアに感染しコントロールされたインターネットコネクテッドデバイス (PC、サーバー、モバイルデバイス、IoT デバイスなど) のコレクションです。通常、ボットネットは、マルウェアの配布や盗用された情報 (クレジットカード番号など) の収集に使用されます。ボットネットの目的と構造によっては、C&C サーバーから分散型サービス拒否を開始するためのコマンドが発行されることもあります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、Lambda 関数は侵害されている可能性があります。詳細については、「侵害された可能性のある Lambda 関数の修復」を参照してください。

CryptoCurrency:Lambda/BitcoinTool.B

Lambda 関数が暗号通貨関連のアクティビティに関連付けられている IP アドレスをクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Lambda Network Activity Monitoring

この検出結果は、AWS 環境のリスト化した Lambda 関数でビットコインやその他の暗号通貨関連アクティビティに紐づけられた IP アドレスがクエリされていることを知らせるものです。脅威アクターは、Lambda 関数を不正な暗号通貨マイニングに不正に転用するために、Lambda 関数を乗っ取ろうとしている可能性があります。

修復のレコメンデーション

この Lambda 関数を使用して暗号通貨のマイニングまたは管理を行う場合、またはこの関数がブロックチェーンアクティビティに関与している場合は、環境で予期されるアクティビティである可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の検索条件では、[検出結果タイプ] 属性に CryptoCurrency:Lambda/BitcoinTool.B という値を使用します。2 つ目のフィルター条件は、ブロックチェーンアクティビティに関係する関数の Lambda 関数名である必要があります。抑制ルール作成の詳細については、「抑制ルール」を参照してください。

このアクティビティが予想されていなかった場合、Lambda 関数が侵害されている可能性があります。詳細については、「侵害された可能性のある Lambda 関数の修復」を参照してください。

Trojan:Lambda/BlackholeTraffic

Lambda 関数は、ブラックホールと呼ばれるリモートホストの IP アドレスに通信しようとしています。

デフォルトの重要度: [Medium] (中)

- 機能: Lambda Network Activity Monitoring

この検出結果は、AWS 環境のリスト化された Lambda 関数がブラックホール (あるいはシンクホール) の IP アドレスと通信しようとしていることを知らせるものです。ブラックホールとは、送受信トラフィックが密かに破棄されるネットワークの場所を指し、意図した受信者にデータが届いていないことは送信元に知らされません。ブラックホール IP アドレスは、稼働していないホストマシンやホストが割り当てられていないアドレスを指定します。記載されている Lambda 関数は侵害されている可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、Lambda 関数は侵害されている可能性があります。詳細については、「侵害された可能性のある Lambda 関数の修復」を参照してください。

Trojan:Lambda/DropPoint

Lambda 関数が、マルウェアによって収集された認証情報やその他の盗難されたデータを保持していることが認識されているリモートホストの IP アドレスに通信しようとしています。

デフォルトの重要度: [Medium] (中)

- 機能: Lambda Network Activity Monitoring

この検出結果は、AWS 環境でリストされた Lambda 関数で、マルウェアが取り込んだ認証情報やその他の盗難されたデータを保持して、リモートホストの IP アドレスに通信しようとしていることを知らせるものです。

修復のレコメンデーション

このアクティビティが予期しないものである場合、Lambda 関数は侵害されている可能性があります。詳細については、「侵害された可能性のある Lambda 関数の修復」を参照してください。

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Lambda 関数がカスタム脅威リストの IP アドレスに接続しています。

デフォルトの重要度: [Medium] (中)

- 機能: Lambda Network Activity Monitoring

この検出結果は、AWS 環境の Lambda 関数が、ユーザーがアップロードした脅威リストに含まれている IP アドレスを使用してアウトバウンド通信していることを知らせるものです。GuardDuty の場合、脅威リストは悪意のある既知の IP アドレスで構成されます。GuardDuty では、アップロード済みの脅威リストに基づいて検出結果を生成します。脅威リストの詳細は、GuardDuty コンソールの検出結果の詳細で確認できます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、Lambda 関数は侵害されている可能性があります。詳細については、「侵害された可能性のある Lambda 関数の修復」を参照してください。

UnauthorizedAccess:Lambda/TorClient

Lambda 関数は Tor Guard または Authority ノードに接続しています。

デフォルトの重要度: [High] (高)

- 機能: Lambda Network Activity Monitoring

この検出結果は、AWS 環境の Lambda 関数が Tor Guard または Authority ノードに接続中であることを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。Tor Guards および Authority ノードは、Tor ネットワークへの初期ゲートウェイとして動作します。このトラフィックは、この Lambda 関数が侵害されている可能性があることを示している可能性があります。現在は、Tor ネットワーク上のクライアントとして動作している場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、Lambda 関数は侵害されている可能性があります。詳細については、「侵害された可能性のある Lambda 関数の修復」を参照してください。

UnauthorizedAccess:Lambda/TorRelay

Lambda 関数は、Tor リレーとして Tor ネットワークに接続中です。

デフォルトの重要度: [High] (高)

- 機能: Lambda Network Activity Monitoring

この検出結果は、AWS 環境の Lambda 関数が Tor リレーとして動作していることを示す方法で、Tor ネットワークに接続中であることを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。Tor は、クライアントの不正な可能性のあるトラフィックをある Tor リレーから別の Tor リレーに転送することにより、通信の匿名性を高めます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、Lambda 関数は侵害されている可能性があります。詳細については、「侵害された可能性のある Lambda 関数の修復」を参照してください。

EC2 検出結果タイプの Malware Protection

GuardDuty Malware Protection for EC2 は、EC2 インスタンスまたはコンテナワークロードのスキャン中に検出されたすべての脅威に対して、単一の Malware Protection for EC2 の検出結果を提供します。この検出結果には、スキャン中に行われた検出の合計数が含まれ、重要度に基づいて、検出された上位 32 個の脅威の詳細が示されます。他の GuardDuty 検出結果とは異なり、同じ EC2 インスタンスまたはコンテナワークロードを再度スキャンしても、EC2 の検出結果に対する Malware Protection は更新されません。

マルウェアを検出するスキャンごとに、EC2 検出結果の新しい Malware Protection が生成されます。Malware Protection for EC2 の検出結果には、検出結果を生成した対応するスキャンに関する情報と GuardDuty、このスキャンを開始した検出結果が含まれます。これにより、疑わしい動作と検出されたマルウェアとの関連付けがより簡単になります。

> **Note**
>
> がコンテナワークロードに対する悪意のあるアクティビティ GuardDuty を検出すると、Malware Protection for EC2 は EC2 レベルの検出結果を生成しません。

以下の検出結果は、EC2 の GuardDuty Malware Protection に固有のものです。

トピック

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile
- Execution:Kubernetes/MaliciousFile
- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

悪意のあるファイルが EC2 インスタンスで検出されました。

デフォルトの重要度: 検出された脅威によって異なります。

- 機能: EBS Malware Protection

この検出結果は、 GuardDuty Malware Protection for EC2 スキャンが AWS 、環境内のリストされた EC2 インスタンスで 1 つ以上の悪意のあるファイルを検出したことを示しています。このリスト化したインスタンスは侵害されている可能性があります。詳細については、次を参照してください。検出結果の詳細にある「脅威の検出」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Execution:ECS/MaliciousFile

悪意のあるファイルが ECS クラスターで検出されました。

デフォルトの重要度: 検出された脅威によって異なります。

- 機能: EBS Malware Protection

この検出結果は、 GuardDuty Malware Protection for EC2 スキャンが、ECS クラスターに属するコンテナワークロードで 1 つ以上の悪意のあるファイルを検出したことを示しています。詳細については、次を参照してください。検出結果の詳細にある「脅威の検出」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、ECS クラスターに属するコンテナが侵害されている可能性があります。詳細については、「侵害された可能性のある ECS クラスターの修復」を参照してください。

Execution:Kubernetes/MaliciousFile

悪意のあるファイルが Kubernetes クラスターで検出されました。

デフォルトの重要度: 検出された脅威によって異なります。

- 機能: EBS Malware Protection

この検出結果は、 GuardDuty Malware Protection for EC2 スキャンが Kubernetes クラスターに属するコンテナワークロードで 1 つ以上の悪意のあるファイルを検出したことを示しています。これが EKS マネージドクラスターの場合、検出結果の詳細には、影響を受ける EKS リソースに関する追加情報が表示されます。詳細については、次を参照してください。検出結果の詳細にある「脅威の検出」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、コンテナのワークロードが侵害されている可能性があります。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Execution:Container/MaliciousFile

悪意のあるファイルがスタンドアロンコンテナで検出されました。

デフォルトの重要度: 検出された脅威によって異なります。

- 機能: EBS Malware Protection

この検出結果は、 GuardDuty Malware Protection for EC2 スキャンがコンテナワークロードで 1 つ以上の悪意のあるファイルを検出し、クラスター情報が特定されていないことを示しています。詳細については、次を参照してください。検出結果の詳細にある「脅威の検出」を参照してください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、コンテナのワークロードが侵害されている可能性があります。詳細については、「侵害された可能性のあるスタンドアロンコンテナの修復」を参照してください。

Execution:EC2/SuspiciousFile

EC2 インスタンスで疑わしいファイルが検出されました。

デフォルトの重要度: 検出された脅威によって異なります。

- 機能: EBS Malware Protection

この検出結果は、 GuardDuty Malware Protection for EC2 スキャンが EC2 インスタンスで 1 つ以上の疑わしいファイルを検出したことを示しています。詳細については、次を参照してください。検出結果の詳細にある「脅威の検出」を参照してください。

`SuspiciousFile` タイプの検出では、アドウェア、スパイウェア、デュアルユースツールなどの望ましくないであろうプログラムが、影響を受けるリソースに存在することが示されます。これらのプログラムは、リソースに悪影響を及ぼしたり、攻撃者が悪意のある目的で使用された可能性があります。例えば、ネットワークツールは、リソースを侵害しようとするハッキングツールとして、敵対者によって合法的または悪意を持って使用される可能性があります。

疑わしいファイルが検出されたら、検出されたファイルが AWS 環境で表示されるかどうかを評価します。ファイルが予期しないものである場合は、次のセクションで提供される修復の推奨事項に従ってください。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Execution:ECS/SuspiciousFile

疑わしいファイルが ECS クラスターで検出されました。

デフォルトの重要度: 検出された脅威によって異なります。

- 機能: EBS Malware Protection

この検出結果は、 GuardDuty Malware Protection for EC2 スキャンが ECS クラスターに属するコンテナで 1 つ以上の疑わしいファイルを検出したことを示しています。詳細については、次を参照してください。検出結果の詳細にある「脅威の検出」を参照してください。

`SuspiciousFile` タイプの検出では、アドウェア、スパイウェア、デュアルユースツールなどの望ましくないであろうプログラムが、影響を受けるリソースに存在することが示されます。これらのプログラムは、リソースに悪影響を及ぼしたり、攻撃者が悪意のある目的で使用された可能性があります。例えば、ネットワークツールは、リソースを侵害しようとするハッキングツールとして、敵対者によって合法的または悪意を持って使用される可能性があります。

疑わしいファイルが検出されたら、検出されたファイルが AWS 環境で表示されるかどうかを評価します。ファイルが予期しないものである場合は、次のセクションで提供される修復の推奨事項に従ってください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、ECS クラスターに属するコンテナが侵害されている可能性があります。詳細については、「侵害された可能性のある ECS クラスターの修復」を参照してください。

Execution:Kubernetes/SuspiciousFile

疑わしいファイルが Kubernetes クラスターで検出されました。

デフォルトの重要度: 検出された脅威によって異なります。

- 機能: EBS Malware Protection

この検出結果は、 GuardDuty Malware Protection for EC2 スキャンが Kubernetes クラスターに属するコンテナで 1 つ以上の疑わしいファイルを検出したことを示しています。これが EKS マネージド

クラスターの場合、検出結果の詳細には、影響を受ける EKS に関する追加情報が表示されます。詳細については、次を参照してください。検出結果の詳細にある「脅威の検出」を参照してください。

SuspiciousFile タイプの検出では、アドウェア、スパイウェア、デュアルユースツールなどの望ましくないであろうプログラムが、影響を受けるリソースに存在することが示されます。これらのプログラムは、リソースに悪影響を及ぼしたり、攻撃者が悪意のある目的で使用された可能性があります。例えば、ネットワークツールは、リソースを侵害しようとするハッキングツールとして、敵対者によって合法的または悪意を持って使用される可能性があります。

疑わしいファイルが検出されたら、検出されたファイルが AWS 環境で表示されるかどうかを評価します。ファイルが予期しないものである場合は、次のセクションで提供される修復の推奨事項に従ってください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、コンテナのワークロードが侵害されている可能性があります。詳細については、「EKS 監査ログのモニタリング検出結果の修正」を参照してください。

Execution:Container/SuspiciousFile

疑わしいファイルがスタンドアロンコンテナで検出されました。

デフォルトの重要度: 検出された脅威によって異なります。

- 機能: EBS Malware Protection

この検出結果は、EC2 スキャンの GuardDuty Malware Protection が、クラスター情報のないコンテナで 1 つ以上の疑わしいファイルを検出したことを示しています。詳細については、次を参照してください。検出結果の詳細にある「脅威の検出」を参照してください。

SuspiciousFile タイプの検出では、アドウェア、スパイウェア、デュアルユースツールなどの望ましくないであろうプログラムが、影響を受けるリソースに存在することが示されます。これらのプログラムは、リソースに悪影響を及ぼしたり、攻撃者が悪意のある目的で使用された可能性があります。例えば、ネットワークツールは、リソースを侵害しようとするハッキングツールとして、敵対者によって合法的または悪意を持って使用される可能性があります。

疑わしいファイルが検出されたら、検出されたファイルが AWS 環境で表示されるかどうかを評価します。ファイルが予期しないものである場合は、次のセクションで提供される修復の推奨事項に従ってください。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、コンテナのワークロードが侵害されている可能性があります。詳細については、「侵害された可能性のあるスタンドアロンコンテナの修復」を参照してください。

S3 検出結果タイプの Malware Protection

GuardDuty は、 で潜在的なセキュリティ脅威を検出した場合にのみ検出結果を生成します AWS アカウント。Malware Protection for S3 の検出結果は、マルウェアスキャンを開始したアップロードされたオブジェクトに、悪意のある可能性があるファイルが含まれていることを示します。

Amazon が で結果を生成する GuardDuty には AWS アカウント、 GuardDuty と Malware Protection for S3 の両方を有効にします。ベストプラクティスは、まず を有効に GuardDuty してから、S3 の Malware Protection を有効にすることです。この順序が異なる場合は、S3 オブジェクトが保護されたバケットにアップロードされる GuardDuty 前に、必ず を有効にしてください。

> **Note**
>
> GuardDuty は、 を有効にする前にスキャンされた S3 オブジェクトの結果を生成できません GuardDuty。既存の S3 オブジェクトをスキャンするには、再度アップロードします。

Object:S3/MaliciousFile

スキャンされた S3 オブジェクトで悪意のあるファイルが検出されました。

デフォルトの重要度: [High] (高)

- 機能: Malware Protection for S3

この検出結果は、マルウェアスキャンがリストされた S3 オブジェクトを悪意のあるものとして検出したことを示しています。詳細については、検出結果の詳細パネルの「脅威の検出」セクションを参照してください。

推奨事項の修正：

この検出結果が予期しないものである場合、S3 オブジェクトは悪意のある可能性があります。推奨される修復手順については、「」を参照してください悪意のある可能性のある S3 オブジェクトの修復。

GuardDuty RDS Protection の検出結果タイプ

GuardDuty RDS Protection は、データベースインスタンスでの異常なログイン動作を検出します。以下の検出結果は サポートされている Amazon Aurora および Amazon RDS データベース 固有のものであり、リソースタイプは `RDSDBInstance` です。結果の重大度と詳細は、結果タイプによって異なります。

トピック

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

ユーザーがアカウント内の RDS データベースへのログインに、異常な方法で成功しました。

デフォルトの重要度: 可変

> **Note**
>
> この検出結果に関連する異常な動作に応じて、デフォルトの重要度は「低」、「中」、「高」になります。
>
> - 低 - この検出結果に関連するユーザー名が、プライベートネットワークに関連付けられた IP アドレスからログインした場合。

- 中 - この検出結果に関連するユーザー名がパブリック IP アドレスからログインした場合。
- 高 - パブリック IP アドレスからのログイン試行の失敗が一貫して続いている場合は、アクセスポリシーが過度に制限されていることを示します。

- 機能: RDS ログインアクティビティのモニタリング

この検出結果は、AWS 環境の RDS データベースで異常なログインの成功が観察されたことを通知するものです。これは、以前に見たことのないユーザーが RDS データベースに初めてログインしたことを示している可能性があります。一般的なシナリオは、個々のユーザーではなくアプリケーションがプログラム的にアクセスするデータベースに内部ユーザーがログインする場合です。

このログイン成功は、GuardDuty の異常検出機械学習 (ML) モデルにより、異常として識別されています。機械学習モデルは、サポートされている Amazon Aurora および Amazon RDS データベース内のすべてのデータベースログインイベントを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用された特定のデータベース接続の詳細など、RDS ログインアクティビティのさまざまな要因を追跡します。潜在的に異常なログインイベントについては、「RDS ログインアクティビティベースの異常」を参照してください。

修復のレコメンデーション

関連付けられたデータベースに対するこのアクティビティが想定外の場合は、関連するデータベースユーザーのパスワードを変更し、利用可能な監査ログを確認することをお勧めします。中および高の重要度の検出結果は、データベースへのアクセスポリシーが過度に寛容であり、ユーザーの認証情報が漏洩または侵害された可能性があることを示している可能性があります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの成功により、侵害された可能性のあるデータベースの修復」を参照してください。

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

アカウント内の RDS データベースで、1 回以上の異常なログイン失敗が確認されました。

デフォルトの重要度: [Low] (低)

- 機能: RDS ログインアクティビティのモニタリング

この結果から、AWS 環境内の RDS データベースで 1 回以上の異常なログイン失敗が確認されたことがわかります。パブリック IP アドレスからのログインに失敗した場合は、アカウントの RDS データベースが、潜在的に悪意のある攻撃者によるブルートフォース攻撃の試みを受けている可能性があります。

この失敗したログインは、GuardDuty の異常検出機械学習 (ML) モデルにより、異常として識別されています。機械学習モデルは、サポートされている Amazon Aurora および Amazon RDS データベース 内のすべてのデータベースログインイベントを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用された特定のデータベース接続の詳細など、RDS ログインアクティビティのさまざまな要因を追跡します。潜在的に異常な RDS ログインアクティビティについては、「RDS ログインアクティビティベースの異常」を参照してください。

修復のレコメンデーション

関連付けられたデータベースに対するこのアクティビティが想定外の場合は、データベースが公開されているか、データベースのアクセスポリシーが過度に許容されている可能性があります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの失敗により、侵害された可能性のあるデータベースの修正」を参照してください。

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

通常とは異なるログイン試行を繰り返したユーザーが、パブリック IP アドレスからアカウントの RDS データベースに異常な方法でのログインに成功しました。

デフォルトの重要度: [High] (高)

- 機能: RDS ログインアクティビティのモニタリング

この検出結果は、ブルートフォースの成功を示す異常なログインが AWS 環境内の RDS データベースで観察されたことを示します。異常なログインの成功の前に、異常なログイン試行失敗の一貫したパターンが観察されました。これは、アカウント内の RDS データベースに関連付けられているユーザーとパスワードが侵害され、悪質な攻撃者によって RDS データベースにアクセスされた可能性があることを示しています。

このブルートフォースの成功は、GuardDuty の異常検出機械学習 (ML) モデルにより、異常として識別されています。機械学習モデルは、サポートされている Amazon Aurora および Amazon RDS データベース 内のすべてのデータベースログインイベントを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。機械学習モデルは、リクエストを行ったユーザー、リクエストが行われた場所、使用された特定のデータベース接続の詳細など、RDS ログインアクティビティのさまざまな要因を追跡します。潜在的に異常な RDS ログインアクティビティについては、「RDS ログインアクティビティベースの異常」を参照してください。

修復のレコメンデーション

このアクティビティは、データベースの認証情報が漏洩または侵害された可能性があることを示しています。関連するデータベースユーザーのパスワードを変更し、利用可能な監査ログを確認して、侵害された可能性のあるユーザーが行ったアクティビティを確認することをお勧めします。通常とは異なるログイン試行が繰り返される場合は、データベースへのアクセスポリシーが過度に寛容であるか、データベースが公開されている可能性があります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの成功により、侵害された可能性のあるデータベースの修復」を参照してください。

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

ユーザーが既知の悪意のある IP アドレスからアカウントの RDS データベースへのログインに成功しました。

デフォルトの重要度: [High] (高)

- 機能: RDS ログインアクティビティのモニタリング

この検出結果は、AWS 環境内の既知の悪意のあるアクティビティに関連付けられた IP アドレスから、成功した RDS ログインアクティビティが発生したことを示します。これは、アカウント内の RDS データベースに関連付けられているユーザーとパスワードが侵害され、悪質な攻撃者によって RDS データベースにアクセスされた可能性があることを示しています。

修復のレコメンデーション

関連付けられたデータベースに対するこのアクティビティが想定外の場合は、ユーザーの認証情報が公開されているか、侵害されている可能性があります。関連するデータベースユーザーのパスワードを変更し、利用可能な監査ログを確認して、侵害されたユーザーが行ったアクティビティを確認す

ることをお勧めします。このアクティビティは、データベースへのアクセスポリシーが過度に寛容であるか、データベースが公開されていることを示している可能性もあります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの成功により、侵害された可能性のあるデータベースの修復」を参照してください。

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

既知の悪意のあるアクティビティに関連する IP アドレスが、アカウントの RDS データベースへのログインに失敗しました。

デフォルトの重要度: [Medium] (中)

- 機能: RDS ログインアクティビティのモニタリング

この検出結果から、既知の悪意のあるアクティビティに関連する IP アドレスが AWS 環境内の RDS データベースにログインしようとしたが、正しいユーザー名またはパスワードを入力できなかったことがわかります。これは、潜在的に悪意のある攻撃者がアカウントの RDS データベースを侵害しようとしている可能性があることを示しています。

修復のレコメンデーション

関連付けられたデータベースに対するこのアクティビティが想定外の場合は、データベースのアクセスポリシーが過度に許容されているか、データベースが公開されている可能性があります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの失敗により、侵害された可能性のあるデータベースの修正」を参照してください。

Discovery:RDS/MaliciousIPCaller

既知の悪意のあるアクティビティに関連する IP アドレスがアカウントの RDS データベースを調べましたが、認証は行われませんでした。

デフォルトの重要度: [Medium] (中)

- 機能: RDS ログインアクティビティのモニタリング

この検出結果から、ログインを試みていないにもかかわらず、既知の悪意のあるアクティビティに関連する IP アドレスが AWS 環境内の RDS データベースを調べたことがわかります。これは、潜在的に悪意のある攻撃者が公的にアクセス可能なインフラストラクチャをスキャンしようとしていることを示している可能性があります。

修復のレコメンデーション

関連付けられたデータベースに対するこのアクティビティが想定外の場合は、データベースのアクセスポリシーが過度に許容されているか、データベースが公開されている可能性があります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの失敗により、侵害された可能性のあるデータベースの修正」を参照してください。

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

ユーザーが Tor 出口ノードの IP アドレスからアカウントの RDS データベースへのログインに成功しました。

デフォルトの重要度: [High] (高)

- 機能: RDS ログインアクティビティのモニタリング

この検出結果は、ユーザーが Tor 出口ノードの IP アドレスから AWS 環境内の RDS データベースに正常にログインしたことを示します。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、匿名ユーザーの真のアイデンティティを隠しているという意図により、アカウント内の RDS リソースへの不正アクセスを示している場合があります。

修復のレコメンデーション

関連付けられたデータベースに対するこのアクティビティが想定外の場合は、ユーザーの認証情報が公開されているか、侵害されている可能性があります。関連するデータベースユーザーのパスワードを変更し、利用可能な監査ログを確認して、侵害されたユーザーが行ったアクティビティを確認することをお勧めします。このアクティビティは、データベースへのアクセスポリシーが過度に寛容であるか、データベースが公開されていることを示している可能性もあります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの成功により、侵害された可能性のあるデータベースの修復」を参照してください。

CredentialAccess:RDS/TorIPCaller.FailedLogin

Tor IP アドレスはアカウントの RDS データベースにログインしようとしましたが、失敗しました。

デフォルトの重要度: [Medium] (中)

- 機能: RDS ログインアクティビティのモニタリング

この検出結果から、Tor 出口ノードの IP アドレスが AWS 環境内の RDS データベースにログインしようとしたが、正しいユーザー名またはパスワードを入力できなかったことがわかります。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、匿名ユーザーの真のアイデンティティを隠しているという意図により、アカウント内の RDS リソースへの不正アクセスを示している場合があります。

修復のレコメンデーション

関連付けられたデータベースに対するこのアクティビティが想定外の場合は、データベースのアクセスポリシーが過度に許容されているか、データベースが公開されている可能性があります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの失敗により、侵害された可能性のあるデータベースの修正」を参照してください。

Discovery:RDS/TorIPCaller

Tor 出口ノードの IP アドレスがアカウントの RDS データベースを調べましたが、認証は行われませんでした。

デフォルトの重要度: [Medium] (中)

- 機能: RDS ログインアクティビティのモニタリング

この検出結果は、Tor 出口ノードの IP アドレスがお客様の AWS 環境の RDS データベースを確認することをお勧めします。これは、潜在的に悪意のある攻撃者が公的にアクセス可能なインフラストラクチャをスキャンしようとしていることを示している可能性があります。Tor は匿名通信を有効化す

るソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、悪意のある攻撃者の真のアイデンティティを隠して、アカウント内の RDS リソースへの不正アクセスを行っていることを示している可能性があります。

修復のレコメンデーション

関連付けられたデータベースに対するこのアクティビティが想定外の場合は、データベースのアクセスポリシーが過度に許容されているか、データベースが公開されている可能性があります。データベースをプライベート VPC に配置し、必要なソースからのみトラフィックを許可するようにセキュリティグループのルールを制限することをお勧めします。詳細については、「ログインイベントの失敗により、侵害された可能性のあるデータベースの修正」を参照してください。

Runtime Monitoring の検出結果タイプ

Amazon は、Amazon EKS クラスター、Fargate および Amazon EC2 Amazon EC2インスタンス内の Amazon EC2 ホストおよびコンテナからのオペレーティングシステムレベルの動作に基づいて潜在的な脅威を示すために、次の Runtime Monitoring の検出結果 GuardDuty を生成します。

> **Note**
>
> Runtime Monitoring の検出結果タイプは、ホストから収集されたランタイムログに基づいています。ログには、悪意のある攻撃者によってコントロールされる可能性のあるファイルパスなどのフィールドが含まれています。これらのフィールドは、ランタイムコンテキストを提供するために検出 GuardDuty 結果にも含まれます。 GuardDuty コンソールの外部で Runtime Monitoring の検出結果を処理する場合は、検出結果フィールドをサニタイズする必要があります。例えば、検出結果フィールドをウェブページに表示するときに、検索フィールドを HTML でエンコードできます。

トピック

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic

- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Backdoor:Runtime/C&CActivity.B!DNS
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand

- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted

CryptoCurrency:Runtime/BitcoinTool.B

Amazon EC2 インスタンスまたはコンテナが暗号通貨関連のアクティビティに関連付けられている IP アドレスをクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境のリスト化した EC2 インスタンスまたはコンテナで暗号通貨関連アクティビティに紐づけられた IP アドレスがクエリされていることを知らせるものです。脅威アクターは、コンピューティングリソースをコントロールして、不正な暗号通貨マイニングに対して悪意を持ち再利用しようとする可能性があります。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスまたはコンテナを使用する場合、またはこれらのいずれかがブロックチェーンのアクティビティに関与している場合は、この CryptoCurrency:Runtime/BitcoinTool.B 検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。ご使用の AWS 環境でこのような場合は、この検出結果の抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の検索条件フィルターでは、[検出結果タイプ] 属性に `CryptoCurrency:Runtime/BitcoinTool.B` という値を使用します。2 つ目のフィルター条件は、インスタンスの [インスタンス ID]、または暗号通貨やブロックチェーン関連のアクティビティに関わるコンテナの [コンテナイメージ ID] です。詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Backdoor:Runtime/C&CActivity.B

Amazon EC2 インスタンスまたはコンテナは、既知のコマンドとコントロールサーバーに関連付けられる IP をクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境のリスト化した EC2 インスタンスまたはコンテナが既知のコマンドとコントロール (C&C) サーバーに関連付けられた IP をクエリしていることを知らせるものです。リストされているインスタンスまたはコンテナが侵害されている可能性があります。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータです。

ボットネットとは、一般的なタイプのマルウェアに感染しコントロールされたインターネットコネクテッドデバイス (PC、サーバー、モバイルデバイス、IoT デバイスなど) のコレクションです。通常、ボットネットは、マルウェアの配布や盗用された情報 (クレジットカード番号など) の収集に使用されます。ボットネットの目的と構造によっては、C&C サーバーから分散型サービス拒否 (DDoS) 攻撃を開始するためのコマンドが発行されることもあります。

> **Note**
>
> クエリされた IP が log4j 関連の場合、関連付けられた検出結果のフィールドには次の値が含まれます。
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、コンソールの検出結果パネル GuardDutyでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

UnauthorizedAccess:Runtime/TorRelay

Amazon EC2 インスタンスまたはコンテナが Tor リレーとして Tor ネットワークに接続しています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境内の EC2 インスタンスまたはコンテナが、Tor リレーとして動作していることを示す方法で Tor ネットワークに接続していることを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。ある Tor リレーから別の Tor リレーにクライアントの不正なトラフィックを転送することで、通信の匿名性を高めます。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

UnauthorizedAccess:Runtime/TorClient

Amazon EC2 インスタンスまたはコンテナが Tor Guard または Authority ノードに接続しています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境内の EC2 インスタンスまたはコンテナが Tor Guard または Authority ノードに接続中であることを知らせるものです。Tor は匿名通信を有効化するソフトウェアで

す。Tor Guards および Authority ノードは、Tor ネットワークへの初期ゲートウェイとして動作します。このトラフィックは、この EC2 インスタンスまたはコンテナが侵害された可能性があり、Tor ネットワーク上のクライアントとして動作していることを示している場合があります。この検出結果は、攻撃者の真のアイデンティティを隠す目的で、 AWS リソースへの不正アクセスを示している可能性があります。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Trojan:Runtime/BlackholeTraffic

Amazon EC2 インスタンスまたはコンテナが既知のブラックホールであるリモートホストの IP アドレスに通信しようとしています。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

この検出結果は、リストされた EC2 インスタンスまたは AWS 環境内のコンテナがブラックホール (またはシンクホール) の IP アドレスと通信しようとしているために侵害されている可能性があることを知らせるものです。ブラックホールとは、送受信トラフィックが密かに破棄されるネットワークの場所を指し、意図した受信者にデータが届いていないことは送信元に知らされません。ブラックホール IP アドレスは、稼働していないホストマシンやホストが割り当てられていないアドレスを指定します。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Trojan:Runtime/DropPoint

Amazon EC2 インスタンスまたはコンテナが、マルウェアによって収集された認証情報やその他の盗難されたデータを保持していることが認識されているリモートホストの IP アドレスに通信しようとしています。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境内の EC2 インスタンスまたはコンテナが、マルウェアによってキャプチャされた認証情報やその他の盗難されたデータを保持していることがわかっているリモートホストの IP アドレスと通信しようとしていることを知らせるものです。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Amazon EC2 インスタンスまたはコンテナが暗号通貨のアクティビティに関連付けられているドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境のリスト化した EC2 インスタンスまたはコンテナで、ビットコイン、またはその他の暗号通貨関連アクティビティに紐づけたドメインがクエリされていることを知らせる

ものです。脅威アクターは、コンピューティングリソースを不正な暗号通貨マイニングに不正に転用するため、コンピュートリソースを乗っ取ろうとする可能性があります。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスまたはコンテナがを使用する場合、またはこれらのいずれかがブロックチェーンのアクティビティに関与している場合は、この CryptoCurrency:Runtime/BitcoinTool.B!DNS 検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。ご使用の AWS 環境でこのような場合は、この検出結果の抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター検索条件で構成する必要があります。1 つ目の条件では、[結果タイプ] 属性に `CryptoCurrency:Runtime/BitcoinTool.B!DNS` という値を使用します。2 つ目のフィルター条件では、暗号通貨またはブロックチェーンアクティビティに関与するインスタンスの [インスタンス ID]、またはコンテナの [コンテナイメージ ID] である必要があります。詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Backdoor:Runtime/C&CActivity.B!DNS

Amazon EC2 インスタンスまたはコンテナが、既知のコマンドとコントロールサーバーに関連付けられるドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境のリスト化した EC2 インスタンスおよびコンテナが既知のコマンドとコントロール (C&C) サーバーに関連付けられているドメインをクエリしていることを知らせるものです。リスト化した EC2 インスタンスまたはコンテナは侵害されている可能性があります。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータです。

ボットネットとは、一般的なタイプのマルウェアに感染し制御されたインターネットコネクテッドデバイス (PC、サーバー、モバイルデバイス、IoT デバイスなど) のコレクションです。通常、ボッ

トネットは、マルウェアの配布や盗用された情報 (クレジットカード番号など) の収集に使用されます。ボットネットの目的と構造によっては、C&C サーバーから分散型サービス拒否 (DDoS) 攻撃を開始するためのコマンドが発行されることもあります。

> **Note**
>
> クエリされたドメイン名が log4j 関連の場合、関連付けられた検出結果のフィールドには次の値が含まれます。
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> がこの検出結果タイプ GuardDuty を生成する方法をテストするには、テストドメイン に対してインスタンス から DNS リクエスト (digLinux の場合は 、Windows nslookup の場合は を使用) を行いますguarddutyc2activityb.com。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Trojan:Runtime/BlackholeTraffic!DNS

Amazon EC2 インスタンスまたはコンテナがブラックホールの IP アドレスにリダイレクトされるドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境のリスト化した EC2 インスタンスまたはコンテナがブラックホール IP アドレスにリダイレクトされるドメイン名をクエリしているため、侵害されている可能性があることを知らせるものです。ブラックホールとは、送受信トラフィックが密かに破棄されるネットワークの場所を指し、意図した受信者にデータが届いていないことは送信元に知らされません。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Trojan:Runtime/DropPoint!DNS

Amazon EC2 インスタンスまたはコンテナが、マルウェアによって収集された認証情報やその他の盗難されたデータを保持していることが認識されているリモートホストのドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境内の EC2 インスタンスまたはコンテナが、マルウェアによってキャプチャされた認証情報やその他の盗難されたデータを保持することが知られているリモートホストのドメイン名をクエリしていることを知らせるものです。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Trojan:Runtime/DGADomainRequest.C!DNS

Amazon EC2 インスタンスまたはコンテナがアルゴリズムを使用して生成されたドメインをクエリしています。このようなドメインは、マルウェアによって悪用されることが多く、EC2 インスタンスまたはコンテナが侵害されている場合があります。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境のリスト化した EC2 インスタンスまたはコンテナがドメイン生成アルゴリズム (DGA) のドメインをクエリしようとしていることを知らせるものです。リソースが侵害されている可能性があります。

DGA は、大量のドメイン名を定期的に生成してコマンドアンドコントロール (C&C) サーバーとのランデブーポイントとするために使用されます。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータであり、一般的なタイプのマルウェアに感染して制御されたインターネットのコネクテッドデバイスのコレクションです。ランデブーポイントの候補数が多いと、感染されたコンピュータは毎日これらのドメイン名の一部にアクセスしてアップデートやコマンドを受け取ろうとするため、ボットネットを効果的にシャットダウンすることが困難となります。

> **Note**
>
> この検出結果は、 GuardDuty 脅威インテリジェンスフィードの既知の DGA ドメインに基づいています。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Trojan:Runtime/DriveBySourceTraffic!DNS

Amazon EC2 インスタンスまたはコンテナがドライブバイダウンロード攻撃の既知の攻撃元であるリモートホストのドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、自動ダウンロード攻撃の既知のソースであるリモートホストのドメイン名をクエリしているため、リスト化した AWS 環境の EC2 インスタンスまたはコンテナが侵害された可能性があることを知らせるものです。これらは、インターネットから意図せずにダウンロードされるコンピュータソフトウェアであり、ウイルス、スパイウェア、マルウェアの自動インストールを開始する場合があります。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Trojan:Runtime/PhishingDomainRequest!DNS

Amazon EC2 インスタンスまたはコンテナがフィッシング攻撃に関与しているドメインをクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境の EC2 インスタンスまたはコンテナがフィッシング攻撃に関与しているドメインをクエリしようとしていることを知らせるものです。フィッシングドメインは、個人を特定できる情報、銀行やクレジットカードの詳細情報とパスワードなど、ユーザーが機密データを

提供するように仕向ける、正当な機関になりすました人物によって設定されます。EC2 インスタンスまたはコンテナがフィッシングウェブサイトに保存されている機密データを検索しようとしたり、フィッシングウェブサイトをセットアップしようとしたりする可能性があります。EC2 インスタンスまたはコンテナが侵害されている可能性があります。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Impact:Runtime/AbusedDomainRequest.Reputation

Amazon EC2 インスタンスまたはコンテナが、既知の悪用されたドメインに関連付けられた評価の低いドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境内にリストされている EC2 インスタンスまたはコンテナが、既知の悪用されたドメインまたは IP アドレスに関連付けられたレピュテーションの低いドメイン名をクエリしていることを知らせるものです。悪用したドメインの例としては、動的 DNS プロバイダーだけでなく、無料のサブドメイン登録を提供する最上位のドメイン名 (TLD) と第 2 位のドメイン名 (2LD) があります。脅威アクターは、無料または低コストでドメインを登録するこれらのサービスを使用する傾向があります。このカテゴリの評価の低いドメインは、レジストラのパーキング IP アドレスを決定する有効期限切れドメインであり、アクティブになっていない可能性があります。パーキング IP は、レジストラがどのサービスにもリンクされていないドメインのトラフィックを管理する場所です。脅威アクターが一般的にこれらのレジストラのサービスまたは C&C のサービス、マルウェアディストリビューションに使用するため、リストされた Amazon EC2 インスタンスまたはコンテナは侵害される可能性があります。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Impact:Runtime/BitcoinDomainRequest.Reputation

Amazon EC2 インスタンスまたはコンテナが、暗号通貨関連のアクティビティに関連付けられている評判の低いドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境のリスト化した EC2 インスタンスまたはコンテナで、ビットコイン、またはその他の暗号通貨関連アクティビティに紐づけた評判の低いドメイン名がクエリされていることを知らせるものです。脅威アクターは、コンピューティングリソースをコントロールして、不正な暗号通貨マイニングに対して悪意を持ち再利用しようとする可能性があります。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスまたはコンテナを使用する場合、またはこれらのリソースがブロックチェーンのアクティビティに関与している場合は、この検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。 AWS ご使用の環境でこのような場合は、この検出結果の抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の検索条件フィルターでは、[検出結果タイプ]

属性に Impact:Runtime/BitcoinDomainRequest.Reputation という値を使用します。2 番目のフィルター条件は、インスタンスの [インスタンス ID] か、コンテナの [コンテナイメージ ID] が暗号通貨やブロックチェーン関連のアクティビティに関係しているかどうかです。詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Impact:Runtime/MaliciousDomainRequest.Reputation

Amazon EC2 インスタンスまたはコンテナが、悪意のある既知のドメインに関連付けられた評判の低いドメインをクエリしています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境内にリストされている EC2 インスタンスまたはコンテナが、悪意のある既知のドメインまたは IP アドレスに関連付けられたレピュテーションの低いドメイン名をクエリしていることを知らせるものです。例えば、ドメインを既知のシンクホール IP アドレスに関連付けることができます。シンクホールドメインは、以前に脅威アクターに制御されたドメインであり、ドメインへのリクエストは、インスタンスが侵害されていることを示している場合があります。これらのドメインは、悪意のある既知のキャンペーンやドメイン生成アルゴリズムと相関している可能性もあります。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Impact:Runtime/SuspiciousDomainRequest.Reputation

Amazon EC2 インスタンスまたはコンテナが、年齢や低人気により、本質的に疑わしい、低評判のドメイン名をクエリしています。

デフォルトの重要度: [Low] (低)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境のリスト化した EC2 インスタンスまたはコンテナが悪意があると疑われたり、過去に悪意のあるドメインだったため評判の低いドメイン名をクエリしていることを知らせるものですが、当社の評判モデルは、既知の脅威と明確に関連付けることができませんでした。これらのドメインは通常、新たに観察されるか、または少量のトラフィックを受信します。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

UnauthorizedAccess:Runtime/MetadataDNSRebind

Amazon EC2 インスタンスまたはコンテナがインスタンスメタデータサービスに解決される DNS ルックアップを実行しています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

> **Note**
>
> 現在、この検出結果タイプは AMD64 アーキテクチャでのみサポートされています。

この検出結果は、 AWS 環境内の EC2 インスタンスまたはコンテナが EC2 メタデータ IP アドレス (169.254.169.254) に解決されるドメインをクエリしていることを知らせるものです。この種類の DNS クエリは、インスタンスが DNS リバインディング技術の対象であることを示している可能性があります。この手法は、インスタンスに関連付けらた IAM 認証情報など、EC2 インスタンスからメタデータを取得するために使用できます。

DNS リバインディングには、EC2 インスタンスで実行されているアプリケーションをだまして URL から返されるデータをロードすることが含まれます。URL のドメイン名は EC2 メタデータ IP アドレス (169.254.169.254) に解決されます。これにより、アプリケーションは EC2 メタデータにアクセスし、攻撃者がそのメタデータを使用できるようにする可能性があります。

EC2 インスタンスが URL の追加を許可する脆弱なアプリケーションを実行している場合や、EC2 インスタンスで実行されているウェブブラウザで、誰かが URL にアクセスする場合のみ、DNS リバインディングを使用して EC2 メタデータにアクセスできます。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

この検出結果に応じて、EC2 インスタンスまたはコンテナで実行されている脆弱性アプリケーションがあるか、誰が検出結果で識別したドメインへアクセスするためブラウザを使用しているかを評価する必要があります。根本的な原因が脆弱なアプリケーションである場合は、脆弱性を修復します。ユーザーが識別したドメインを閲覧した場合、ドメインをブロックするか、ユーザーがそのドメインにアクセスできないようにします。この検出結果が上記のいずれかのケースに関連していると判断した場合は、EC2 インスタンスに関連付けられたセッションを取り消す必要があります。

一部の AWS お客様は、メタデータ IP アドレスを権威 DNS サーバーのドメイン名に意図的にマッピングします。ご利用の環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の検索条件フィルターでは、[検出結果タイプ] 属性に `UnauthorizedAccess:Runtime/MetaDataDNSRebind` という値を使用します。2 番目のフィルター条件は、[DNS リクエストドメイン] またはコンテナの [コンテナイメージ ID] です。[DNS リクエストのドメイン] を使用します。値

はメタデータの IP アドレス (169.254.169.254) にマッピングしたドメインと一致する必要があります。抑制ルール作成の詳細については、「抑制ルール」を参照してください。

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Execution:Runtime/NewBinaryExecuted

コンテナで新しく作成、または最近変更されたバイナリファイルが実行されました。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

この検出結果から、コンテナ内で新たに作成、または変更されたバイナリファイルが実行されたことがわかります。実行時にコンテナを不変に保つことがベストプラクティスであり、バイナリファイル、スクリプト、またはライブラリはコンテナの存続期間中に作成または変更しないでください。この動作は、潜在的な侵害の一環として、コンテナへのアクセスを取得し、マルウェアやその他のソフトウェアをダウンロードして実行した悪意のあるアクターを示します。このタイプのアクティビティは侵害の兆候である可能性がありますが、一般的な使用パターンでもあります。したがって、GuardDuty は メカニズムを使用してこのアクティビティの疑わしいインスタンスを識別し、疑わしいインスタンスに対してのみこの検出結果タイプを生成します。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

PrivilegeEscalation:Runtime/DockerSocketAccessed

コンテナ内のプロセスは、Docker ソケットを使用して Docker デーモンと通信しています。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

Docker ソケットは、Docker デーモン (dockerd) がクライアントとの通信に使用する Unix ドメインソケットです。クライアントは、Docker ソケットを介して Docker デーモンと通信してコンテナを作成するなど、さまざまなアクションを実行できます。コンテナプロセスが Docker ソケットにアクセスするのは疑わしい状況です。コンテナプロセスは、Docket ソケットと通信して特権コンテナを作成することで、コンテナからエスケープしてホストレベルのアクセスを得ることができます。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

PrivilegeEscalation:Runtime/RuncContainerEscape

runC を介したコンテナエスケープの試行が検出されました。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

RunC は、Docker や Containerd などの高レベルのコンテナランタイムがコンテナのスポーンと実行に使用する低レベルのコンテナランタイムです。RunC は、コンテナ作成の低レベルタスクを実行する必要があるため、常にルート権限で実行されます。脅威アクターは、runC バイナリの脆弱性を変更または悪用することで、ホストレベルのアクセスを取得できます。

この検出結果は、runC バイナリの変更と、次の runC の脆弱性を悪用しようとする潜在的な試みを検出します。

- CVE-2019-5736 – の悪用CVE-2019-5736には、コンテナ内から runC バイナリを上書きすることが含まれます。この検出結果は、runC バイナリがコンテナ内のプロセスによって変更されると呼び出されます。
- CVE-2024-21626 – の悪用CVE-2024-21626には、現在の作業ディレクトリ (CWD) またはコンテナをオープンファイル記述子 に設定する必要があります`/proc/self/fd/`*`FileDescriptor`*。

この検出結果は、 の現在の作業ディレクトリを持つコンテナプロセス/proc/self/fd/が検出されたときに呼び出されます/proc/self/fd/7。例えば、。

この検出結果は、悪意のある攻撃者が次のいずれかのタイプのコンテナで悪用を実行しようとしたことを示している可能性があります。

- 攻撃者がコントロールするイメージを含んだ新しいコンテナ。
- ホストレベルの runC バイナリに対する書き込み権限を持つアクターがアクセス可能な既存のコンテナ。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

CGroups リリースエージェントを介したコンテナエスケープの試行が検出されました。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果から、コントロールグループ (cgroup) リリースエージェントファイルを変更しようとした試みが検出されたことがわかります。Linux はコントロールグループ (cgroup) を使用して、プロセスの集合のリソース使用量を制限したり、説明したり、分離したりします。各 cgroup にはリリースエージェントファイル (release_agent) があります。これは cgroup 内のいずれかのプロセスが終了したときに Linux が実行するスクリプトです。リリースエージェントファイルは常にホストレベルで実行されます。コンテナ内の脅威アクターは、cgroup に属するリリースエージェントファイルに任意のコマンドを書き込むことで、ホストに逃げることができます。その cgroup 内のプロセスが終了すると、アクターによって書き込まれたコマンドが実行されます。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

DefenseEvasion:Runtime/ProcessInjection.Proc

proc ファイルシステムを使用したプロセスインジェクションが、コンテナまたは Amazon EC2 インスタンスで検出されました。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

プロセスインジェクションは、脅威アクターが防御を回避し潜在的にアクセス許可を昇格させるため、プロセスにコードを挿入するために使用する手法です。proc ファイルシステム (procfs) は、プロセスの仮想メモリをファイルとして表示する Linux の特別なファイルシステムです。そのファイルのパスは `/proc/PID/mem` で、`PID` はプロセスの固有の ID です。脅威アクターは、このファイルに書き込んで、プロセスにコードを挿入できます。この検出結果により、このファイルへの書き込みを試みる可能性が明らかになりました。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティは予期しないものである場合、リソースタイプは予期しないものである可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

DefenseEvasion:Runtime/ProcessInjection.Ptrace

ptrace システムコールを使用したプロセスインジェクションが、コンテナまたは Amazon EC2 インスタンスで検出されました。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

プロセスインジェクションは、脅威アクターが防御を回避し潜在的にアクセス許可を昇格させるため、プロセスにコードを挿入するために使用する手法です。プロセスは ptrace システムコールを使って、別のプロセスにコードを挿入できる。この検出結果により、ptrace システムコールを使って、プロセスへのコードの挿入を試みる可能性が明らかになりました。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティは予期しないものである場合、リソースタイプは予期しないものである可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

仮想メモリへの直接書き込みによるプロセスインジェクションが、コンテナまたは Amazon EC2 インスタンスで検出されました。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

プロセスインジェクションは、脅威アクターが防御を回避し潜在的にアクセス許可を昇格させるため、プロセスにコードを挿入するために使用する手法です。プロセスは、`process_vm_writev` などのシステムコールを使用して、別のプロセスの仮想メモリにコードを直接挿入することができます。この検出結果により、プロセスの仮想メモリに書き込むためのシステムコールを使って、プロセスへのコードの挿入を試みる可能性が明らかになりました。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティは予期しないものである場合、リソースタイプは予期しないものである可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Execution:Runtime/ReverseShell

コンテナまたは Amazon EC2 インスタンス内のプロセスによってリバースシェルが作成されました。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

リバースシェルは、ターゲットホストからアクターのホストへの接続で作成されるシェルセッションです。これは、アクターのホストからターゲットのホストに対して開始される通常のシェルとは逆です。脅威アクターは、ターゲットへの最初のアクセス権を取得した後、リバースシェルを作成してターゲット上でコマンドを実行します。この検出結果により、リバースシェルの作成を試みる可能性が明らかになりました。

修復のレコメンデーション

このアクティビティは予期しないものである場合、リソースタイプは予期しないものである可能性があります。

DefenseEvasion:Runtime/FilelessExecution

コンテナまたは Amazon EC2 インスタンス内のプロセスが、メモリからコードを実行しています。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

この検出結果により、ディスク上のメモリ内の実行可能ファイルを使用してプロセスが実行されたときに通知されます。これは、ファイルシステムのスキャンによる検出を回避するために、悪意のある実行可能ファイルをディスクに書き込まないようにする、一般的な防御回避の手法です。この手法はマルウェアによって使用されていますが、正当な使用例もいくつかあります。例の 1 つは、コンパイルされたコードをメモリに書き込み、メモリから実行する just-in-time (JIT) コンパイラです。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Impact:Runtime/CryptoMinerExecuted

コンテナまたは Amazon EC2 インスタンスが、暗号通貨マイニングアクティビティに関連するバイナリファイルを実行しています。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、 AWS 環境内のコンテナまたは EC2 インスタンスが、暗号通貨マイニングアクティビティに関連付けられたバイナリファイルを実行していることを知らせるものです。脅威アクターは、コンピューティングリソースをコントロールして、不正な暗号通貨マイニングに対して悪意を持ち再利用しようとする可能性があります。

ランタイムエージェントは、複数のリソースタイプからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、 GuardDuty コンソールの検出結果パネルでリソースタイプを表示します。

修復のレコメンデーション

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。影響を受けるリソースを特定するには、 GuardDuty コンソールで検出結果の詳細でリソースタイプを表示し、「」を参照してくださいRuntime Monitoring 検出結果の修正。

Execution:Runtime/NewLibraryLoaded

新しく作成または最近変更されたライブラリが、コンテナ内のプロセスによってロードされました。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

この検出結果から、ライブラリが実行時にコンテナ内で作成または変更され、コンテナ内で実行されているプロセスによって読み込まれたことがわかります。ベストプラクティスは、実行時にはコンテナを不変のままにし、コンテナの存続期間中はバイナリファイル、スクリプト、またはライブラリを作成または変更しないことです。新しく作成または変更されたライブラリをコンテナにロードすると、不審なアクティビティが発生する可能性があります。この動作は、悪意のある攻撃者が潜在的な侵害の一環としてコンテナにアクセスし、マルウェアやその他のソフトウェアをダウンロードして実行した可能性があることを示しています。このタイプのアクティビティは侵害の兆候である可能性がありますが、一般的な使用パターンでもあります。したがって、 GuardDuty は メカニズムを使用してこのアクティビティの疑わしいインスタンスを識別し、疑わしいインスタンスに対してのみこの検出結果タイプを生成します。

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。影響を受けるリソースを特定するには、コンソールで検出結果の詳細で GuardDutyリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

コンテナ内のプロセスが、実行時にホストファイルシステムをマウントしました。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

複数のコンテナエスケープ手法では、実行時にホストファイルシステムをコンテナ内にマウントします。この検出結果から、コンテナ内のプロセスがホストファイルシステムをマウントしようとした可能性があり、ホストへのエスケープが試みられた可能性があることがわかります。

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。影響を受けるリソースを特定するには、コンソールで検出結果の詳細で GuardDutyリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

PrivilegeEscalation:Runtime/UserfaultfdUsage

あるプロセスが、**userfaultfd** システム呼び出しを使用してユーザースペースのページフォールトを処理しました。

デフォルトの重要度: [Medium] (中)

- 機能: Runtime Monitoring

通常、ページフォールトはカーネルスペースのカーネルによって処理されます。しかし、`userfaultfd` システムコールを使うと、プロセスはユーザースペースのファイルシステムのページフォールトを処理できるようになります。これはユーザースペースのファイルシステムの実装を可能にする便利な機能です。一方で、潜在的に悪意のあるプロセスによってユーザースペースからカーネルを妨害するためにも使用される可能性があります。`userfaultfd` システムコールを使ってカーネルを中断させることは、カーネルの競合状態を悪用している最中にレースウィンドウを延長するため、一般的に悪用の手法です。`userfaultfd` を使用すると、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上で不審なアクティビティが行われたことを示している可能性があります。

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。影響を受けるリソースを特定するには、コンソールで検出結果の詳細で GuardDutyリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Execution:Runtime/SuspiciousTool

コンテナまたは Amazon EC2 インスタンスでバイナリファイルまたはスクリプトが実行されており、ペネストエンゲージメントなどの攻撃的なセキュリティシナリオで頻繁に使用されます。

デフォルトの重要度: 可変

この検出結果の重要度は、検出された疑わしいツールが二重使用と見なされるか、攻撃的な使用のみを目的としているかに応じて、高または低のいずれかになります。

- 機能: Runtime Monitoring

この検出結果は、疑わしいツールが環境内の EC2 インスタンスまたはコンテナで実行されたことを知らせるものです AWS 。これには、バックドアツール、ネットワークスキャナー、ネットワークスニファとも呼ばれる、ペンテストエンゲージメントで使用されるツールが含まれます。これらのツールはすべて無害なコンテキストで使用できますが、悪意のある意図を持つ脅威アクターによって頻繁に使用されます。攻撃的なセキュリティツールを観察すると、関連する EC2 インスタンスまたはコンテナが侵害されている可能性があります。

GuardDuty は、関連するランタイムアクティビティとコンテキストを調べて、関連するアクティビティとコンテキストが疑わしい可能性がある場合にのみこの検出結果を生成します。

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。影響を受けるリソースを特定するには、コンソールで検出結果の詳細で GuardDutyリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Execution:Runtime/SuspiciousCommand

疑わしいコマンドがAmazon EC2 インスタンスまたは侵害を示すコンテナで実行されました。

デフォルトの重要度: 可変

観察された悪意のあるパターンの影響に応じて、この検出結果タイプの重要度は低、中、または高のいずれかになります。

- 機能: Runtime Monitoring

この検出結果は、疑わしいコマンドが実行されたことを知らせ、 AWS 環境内の Amazon EC2 インスタンスまたはコンテナが侵害されたことを示します。これは、ファイルが疑わしいソースからダウンロードされて実行されたか、実行中のプロセスがコマンドラインに既知の悪意のあるパターンを表

示することを意味します。これはさらに、マルウェアがシステムで実行されていることを示しています。

GuardDuty は、関連するランタイムアクティビティとコンテキストを調べて、関連するアクティビティとコンテキストが疑わしい可能性がある場合にのみこの検出結果を生成します。

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。影響を受けるリソースを特定するには、コンソールで検出結果の詳細で GuardDutyリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

DefenseEvasion:Runtime/SuspiciousCommand

コマンドは、リストされた Amazon EC2 インスタンスまたはコンテナで実行され、ファイアウォールや重要なシステムサービスなどの Linux 防御メカニズムを変更または無効にしようとします。

デフォルトの重要度: 可変

どの防御メカニズムが変更または無効化されたかに応じて、この検出結果タイプの重要度は高、中、低のいずれかになります。

- 機能: Runtime Monitoring

この検出結果は、ローカルシステムのセキュリティサービスから攻撃を隠そうとするコマンドが実行されたことを知らせるものです。これには、Unix ファイアウォールの無効化、ローカル IP テーブルの変更、crontabエントリの削除、ローカルサービスの無効化、`LDPreload`関数の引き継ぎなどのアクションが含まれます。変更は非常に疑わしいものであり、侵害の潜在的な指標です。したがって、これらのメカニズムはシステムのさらなる侵害を検出または防止します。

GuardDuty は、関連するランタイムアクティビティとコンテキストを調べて、関連するアクティビティとコンテキストが疑わしい可能性がある場合にのみこの検出結果を生成します。

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。侵害された可能性のあるリソースを特定するには、コンソールで検出結果の詳細で GuardDutyリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

DefenseEvasion:Runtime/PtraceAntiDebugging

コンテナまたは Amazon EC2 インスタンスのプロセスが、ptrace システムコールを使用してデバッグ対策を実行しました。

デフォルトの重要度: [Low] (低)

- 機能: Runtime Monitoring

この検出結果は、Amazon EC2 インスタンスまたは AWS 環境内のコンテナで実行されているプロセスが、 PTRACE_TRACEMEオプションを指定して ptrace システムコールを使用していることを示しています。このアクティビティにより、アタッチされたデバッガーが実行中のプロセスからデタッチされます。デバッガーがアタッチされていない場合、効果はありません。ただし、アクティビティ自体が疑惑を引き起こします。これは、マルウェアがシステムで実行されていることを示している可能性があります。Malware は、デバッグ防止技術を頻繁に使用して分析を回避し、これらの技術は実行時に検出できます。

GuardDuty は、関連するランタイムアクティビティとコンテキストを調べて、関連するアクティビティとコンテキストが疑わしい可能性がある場合にのみこの検出結果を生成します。

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。影響を受けるリソースを特定するには、コンソールで検出結果の詳細で GuardDutyリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

Execution:Runtime/MaliciousFileExecuted

悪意のある既知の実行可能ファイルが Amazon EC2 インスタンスまたはコンテナで実行されている。

デフォルトの重要度: [High] (高)

- 機能: Runtime Monitoring

この検出結果は、既知の悪意のある実行可能ファイルが Amazon EC2 インスタンスまたは AWS 環境内のコンテナで実行されたことを知らせるものです。これは、インスタンスまたはコンテナが侵害された可能性があり、マルウェアが実行されたことを示す強力な指標です。

Malware は、デバッグ防止技術を頻繁に使用して分析を回避し、これらの技術は実行時に検出できます。

GuardDuty は、関連するランタイムアクティビティとコンテキストを調べて、関連するアクティビティとコンテキストが疑わしい可能性がある場合にのみこの検出結果を生成します。

ランタイムエージェントは、複数のリソースからのイベントをモニタリングします。影響を受けるリソースを特定するには、コンソールで検出結果の詳細で GuardDutyリソースタイプを表示します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、リソースが侵害されている可能性があります。詳細については、「Runtime Monitoring 検出結果の修正」を参照してください。

GuardDuty S3 検索タイプ

以下の結果は Amazon S3 リソースに固有のもので、S3Bucketデータソースが S3 のデータイベントか、CloudTrail **AccessKey**CloudTrail データソースが管理イベントかのリソースタイプになります。検出結果の重要度と詳細は、検出結果タイプとバケットに関連付けられている許可によって異なります。

ここにリストされている検出結果には、検出結果タイプの生成に使用されるデータソースとモデルが含まれます。データソースとモデルの詳細については、「基礎データソース」を参照してください。

> **Important**
>
> S3 CloudTrail のデータイベントのデータソースに関する結果は、S3 保護が有効になっている場合にのみ生成されます GuardDuty。2020 年 7 月 31 日よりも後に作成されたすべてのアカウントでは、S3 Protection がデフォルトで有効になっています。S3 Protection を有効または無効にする方法については、「Amazon での Amazon S3 Protection GuardDuty」を参照してください。

すべての S3Bucket タイプの検出結果では、問題のバケットに対するアクセス権限と検出結果に関係するユーザーのアクセス権限を確認することをお勧めします。予期しないアクティビティについては、「侵害された可能性のある S3 バケットの修復」に記載されている修復レコメンデーションを参照してください。

トピック

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write
- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

S3 オブジェクトの検出に一般的に使用される API が、異常な方法で呼び出されました。

デフォルトの重要度: [Low] (低)

- データソース:S3 CloudTrail のデータイベント

この検出結果は、IAM エンティティが S3 API を呼び出して、環境内の `ListObjects` などの S3 バケットを検出したことを知らせるものです。この種のアクティビティは、攻撃者が情報を収集して、AWS お客様の環境が広範囲にわたる攻撃を受けやすいかどうかを判断する攻撃の発見段階に関連しています。IAM エンティティが異常な方法で API を呼び出したため、このアクティビティは疑わしいものです。例えば、過去の履歴がない IAM エンティティが S3 API を呼び出したり、IAM エンティティが通常とは異なる場所から S3 API 呼び出したりした場合です。

この API は、異常検知機械学習 (ML) GuardDuty モデルによって異常と判断されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API、リクエストされたバケット、および API 呼び出しの数など、API リクエストのさまざまな要因を追跡します。リクエストを呼び出したユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細」を参照してください。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Discovery:S3/MaliciousIPCaller

AWS 環境内のリソースの検出によく使用される S3 API が、既知の悪意のある IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- データソース:CloudTrail S3 のデータイベント

この検出結果は、S3 API オペレーションが悪意のある既知のアクティビティと関連した IP アドレスから呼び出されたことを知らせるものです。監視対象の API は通常、攻撃者が環境に関する情報を収集している攻撃の発見段階に関連付けられます。 AWS 例には、`GetObjectAcl` や `ListObjects` が含まれます。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Discovery:S3/MaliciousIPCaller.Custom

S3 API がカスタム脅威リストにある IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- データソース:S3 CloudTrail のデータイベント

この検出結果は、`GetObjectAcl` または `ListObjects` などの S3 API が、アップロード済みの脅威リストに含まれている IP アドレスから呼び出されたことを知らせています。この検出結果に関連する脅威リストは、検出結果の詳細の [Additional information] (追加情報) セクションにリストされています。このタイプのアクティビティは攻撃の検出段階に関連しており、攻撃者は、 AWS 環境がより広範な攻撃を受けやすいかどうかを判断するために情報を収集しています。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Discovery:S3/TorIPCaller

S3 API が Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース:S3 CloudTrail のデータイベント

この検出結果は、`GetObjectAcl` や `ListObjects` などの S3 API が Tor 出口ノードの IP アドレスから呼び出されたことを知らせるものです。この種のアクティビティは、攻撃者が情報を収集して、 AWS 環境が広範囲にわたる攻撃を受けやすいかどうかを判断する攻撃の発見段階に関連しています。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノー

ド間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。これは、 AWS 攻撃者の正体を隠す目的でリソースに不正にアクセスしたことを示している可能性があります。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Exfiltration:S3/AnomalousBehavior

IAM エンティティが疑わしい方法で S3 API を呼び出しました。

デフォルトの重要度: [High] (高)

- データソース:S3 CloudTrail のデータイベント

この検出結果から、IAM エンティティが S3 バケットの関連している API コールを行い、このアクティビティがそのエンティティの確立されたベースラインと異なっていることがわかります。このアクティビティで使用された API コールは、攻撃の抽出段階に関連付けられており、攻撃者はデータを収集します。IAM エンティティが異常な方法で API を呼び出したため、このアクティビティは疑わしいものです。例えば、過去の履歴がない IAM エンティティが S3 API を呼び出したり、IAM エンティティが通常とは異なる場所から S3 API 呼び出したりした場合です。

この API は、 GuardDutyの異常検知機械学習 (ML) モデルによって異常と判断されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API、リクエストされたバケット、および API 呼び出しの数など、API リクエストのさまざまな要因を追跡します。リクエストを呼び出したユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細」を参照してください。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Exfiltration:S3/MaliciousIPCaller

AWS 環境からデータを収集するために一般的に使用される S3 API が、既知の悪意のある IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- データソース:CloudTrail S3 のデータイベント

この検出結果は、S3 API オペレーションが悪意のある既知のアクティビティと関連した IP アドレスから呼び出されたことを知らせるものです。観察された API は、攻撃者がネットワークからデータを収集しようとしている侵入戦術に一般的に関連しています。例には、`GetObject` や `CopyObject` が含まれます。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Impact:S3/AnomalousBehavior.Delete

IAM エンティティが疑わしい方法でデータを削除をしようとした S3 API を呼び出しました。

デフォルトの重要度: [High] (高)

- データソース:S3 CloudTrail のデータイベント

この結果から、 AWS 環境内の IAM エンティティが S3 バケットに関する API 呼び出しを行っていて、この動作がそのエンティティで確立されたベースラインと異なることがわかります。このアクティビティで使用された API コールは、データを削除しようとする攻撃に関連付けられています。IAM エンティティが異常な方法で API を呼び出したため、このアクティビティは疑わしいものです。例えば、過去の履歴がない IAM エンティティが S3 API を呼び出したり、IAM エンティティが通常とは異なる場所から S3 API 呼び出したりした場合です。

この API は、 GuardDutyの異常検知機械学習 (ML) モデルによって異常と判断されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連

する異常なイベントを特定します。リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API、リクエストされたバケット、および API 呼び出しの数など、API リクエストのさまざまな要因を追跡します。リクエストを呼び出したユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細」を参照してください。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

S3 バケットのコンテンツを監査して、以前のオブジェクトバージョンを復元できるかどうか、または復元する必要があるかどうかを判断することをお勧めします。

Impact:S3/AnomalousBehavior.Permission

アクセスコントロールリスト (ACL) のアクセス許可設定に一般的に使用される API が異常な方法で呼び出されました。

デフォルトの重要度: [High] (高)

- データソース:S3 のデータイベント CloudTrail

この結果から、 AWS 環境内の IAM エンティティが、リストされている S3 バケットのバケットポリシーまたは ACL を変更したことが通知されます。この変更により、S3 バケットが認証されたすべてのユーザーに公開される可能性があります。 AWS

この API は、 GuardDutyの異常検知機械学習 (ML) モデルによって異常と判定されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API、リクエストされたバケット、および API 呼び出しの数など、API リクエストのさまざまな要因を追跡します。リクエストを呼び出したユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細」を参照してください。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

S3 バケットのコンテンツを監査して、オブジェクトが予期せずパブリックアクセスを許可されていなかったか確認することをお勧めします。

Impact:S3/AnomalousBehavior.Write

IAM エンティティが疑わしい方法でデータの書き込みをしようとした S3 API を呼び出しました。

デフォルトの重要度: [Medium] (中)

- データソース:S3 のデータイベント CloudTrail

この結果から、 AWS 環境内の IAM エンティティが S3 バケットに関する API 呼び出しを行っていて、この動作がそのエンティティで確立されたベースラインと異なることがわかります。このアクティビティで使用された API コールは、データを書き込もうとする攻撃に関連付けられています。IAM エンティティが異常な方法で API を呼び出したため、このアクティビティは疑わしいものです。例えば、過去の履歴がない IAM エンティティが S3 API を呼び出したり、IAM エンティティが通常とは異なる場所から S3 API 呼び出したりした場合です。

この API は、 GuardDutyの異常検知機械学習 (ML) モデルによって異常と判断されました。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた特定の API、リクエストされたバケット、および API 呼び出しの数など、API リクエストのさまざまな要因を追跡します。リクエストを呼び出したユーザーアイデンティティにおいて API リクエストのどの要因が異常なのかという詳細については、「検出結果の詳細」を参照してください。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

S3 バケットのコンテンツを監査して、この API 呼び出しが悪意のあるデータや不正なデータを書き込んでいなかったか確認することをお勧めします。

Impact:S3/MaliciousIPCaller

AWS 環境内のデータやプロセスの改ざんによく使用される S3 API が、既知の悪意のある IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- データソース:S3 CloudTrail のデータイベント

この検出結果は、S3 API オペレーションが悪意のある既知のアクティビティと関連した IP アドレスから呼び出されたことを知らせるものです。監視対象の API は、攻撃者が環境内のデータを操作、中断、または破壊しようとするインパクト戦術に関連しているのが一般的です。 AWS 例には、`PutObject` や `PutObjectAcl` が含まれます。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

PenTest:S3/KaliLinux

S3 API が Kali Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース:S3 のデータイベント CloudTrail

この結果から、Kali Linux を実行しているマシンが、アカウントの認証情報を使用して S3 API 呼び出しを行っていることがわかります。 AWS 認証情報は侵害されている可能性があります。Kali Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。また、攻撃者はこのツールを使用して EC2 設定の弱点を発見し、お客様の環境に不正にアクセスします。 AWS

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

PenTest:S3/ParrotLinux

S3 API が Parrot Security Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース:S3 CloudTrail のデータイベント

この結果から、Parrot Security Linux を実行しているマシンが、アカウントの認証情報を使用して S3 API 呼び出しを行っていることがわかります。 AWS 認証情報は侵害されている可能性があります。Parrot Security Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。このツールを攻撃者が利用して EC2 設定の脆弱性を探り出し、 AWS 環境への未承認のアクセスを取得する場合があります。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

PenTest:S3/PentooLinux

S3 API が Pentoo Linux マシンから呼び出されました。

デフォルトの重要度: [Medium] (中)

- データソース:S3 CloudTrail のデータイベント

この結果から、Pentoo Linux を実行しているマシンが、アカウントの認証情報を使用して S3 API 呼び出しを行っていることがわかります。 AWS 認証情報は侵害されている可能性があります。Pentoo Linux は、セキュリティプロフェッショナルが EC2 インスタンスの脆弱性を特定してパッチを適用するために使う一般的な侵入テストツールです。また、攻撃者はこのツールを使用して EC2 設定の弱点を発見し、お客様の環境に不正にアクセスします。 AWS

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Policy:S3/AccountBlockPublicAccessDisabled

IAM エンティティが、アカウント上の S3 ブロックパブリックアクセスを無効にするために使用される API を呼び出しました。

デフォルトの重要度: [Low] (低)

- データソース:CloudTrail 管理イベント

この検出結果は、Amazon S3 ブロックパブリックアクセスがアカウントレベルで無効されたことを知らせるものです。S3 ブロックパブリックアクセス設定が有効化されると、それらはデータが誤って公開されるのを防ぐためのセキュリティ対策として、バケット上でポリシー、またはアクセスコントロールリスト (ACL) をフィルタリングするために使われます。

バケット内、またはバケット内のオブジェクトへの公開アクセスを許可するために、通常、S3 ブロックパブリックアクセスは、アカウントでは無効になっています。アカウントのために S3 ブロックパブリックアクセスを無効にすると、バケットへのアクセスは、個々のバケットに適用されるポリシー、ACL、またはバケットレベルのパブリックアクセス設定によって制御されます。これは、必ずしもバケットがパブリックに共有されているということではありませんが、アクセスへの適切なレベルが提供されているのを確認するために、バケットに対して適用される許可を監査する必要があります。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Policy:S3/BucketAnonymousAccessGranted

IAM プリンシパルは、バケットポリシーまたは ACL を変更することにより、インターネットへの S3 バケットへのアクセスを許可しています。

デフォルトの重要度: [High] (高)

- データソース:CloudTrail 管理イベント

この検出結果から、IAM エンティティが、そのバケット上のバケットポリシーまたは ACL を変更したため、リストされた S3 バケットがインターネット上でパブリックにアクセス可能になったことを知らせるものです。ポリシーまたは ACL の変更が検出された後に、Zelkova によって提供された自動推論を使用して、バケットがパブリックアクセス可能かどうかを判断します。

> **Note**
>
> バケットの ACL またはバケットポリシーが明示的に拒否またはすべてを拒否するように設定されている場合、この検出結果はバケットの現在の状態を反映していない可能性があります。この検出結果には、S3 バケットで有効になっている可能性のある S3 ブロックパブリックアクセス設定は反映されません。このような場合、検出結果の `effectivePermission` 値には `UNKNOWN` としてマークされます。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Policy:S3/BucketBlockPublicAccessDisabled

IAM エンティティが、バケットの S3 ブロックパブリックアクセスを無効にするために使用される API を呼び出しました。

デフォルトの重要度: [Low] (低)

- データソース:CloudTrail 管理イベント

この検出結果から、リストされた S3 バケットのために、ブロックパブリックアクセスが無効になったことを知らせるものです。有効にすると、S3 ブロックパブリックアクセス設定が使われ、バケットに適用されるポリシーまたは アクセスコントロールリスト (ACL) をフィルタリングし、データが誤って公開される安全対策となります。

通常、S3 ブロックパブリックアクセスは、バケット上で無効にされ、バケットまたはバケット内のオブジェクトへの公開アクセスを許可します。S3 ブロックパブリックアクセスがこのバケットに対して無効になっている場合、バケットに適用されるポリシーまたはそれに適用される ACL によって、バケットへのアクセスが制御されます。これは、バケットがパブリックに共有されているということではありませんが、バケットに適用されているポリシーと ACL を監査して、適切な許可が適用されていることを確認する必要があります。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Policy:S3/BucketPublicAccessGranted

IAM プリンシパルは、バケットポリシーまたは ACL を変更して S3 AWS バケットへのパブリックアクセスをすべてのユーザーに許可しました。

デフォルトの重要度: [High] (高)

- データソース:CloudTrail 管理イベント

この結果から、IAM エンティティが S3 バケットのバケットポリシーまたは ACL を変更したため、表示された S3 AWS バケットが認証されたすべてのユーザーに公開されたことがわかります。ポリシーまたは ACL の変更が検出された後に、Zelkova によって提供された自動推論を使用して、バケットがパブリックアクセス可能かどうかを判断します。

> **Note**
>
> バケットの ACL またはバケットポリシーが明示的に拒否またはすべてを拒否するように設定されている場合、この検出結果はバケットの現在の状態を反映していない可能性があります。この検出結果には、S3 バケットで有効になっている可能性のある S3 ブロックパブリックアクセス設定は反映されません。このような場合、検出結果の `effectivePermission` 値には `UNKNOWN` としてマークされます。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Stealth:S3/ServerAccessLoggingDisabled

バケットのために S3 サーバーアクセスのログ記録が無効になりました。

デフォルトの重要度: [Low] (低)

- データソース:管理イベント CloudTrail

この結果から、 AWS 環境内のバケットの S3 サーバーアクセスロギングが無効になっていることがわかります。無効にすると、特定の S3 バケットにアクセスしようとしてもウェブリクエストログは作成されませんが、バケットへの S3 管理 API コール (など) は引き続き追跡されます。DeleteBucketこのバケットで S3 データイベントロギングが有効になっている場合でも、バケット内のオブジェクトに対するウェブリクエストは引き続き追跡されます。 CloudTrail ログ記録の無効化は、許可されていないユーザーがその形跡を隠すために頻繁に使用する手法です。S3 ログの詳細については、「S3 サーバーアクセスログ」と「S3 ログオプション」を参照してください。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

S3 API がカスタム脅威リストにある IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- データソース:CloudTrail S3 のデータイベント

この検出結果は、アップロードした脅威リストに含まれたIP アドレスから S3 API オペレーション (`PutObject` や `PutObjectAcl` など) が呼び出されたことを知らせるものです。この検出結果に関連する脅威リストは、検出結果の詳細の [Additional information] (追加情報) セクションにリストされています。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

UnauthorizedAccess:S3/TorIPCaller

S3 API が Tor 出口ノードの IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

- データソース:S3 CloudTrail のデータイベント

この検出結果は、Tor 出口ノードの IP アドレスから S3 API オペレーション (`PutObject` や `PutObjectAcl` など) が呼び出されたことを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。この結果から、攻撃者の正体を隠す目的で、 AWS リソースに不正にアクセスされた可能性があります。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

廃止された検出結果タイプ

検出結果は、GuardDuty で検出した潜在的なセキュリティ問題に関する詳細を含む通知です。新しく追加されたタイプや廃止されたタイプを含む、GuardDuty の検出結果タイプの重要な変更点については、「Amazon のドキュメント履歴 GuardDuty」を参照してください。

GuardDuty により生成された、次の検出結果タイプは廃止されています (今後生成されません)。

> **Important**
>
> GuardDuty の廃止された検出結果タイプを再アクティブ化することはできません。

トピック

Exfiltration:S3/ObjectRead.Unusual

IAM エンティティが疑わしい方法で S3 API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

- データソース: S3 CloudTrail データイベント

この検出結果は、AWS 環境中の IAM エンティティは、S3 バケットを含み、そのエンティティの確立されたベースラインとは異なる API コールが実行されていることを知らせるものです。このアクティビティで使用された API コールは、攻撃の抽出段階に関連付けられており、攻撃者はデータを収集しようとしています。IAM エンティティが API を呼び出した方法が異常だったため、このアクティビティは疑わしいものです。例えば、この IAM エンティティに以前このタイプの API を呼び出した履歴がない場合や、API が異常な場所から呼び出された場合などです。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Impact:S3/PermissionsModification.Unusual

IAM エンティティが API を呼び出して、1 つ以上の S3 リソースの許可を変更しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、IAM エンティティが、AWS 環境内の 1 つ以上のバケットまたはオブジェクトの許可を変更するように設計された API コールを行っていることを知らせるものです。このアクションは、攻撃者により、アカウント外で情報を共有できるよう実行された可能性があります。IAM エンティティが API を呼び出した方法が異常だったため、このアクティビティは疑わしいものです。例えば、この IAM エンティティに以前このタイプの API を呼び出した履歴がない場合や、API が異常な場所から呼び出された場合などです。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Impact:S3/ObjectDelete.Unusual

IAM エンティティが S3 バケット内のデータを削除するために使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、AWS 環境内の特定の IAM エンティティが、バケット自体を削除して、リストされた S3 バケットのデータを削除するように設計された API コールを実行していることを知らせるものです。IAM エンティティが API を呼び出した方法が異常だったため、このアクティビティは疑わしいものです。例えば、この IAM エンティティに以前このタイプの API を呼び出した履歴がない場合や、API が異常な場所から呼び出された場合などです。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Discovery:S3/BucketEnumeration.Unusual

IAM エンティティが、ネットワーク内の S3 バケットを検出するために使用される S3 API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、IAM エンティティが S3 API を呼び出して、環境内の `ListBuckets` などの S3 バケットを検出したことを知らせるものです。このタイプのアクティビティは攻撃の検出段階に関連しており、攻撃者は、AWS 環境がより広範な攻撃を受けやすいかどうかを判断するために情報を収集しています。IAM エンティティが API を呼び出した方法が異常だったため、このアクティビティは疑わしいものです。例えば、この IAM エンティティに以前このタイプの API を呼び出した履歴がない場合や、API が異常な場所から呼び出された場合などです。

修復のレコメンデーション

関連付けられたプリンシパルに対してこのアクティビティが予期せぬ場合は、認証情報が公開されているか、S3 許可が十分に制限されていないことを示している可能性があります。詳細については、「侵害された可能性のある S3 バケットの修復」を参照してください。

Persistence:IAMUser/NetworkPermissions

IAM ユーザーが、AWS アカウントのセキュリティグループ、ルート、ACL のネットワーク許可を変更するために一般的に使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、AWS 環境の特定のプリンシパル (AWS アカウントのルートユーザー、IAM ロール、またはユーザー) が確立されたベースラインとは異なる動作をしていることを示しています。このプリンシパルには、この API 呼び出しの履歴はありません。

この検出結果は、ネットワーク構成設定が不審な状況下で変更された場合、例えば、プリンシパルが CreateSecurityGroup API を呼び出したが、それ以前に呼び出しの履歴がない場合などにトリガーされます。攻撃者はよく、セキュリティグループの変更を試み、さまざまなポートで特定のインバウンドトラフィックを許可させて彼らが EC2 インスタンスにアクセスする能力を向上させようとします。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Persistence:IAMUser/ResourcePermissions

プリンシパルが、AWS アカウント のさまざまなリソースのセキュリティアクセスポリシーを変更するために一般的に使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は「高」になります。

この検出結果は、AWS 環境の特定のプリンシパル (AWS アカウントのルートユーザー、IAM ロール、またはユーザー) が確立されたベースラインとは異なる動作をしていることを示しています。このプリンシパルには、この API 呼び出しの履歴はありません。

この検出結果は、AWS リソースにアタッチされたポリシーや許可に変更が見られた場合、例えば、AWS 環境のプリンシパルが PutBucketPolicy API を呼び出したが、それ以前に呼び出しの履歴がない場合などにトリガーされます。Amazon S3 など一部のサービスでは、リソースに対するプリンシパルアクセスを 1 つ以上付与する、リソースにアタッチされた許可をサポートします。盗まれた認証情報が使用されると、攻撃者はリソースにアタッチされたポリシーを変更し、自身にそのリソースに対する今後のアクセスを付与できます。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Persistence:IAMUser/UserPermissions

プリンシパルが、AWS アカウントの IAM ユーザー、グループ、ポリシーを追加、変更、削除するために一般的に使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、AWS 環境の特定のプリンシパル (AWS アカウントのルートユーザー、IAM ロール、またはユーザー) が確立されたベースラインとは異なる動作をしていることを示しています。このプリンシパルには、この API 呼び出しの履歴はありません。

この検出結果は、AWS 環境のユーザー関連の許可に不審な変更があった場合、例えば、AWS 環境のプリンシパルが `AttachUserPolicy` API を呼び出したが、それ以前に呼び出しの履歴がない場合などにトリガーされます。攻撃者は、盗まれた認証情報を使用して、新規ユーザーの作成、既存ユーザーに対するアクセスポリシーの追加、またはアクセスキーの作成により、元のアクセスポイントが閉じられている場合であってもアカウントへのアクセスを最大化することがあります。例えば、アカウントの所有者が特定の IAM ユーザーまたはパスワードが盗まれたことに気づいてアカウントから削除したとします。ただし、不正に作成された管理者プリンシパルによって作成された他のユーザーを削除することはなく、攻撃者が AWS アカウントにアクセスできる状態にしてしまう可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

PrivilegeEscalation:IAMUser/AdministrativePermissions

プリンシパルがそれ自体に非常に寛容なポリシーを割り当てようとしました。

デフォルトの重要度: [Low] (低)*

> **Note**
>
> 特権のエスカレーションに失敗した場合のこの検出結果の重要度は [Low] (低) で、特権のエスカレーションに成功した場合は [Medium] (中) です。

この検出結果は、AWS 環境の特定の IAM エンティティが特権エスカレーション攻撃を示す可能性のある動作をしていることを示します。この検出結果は、IAM ユーザーまたはロールが許容度の高いポリシーを割り当てようとするとトリガーされます。問題となるユーザーまたはロールが管理者特権を持つことを意図しない場合は、ユーザーの認証情報が危険にさらされているか、ロールの許可が正しく設定されていない可能性があることを示します。

攻撃者は、盗まれた認証情報を使用して、新規ユーザーの作成、既存ユーザーに対するアクセスポリシーの追加、またはアクセスキーの作成により、元のアクセスポイントが閉じられている場合であってもアカウントへのアクセスを最大化します。アカウントの所有者が特定の IAM ユーザーのサインイン認証情報が盗まれたことに気づいてアカウントから削除したとしても、不正に作成した管理者プリンシパルによって作成された他のユーザーを削除せず、その AWS アカウントに攻撃者がアクセスすることが可能なままになっている場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Recon:IAMUser/NetworkPermissions

プリンシパルが、AWS アカウントのセキュリティグループ、ルート、ACL のネットワークアクセス許可を変更するために一般的に使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、AWS 環境の特定のプリンシパル (AWS アカウントのルートユーザー、IAM ロール、またはユーザー) が確立されたベースラインとは異なる動作をしていることを示しています。このプリンシパルには、この API 呼び出しの履歴はありません。

この検出結果は、AWS アカウントのリソース許可が不審な状況下で調査された場合にトリガーされます。例えば、プリンシパルが `DescribeInstances` API を呼び出したが、それ以前に呼び出しの履歴がない場合です。攻撃者は盗まれた認証情報を使用して、より重要な認証情報を見つけたり、入手した認証情報の機能を特定するために、ユーザーの AWS リソースの偵察を行うことがあります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Recon:IAMUser/ResourcePermissions

プリンシパルが、AWS アカウントのさまざまなリソースのセキュリティアクセスポリシーを変更するために一般的に使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、AWS 環境の特定のプリンシパル (AWS アカウントのルートユーザー、IAM ロール、またはユーザー) が確立されたベースラインとは異なる動作をしていることを示しています。このプリンシパルには、この API 呼び出しの履歴はありません。

この検出結果は、AWS アカウントのリソース許可が不審な状況下で調査された場合にトリガーされます。例えば、プリンシパルが `DescribeInstances` API を呼び出したが、それ以前に呼び出しの履歴がない場合です。攻撃者は盗まれた認証情報を使用して、より重要な認証情報を見つけたり、入手した認証情報の機能を特定するために、ユーザーの AWS リソースの偵察を行うことがあります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Recon:IAMUser/UserPermissions

プリンシパルが、AWS アカウントの IAM ユーザー、グループ、ポリシーを追加、変更、削除するために一般的に使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、AWS 環境のユーザー許可が不審な状況下で調査された場合にトリガーされます。例えば、プリンシパル (AWS アカウントのルートユーザー、IAM ロール、または IAM ユーザー) が `ListInstanceProfilesForRole` API を呼び出したが、それ以前に呼び出しの履歴がない場合です。攻撃者は盗まれた認証情報を使用して、より重要な認証情報を見つけたり、入手した認証情報の機能を特定するために、ユーザーの AWS リソースの偵察を行うことがあります。

この検出結果は、AWS 環境の特定のプリンシパルが通常とは異なる動作をしていることを示しています。このプリンシパルには、このような API コールの履歴はありません。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

ResourceConsumption:IAMUser/ComputeResources

プリンシパルが、EC2 インスタンスなどのコンピューティングリソースを起動するために一般的に使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、AWS 環境にリストされたアカウント内の EC2 インスタンスが不審な状況下で起動された場合にトリガーされます。この検出結果は、AWS 環境の特定のプリンシパルが確立されたベースラインとは異なる動作をしていることを示しています。例えば、プリンシパル (AWS アカウントのルートユーザー、IAM ロール、または IAM ユーザー) が `RunInstances` API を呼び出したが、それ以前に呼び出しの履歴がない場合です。これは、攻撃者が盗まれた認証情報を使用して、コンピューティング時間を盗難 (暗号通貨マイニングやパスワードのクラッキングなど) している可能性を示します。または、攻撃者が AWS 環境の EC2 インスタンスおよび認証情報を使用してアカウントへのアクセスを維持している可能性を示している場合もあります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

Stealth:IAMUser/LoggingConfigurationModified

プリンシパルが、AWS アカウントの CloudTrail によるログ記録の停止、既存のログの削除、その他アクティビティの痕跡を消すために一般的に使用される API を呼び出しました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、環境内でリストされた AWS アカウントのログ記録設定が不審な状況下で変更された場合にトリガーされます。この検出結果は、AWS 環境の特定のプリンシパルが確立されたベースラインとは異なる動作をしていることを知らせるものです。例えば、プリンシパル (AWS アカウントのルートユーザー、IAM ロール、または IAM ユーザー) が `StopLogging` API を呼び出したが、それ以前に呼び出しの履歴がない場合です。これは、攻撃者が自身のアクティビティの痕跡を消去することで自身の行動を隠そうとしていることを示す場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

UnauthorizedAccess:IAMUser/ConsoleLogin

AWS アカウントのプリンシパルによる通常とは違うコンソールへのログインが確認されました。

デフォルトの重要度: [Medium] (中)*

> **Note**
>
> この検出結果のデフォルトの重要度は [Medium] (中) です。ただし、インスタンスで作成される一時的な AWS 認証情報を使用して API が呼び出された場合、検出結果の重要度は [High] (高) になります。

この検出結果は、コンソールへのログインが不審な状況下で検出された場合にトリガーされます。例えば、プリンシパルが、これまで行ったことのない ConsoleLogin API の呼び出しを、これまで使用したことのないクライアントまたは通常とは異なる場所から行った場合などです。これは、盗まれた認証情報が AWS アカウントにアクセスするために使用されているか、有効なユーザーが無効または安全ではない方法 (例えば、許可された VPN 経由ではないなど) でアカウントにアクセスしている可能性を示します。

この検出結果は、AWS 環境の特定のプリンシパルが通常とは異なる動作をしていることを知らせるものです。このプリンシパルには、この特定の場所からこのクライアントアプリケーションを使用してログインしたアクティビティの履歴はありません。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

UnauthorizedAccess:EC2/TorIPCaller

EC2 インスタンスが Tor 出口ノードからのインバウンド接続を受信しています。

デフォルトの重要度: [Medium] (中)

この検出結果は、AWS 環境内の EC2 インスタンスが Tor 出口ノードからのインバウンド接続を受信していることを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。通信を暗号化し、一連のネットワークノード間のリレー中にランダムに通信をバウンスさせます。最後の Tor ノードは出口ノードと呼ばれます。この検出結果は、攻撃者が真のアイデンティティを隠して、AWS リソースへの未承認のアクセスを行っていることを示している場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Backdoor:EC2/XORDDOS

EC2 インスタンスが通信しようとしている IP アドレスには XOR DDoS マルウェアが関連付けられています。

デフォルトの重要度: [High] (高)

この検出結果は、AWS 環境内の EC2 インスタンスが通信しようとしている IP アドレスに XOR DDoS マルウェアが関連付けられていることを知らせるものです。この EC2 インスタンスは侵害されている可能性があります。XOR DDoS は、Linux システムをハイジャックするトロイの木馬マルウェアです。システムへのアクセスを得るため、このマルウェアは Linux 上の Secure Shell (SSH) サービスへのパスワードを発見するためのブルートフォース攻撃を開始します。SSH 認証情報を取得してログインに成功すると、ルートユーザー権限を使用して、XOR DDoS をダウンロードしてインストールするスクリプトを実行します。その後、このマルウェアはボットネットの一部として、他のターゲットに対する分散型サービス拒否 (DDoS) 攻撃を開始します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

Behavior:IAMUser/InstanceLaunchUnusual

ユーザーが起動した EC2 インスタンスのタイプが通常と異なります。

デフォルトの重要度: [High] (高)

この検出結果は、AWS 環境の特定のユーザーが通常とは異なる動作をしていることを知らせるものです。このユーザーには、このタイプの EC2 インスタンスを起動した履歴がありません。サインイン認証情報は侵害されている可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

CryptoCurrency:EC2/BitcoinTool.A

EC2 インスタンスはビットコインマイニングプールと通信しています。

デフォルトの重要度: [High] (高)

この検出結果は、AWS 環境の EC2 インスタンスがビットコインマイニングプールと通信していることを知らせるものです。暗号通貨マイニングの分野で、マイニングプールとはマイナー (採掘者) によるリソースの共同出資 (プール) であり、ネットワークで処理能力を共有し、ブロックの解決に貢献した度合いに応じて報酬の分配を受ける仕組みです。この EC2 インスタンスをビットコインマイニングに使用していない限り、EC2 インスタンスは侵害されている可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

UnauthorizedAccess:IAMUser/UnusualASNCaller

API が通常とは異なるネットワークの IP アドレスから呼び出されました。

デフォルトの重要度: [High] (高)

この検出結果は、特定のアクティビティが通常とは異なるネットワークの IP アドレスから呼び出されたことを知らせるものです。これは、記述されたユーザーの AWS の使用履歴全体で一度も確認されていないネットワークです。このアクティビティには、コンソールログイン、EC2 インスタンスの起動、新しい IAM ユーザーの作成、AWS 権限の変更などが含まれます。これは、AWS リソースへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合は、認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。

リソース別の検出結果タイプ

以下のページは、 GuardDuty 結果に関連付けられたリソースタイプ別に分類されています。

- EC2 の検出結果タイプ
- Runtime Monitoring の検出結果タイプ
- IAM の検出結果タイプ
- EKS 監査ログの検出結果タイプ
- Lambda Protection の検出結果タイプ
- EC2 検出結果タイプの Malware Protection
- S3 検出結果タイプの Malware Protection
- RDS Protection の検出結果タイプ
- S3 の検出結果タイプ

検出結果の表

次の表は、有効なすべての検出結果タイプを基本データソースまたは機能別にソートをして示しています。次のアスタリスク付きの検出結果タイプの重要度は異なる可能性があります。検出結果タイプの変動する重要度については、該当の検出結果タイプの詳細説明を参照してください。

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail S3 のデータイベント	低
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3 のデータイベント	高い
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail S3 のデータイベント	高い
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail S3 のデータイベント	中程度
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail S3 のデータイベント	高い
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3 のデータイベント	高い
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail S3 のデータイベント	高い
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail S3 のデータイベント	高い
Impact:S3/Anomalou	Amazon S3	CloudTrail S3 のデータイベント	中程度

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
sBehavior.Write			
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3 のデータイベント	高い
PenTest:S3/KaliLinux	Amazon S3	CloudTrail S3 のデータイベント	中程度
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail S3 のデータイベント	中程度
PenTest:S3/PentooLinux	Amazon S3	CloudTrail S3 のデータイベント	中程度
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail S3 のデータイベント	高い
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail S3 のデータイベント	高い
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理イベント	中程度
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理イベント	中程度

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理イベント	低
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理イベント	高い
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理イベント	高い
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理イベント	中程度
PenTest:IAMUser/KaliLinux	IAM	CloudTrail 管理イベント	中程度
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail 管理イベント	中程度
PenTest:IAMUser/PentooLinux	IAM	CloudTrail 管理イベント	中程度

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理イベント	中程度
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail 管理イベント	[Low] (低)*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail 管理イベント	[High] (高)*
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail 管理イベント	低
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail 管理イベント	高い
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail 管理イベント	低

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail 管理イベント	高い
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理イベント	中程度
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail 管理イベント	中程度
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail 管理イベント	中程度
Recon:IAMUser/TorIPCaller	IAM	CloudTrail 管理イベント	中程度
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail 管理イベント	低
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail 管理イベント	低

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail 管理イベント	中程度
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail 管理イベント	中程度
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail 管理イベント	中程度
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail 管理イベント	中程度
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail S3 の管理イベントまたは CloudTrail データイベント	低

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail S3 の管理イベントまたは CloudTrail データイベント	高い
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNS ログ	高い
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNS ログ	高い
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNS ログ	中程度
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNS ログ	高い
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNS ログ	高い

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNS ログ	低
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNS ログ	中程度
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNS ログ	高い
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNS ログ	高い
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNS ログ	高い
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNS ログ	高い
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNS ログ	中程度
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNS ログ	高い

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNS ログ	高い
Execution:Container/MaliciousFile	コンテナ	EBS Malware Protection	検出された脅威によって異なります
Execution:Container/SuspiciousFile	コンテナ	EBS Malware Protection	検出された脅威によって異なります
Execution:EC2/MaliciousFile	EC2	EBS Malware Protection	検出された脅威によって異なります
Execution:EC2/SuspiciousFile	EC2	EBS Malware Protection	検出された脅威によって異なります
Execution:ECS/MaliciousFile	ECS	EBS Malware Protection	検出された脅威によって異なります
Execution:ECS/SuspiciousFile	ECS	EBS Malware Protection	検出された脅威によって異なります
Execution:Kubernetes/MaliciousFile	Kubernetes	EBS Malware Protection	検出された脅威によって異なります

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBS Malware Protection	検出された脅威によって異なります
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	EKS 監査ログ	中程度
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 監査ログ	高い
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 監査ログ	高い
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 監査ログ	高い

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKS 監査ログ	高い
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 監査ログ	高い
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 監査ログ	高い
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 監査ログ	高い
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	EKS 監査ログ	高い
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	EKS 監査ログ	[Low] (低)

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 監査ログ	中程度
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 監査ログ	中程度
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 監査ログ	中程度
Discovery:Kubernetes/TorIPCaller	Kubernetes	EKS 監査ログ	中程度
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	EKS 監査ログ	中程度
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	EKS 監査ログ	中程度

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	EKS 監査ログ	[Low] (低)
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 監査ログ	高い
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 監査ログ	高い
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 監査ログ	高い
Impact:Kubernetes/TorIPCaller	Kubernetes	EKS 監査ログ	高い
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	EKS 監査ログ	中程度

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKS 監査ログ	中程度
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS 監査ログ	中程度
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS 監査ログ	高い
Persistence:Kubernetes/TorIPCaller	Kubernetes	EKS 監査ログ	中程度
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	EKS 監査ログ	高い
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	EKS 監査ログ	高い

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	EKS 監査ログ	中程度
Policy:Kubernetes/ExposedDashboard	Kubernetes	EKS 監査ログ	中程度
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKS 監査ログ	[Medium] (中)*
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKS 監査ログ	[Low] (低)

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKS 監査ログ	高い
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKS 監査ログ	高い
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	EKS 監査ログ	中程度
Backdoor:Lambda/C&CActivity.B	Lambda	Lambda Network Activity Monitoring	高い
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Lambda Network Activity Monitoring	高い

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Trojan:Lambda/BlackholeTraffic	Lambda	Lambda Network Activity Monitoring	中程度
Trojan:Lambda/DropPoint	Lambda	Lambda Network Activity Monitoring	中程度
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Lambda Network Activity Monitoring	中程度
UnauthorizedAccess:Lambda/TorClient	Lambda	Lambda Network Activity Monitoring	高い
UnauthorizedAccess:Lambda/TorRelay	Lambda	Lambda Network Activity Monitoring	高い
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	低

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	高い
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	可変*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	中程度
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	高い
CredentialAccess:RDS/TorIPCaller.FailedLogin	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	中程度

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	高い
Discovery:RDS/MaliciousIPCaller	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	中程度
Discovery:RDS/TorIPCaller	サポートされている Amazon Aurora および Amazon RDS データベース	RDS ログインアクティビティのモニタリング	中程度
Backdoor:Runtime/C&CActivity.B	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
Backdoor:Runtime/C&CActivity.B!DNS	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
CryptoCurrency:Runtime/BitcoinTool.B	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
CryptoCurrency:Runtime/BitcoinTool.B!DNS	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
DefenseEvasion:Runtime/FilelessExecution	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
DefenseEvasion:Runtime/ProcessInjection.Proc	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
DefenseEvasion:Runtime/ProcessInjection.Ptrace	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
DefenseEvasion:Runtime/PtraceAntiDebugging	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	低

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
DefenseEvasion:Runtime/SuspiciousCommand	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
Execution:Runtime/MaliciousFileExecuted	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
Execution:Runtime/NewBinaryExecuted	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
Execution:Runtime/NewLibraryLoaded	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
Execution:Runtime/SuspiciousCommand	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	変数
Execution:Runtime/SuspiciousTool	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	変数

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Execution:Runtime/ReverseShell	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
Impact:Runtime/AbusedDomainRequest.Reputation	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
Impact:Runtime/BitcoinDomainRequest.Reputation	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
Impact:Runtime/CryptoMinerExecuted	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
Impact:Runtime/MaliciousDomainRequest.Reputation	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
Impact:Runtime/SuspiciousDomainRequest.Reputation	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	低

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
PrivilegeEscalation:Runtime/DockerSocketAccessed	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
PrivilegeEscalation:Runtime/RuncContainerEscape	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
PrivilegeEscalation:Runtime/UserfaultfdUsage	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
Object:S3/MaliciousFile	S3Object	S3 のマルウェア保護	高い

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Trojan:Runtime/BlackholeTraffic	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
Trojan:Runtime/BlackholeTraffic!DNS	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
Trojan:Runtime/DropPoint	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度
Trojan:Runtime/DGADomainRequest.C!DNS	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
Trojan:Runtime/DriveBySourceTraffic!DNS	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
Trojan:Runtime/DropPoint!DNS	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	中程度

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Trojan:Runtime/PhishingDomainRequest!DNS	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
UnauthorizedAccess:Runtime/MetadataDNSRebind	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
UnauthorizedAccess:Runtime/TorClient	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	高い
UnauthorizedAccess:Runtime/TorRelay	インスタンス、EKS クラスター、ECS クラスター、またはコンテナ	Runtime Monitoring	[High] (高)
Backdoor:EC2/C&CActivity.B	EC2	VPC フローログ	[High] (高)
Backdoor:EC2/DenialOfService.Dns	EC2	VPC フローログ	[High] (高)
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC フローログ	[High] (高)

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
Backdoor:EC2/DenialOfService.Udp	EC2	VPC フローログ	[High] (高)
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC フローログ	[High] (高)
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC フローログ	[High] (高)
Backdoor:EC2/Spambot	EC2	VPC フローログ	[Medium] (中)
Behavior:EC2/NetworkPortUnusual	EC2	VPC フローログ	[Medium] (中)
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC フローログ	[Medium] (中)
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC フローログ	[High] (高)
DefenseEvasion:EC2/UnusualDNSResolver	EC2	VPC フローログ	[Medium] (中)

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
DefenseEvasion:EC2/UnusualDoHActivity	EC2	VPC フローログ	[Medium] (中)
DefenseEvasion:EC2/UnusualDoTActivity	EC2	VPC フローログ	[Medium] (中)
Impact:EC2/PortSweep	EC2	VPC フローログ	[High] (高)
Impact:EC2/WinRMBruteForce	EC2	VPC フローログ	[Low] (低)*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC フローログ	[High] (高)
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC フローログ	[Low] (低)*
Recon:EC2/Portscan	EC2	VPC フローログ	[Medium] (中)
Trojan:EC2/BlackholeTraffic	EC2	VPC フローログ	[Medium] (中)
Trojan:EC2/DropPoint	EC2	VPC フローログ	[Medium] (中)

結果タイプ	リソースタイプ	基本データソース/機能	検出結果の重要度
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC フローログ	[Medium] (中)
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC フローログ	[Low] (低)*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	VPC フローログ	[Low] (低)*
UnauthorizedAccess:EC2/TorClient	EC2	VPC フローログ	[High] (高)
UnauthorizedAccess:EC2/TorRelay	EC2	VPC フローログ	[High] (高)

Amazon の検出 GuardDuty 結果の管理

GuardDuty には、結果のソート、保存、管理に役立ついくつかの重要な機能が用意されています。これらの特徴によって、特定の環境に合わせて検出結果を調整したり、重要度の低い検出結果のノイズを減らしたり、特殊な AWS 環境の脅威に焦点を当てたりすることができます。このページのトピックを参照して、これらの機能を使用して の検出結果の値を増やす方法を理解 GuardDutyしてください。

トピック:

[要約] ダッシュボード

コンソールで使用できる GuardDuty概要ダッシュボードのコンポーネントについて説明します。

検出結果のフィルタリング

指定した基準に基づいて GuardDuty 結果をフィルタリングする方法について説明します。

抑制ルール

サプレッションルールを使用して に GuardDuty アラートを送信する検出結果を自動的にフィルタリングする方法について説明します。抑制ルールは、フィルターに基づいて検出結果を自動的にアーカイブします。

信頼できる IP リストと 脅威リストの使用

パブリックにルーティング可能な IP アドレスに基づいて、IP リストと脅威リストを使用して GuardDuty モニタリングスコープをカスタマイズします。信頼できる IP リストは、信頼できると思われる IP から非 DNS の検出結果が生成されないようにします。一方、Threat Intel Lists は、ユーザー定義 IP からのアクティビティを GuardDuty から警告します。 IPs

検出結果のエクスポート

生成された検出結果を Amazon S3 バケットにエクスポートして、 で 90 日間の検出結果保持期間を経過したレコードを維持できるようにします GuardDuty。この履歴データを使用して、アカウント内の潜在的な疑わしいアクティビティを追跡し、推奨される修復ステップが成功したかどうかを評価します。

Amazon CloudWatch Events を使用した GuardDuty 結果へのカスタムレスポンスの作成

Amazon CloudWatch イベントを通じて GuardDuty 検出結果の自動通知を設定します。また、CloudWatch イベントを通じて他のタスクを自動化して、検出結果への対応に役立てることもできます。

Malware Protection for EC2 スキャン中にリソースをスキップする CloudWatch ログと理由を理解する

EC2 の GuardDuty Malware Protection の CloudWatch ログを監査する方法と、影響を受けた Amazon EC2 インスタンスまたは Amazon EBS ボリュームがスキャンプロセス中にスキップされた理由について説明します。

Malware Protection for EC2 GuardDuty での誤検出の報告

GuardDuty Malware Protection for EC2 での誤検出エクスペリエンスと、誤検出の脅威検出を報告する方法について説明します。

[要約] ダッシュボード

サマリーダッシュボードには、 GuardDuty 現在の地域で発生した調査結果を集約して表示できます AWS アカウント 。現在、ダッシュボードでは最大 5,000 件の検出結果をサポートしています。ただし、すべての結果の詳細は、 GuardDuty コンソールの [Findings] ページ、GetFindingsListFindingsまたはのいずれかを使用して表示できます。

> **Note**
>
> 調査結果の概要は、 GuardDuty コンソール https://console.aws.amazon.com/guardduty/ でのみ参照できます。

以下のセクションは、ダッシュボードにアクセスしてそのコンポーネントを理解するのに役立ちます。

コンテンツ

- [要約] ダッシュボードへのアクセス
- [要約] ダッシュボードについて
- [要約] ダッシュボードのフィードバックを送信する

[要約] ダッシュボードへのアクセス

GuardDuty コンソールの Summary ダッシュボードには、現在の地域で生成された最大 5,000 GuardDuty 件の調査結果がまとめて表示されます。

[要約] ダッシュボードにアクセスするには

1. https://console.aws.amazon.com/guardduty/ GuardDuty でコンソールを開きます。
2. ナビゲーションペインで 概要 を選択します。コンソールを開くと、 GuardDuty サマリーダッシュボードが表示されます。
3. デフォルトでは、同日、つまり [今日] の概要が表示されます。 GuardDutyコンソールには、過去 2 日間、過去 7 日間、過去 30 日間の概要を表示するオプションがあります。デフォルトの時間範囲を変更するには、[要約] ペインの上にあるドロップダウンからいずれかのオプションを選択します。
4. データをフィルタリングする

   - [最も多い検出結果を含むアカウント]、[最も多い検出結果を含むリソース]、および [最も低頻度の検出結果] ウィジェットを使用すると、検出結果の重要度に基づいてデータをフィルタリングできます。
   - [最も多い検出結果を含むリソース] ウィジェットでは、影響を受ける可能性のあるリソースタイプに基づいてデータをフィルタリングするのにも役立ちます。

     メンバーアカウントで、自分のアカウントに属する、影響を受ける可能性のあるリソースの詳細を確認できます。 GuardDuty 管理者アカウントで、影響を受ける可能性のあるリソースの詳細を確認したい場合は、 GuardDuty 関連するメンバーアカウントの認証情報を使用してコンソールを開きます。
5. 保護プランの適用範囲

   保護プランの適用範囲には、 GuardDuty 組織内で有効になっているメンバーアカウントの数が表示されます。 GuardDuty 統計情報は委任された管理者にのみ表示されます。

[要約] ダッシュボードについて

[要約] ダッシュボードには、集計されたデータが次のセクションに表示されます。要約を確認して理解する前に、コンソールの上部にあるリージョンセレクターから希望の AWS リージョン が選択されていることを確認してください。また、[要約] ペインの上にあるドロップダウンメニューから、希

望の時間範囲を選択してください。選択したパラメータで検出結果が生成されなかった場合、どのウィジェットでもデータは利用できません。

最大 5,000 件の調査結果のうち、結果が最も多いアカウント、 GuardDuty 調査結果が最も多いリソース、発生件数が最も少ない結果を含む概要ダッシュボードには、上位 5 件の結果に基づくデータが表示されます。より詳細な分析については、 GuardDuty コンソールの調査結果ページを参照してください。

概要

このセクションでは、次のデータを提供します。

- 検出結果の合計: 現在のリージョンでご自身のアカウント内に生成された検出結果の総数を示します。
- 重要度が高い結果: GuardDuty現在の地域で重要度が高い結果の数を示します。
- 検出結果を含むリソース: 検出結果に関連付けられていて、漏洩した可能性があるリソースの数を示します。
- 検出結果のあるアカウント: 少なくとも 1 つの検出結果が生成されたアカウントの数を示します。スタンドアロンアカウントの場合、このフィールドの値は 1 です。

過去 7 日間と過去 30 日の時間範囲について、[要約] ペインでは、それぞれ、週比 (WoW) や前月比 (MoM) で生成された検出結果の差が割合で表示される場合があります。前週または前月に検出結果が得られなかった場合、比較するデータがないため、差の割合は取得できない可能性があります。

GuardDuty 管理者アカウントの場合、これらのフィールドにはすべて、組織内のすべてのメンバーアカウントの要約データが表示されます。

重要度別の検出結果

このセクションでは、選択された時間範囲に対する検出結果の総数が、棒グラフで表示されます。選択された時間範囲内の特定の日付に生成された、重要度が低、中、または高の検出結果の数を表示できます。

最も一般的な検出結果タイプ

このセクションでは、現在の地域で生成された最大 5,000 件の結果の中から、 GuardDuty よく見られる調査結果のトップ 5 種類を円グラフで示します。この円グラフでは、各セクターにカーソルを合わせると、次のデータが表示されます。

- 検出結果数: 選択された時間範囲内でこの検出結果が生成された回数を示します。
- 重要度: 検出結果の重要度レベル (「中」や「高」など) を示します。
- 割合: この検出結果タイプの割合を円グラフで示します。
- 最終生成: この検出結果タイプが最後に生成されてからどれくらいの時間が経過したかを示します。

検出結果が最も多いアカウント

このセクションでは、次のデータを提供します。

- アカウント:結果が生成された場所の AWS アカウント ID を示します。
- 検出結果数: このアカウント ID の検出結果が生成された回数を示します。
- 最終生成: このアカウント ID の検出結果タイプが最後に生成されてからどれくらいの時間が経過したかを示します。
- 重要度高: デフォルトでは、重要度の高い検出結果タイプのデータが表示されます。このフィールドに指定できるオプションは、[重要度高]、[重要度中]、および [すべての重要度] です。

検出結果を含むリソース

このセクションでは、次のデータを提供します。

- リソース: 影響を受ける可能性のあるリソースタイプを示します。このリソースがアカウントに属している場合は、クイックリンクにアクセスしてリソースの詳細を表示できます。 GuardDuty 管理者アカウントの場合、 GuardDuty そのリソースが属するメンバーアカウントの認証情報を使用してコンソールにアクセスすると、影響を受ける可能性のあるリソースの詳細を確認できます。
- アカウント:このリソースが属する AWS アカウント ID を示します。
- 検出結果回数: このリソースが検出結果に関連付けられた回数を示します。
- 最終生成: このリソースに関連付けられた検出結果タイプが最後に生成されてからどれくらいの時間が経過したかを示します。
- すべてのリソースタイプ: デフォルトでは、すべてのリソースタイプのデータが表示されます。ドロップダウンを使用して、インスタンスAccessKey、Lambda などの特定のリソースタイプのデータを表示できます。
- 重要度高: デフォルトでは、重要度の高い検出結果タイプのデータが表示されます。ドロップダウンを使用すると、他の重要度レベルのデータを表示できます。選択できるオプションは、[重要度高]、[重要度中]、および [すべての重要度] です。

最も少ない検出結果

このセクションでは、ご使用の環境ではあまり生成されない検出タイプの詳細を説明します。 AWS このインサイトは、環境内の新たな脅威パターンを調査して対策を講じるのに役立ちます。この表には次のデータが表示されます。

- 検出結果タイプ: 検出結果タイプ名を示します。
- 検出結果数: 選択された時間範囲でこのタイプの検出結果が生成された回数を示します。
- 最終生成: この検出結果タイプが最後に生成されてからどれくらいの時間が経過したかを示します。
- 重要度高: デフォルトでは、重要度の高い検出結果タイプのデータが表示されます。このフィールドに指定できるオプションは、[重要度高]、[重要度中]、および [すべての重要度] です。

保護プランの適用範囲

このセクションには、お客様の組織に属し、現在で 1 つ以上の機能および追加機能 (該当する場合) の設定を有効にしているアクティブなメンバーアカウントの数が表示されます AWS リージョン。

組織内のメンバーアカウントの統計情報を表示できるのは、 GuardDuty 委任された管理者のみです。機能が設定されていない場合は、「アクション」列の「設定」を選択します。

AWS 新しい組織を作成すると、組織全体の統計が生成されるまでに最大 24 時間かかることがあります。

[要約] ダッシュボードのフィードバックを送信する

GuardDuty サマリーダッシュボードの使いやすさ、機能、パフォーマンスに関するフィードバックを提供することをお勧めします。これはダッシュボードの改善につながります。

概要ダッシュボードにフィードバックをするには

1. https://console.aws.amazon.com/guardduty/ GuardDuty でコンソールを開きます。
2. ナビゲーションペインで 概要 を選択します。 GuardDutyコンソールを開くと、サマリーダッシュボードが表示されます。
3. ダッシュボードの右上隅にある [フィードバック] を選択します。フォームが開きます。フィードバックを入力したら、[送信] を選択します。

検出結果のフィルタリング

検出結果フィルターを使用すると、指定した条件に一致する検出結果を表示し、一致しない検出結果を除外できます。Amazon GuardDuty コンソールを使用して検出結果フィルターを簡単に作成することも、JSON を使用して CreateFilter API で作成することもできます。コンソールでフィルターを作成する方法については、次のセクションを参照してください。これらのフィルターを使用して受信した検出結果を自動的にアーカイブするには、「抑制ルール」を参照してください。

GuardDuty コンソールでのフィルターの作成

検出結果フィルターは、 GuardDuty コンソールを使用して作成およびテストできます。抑制ルールやその後のフィルターオペレーションで使用するためにコンソールを通して作成したフィルターは、保存できます。フィルターは、少なくとも 1 つのフィルター基準で構成されます。その基準は少なくとも 1 つの値と組み合わさった 1 つのフィルター属性で構成されています。

フィルターを作成する際には、次の点に注意してください。

- フィルターでは、ワイルドカードを使用できません。
- 特定のフィルターのための基準として、最少 1 から最大 50 までの属性を指定できます。
- カウント ID などの属性値をフィルタリングするための [equal to] (等しい) または [not equal to] (等しくない) の条件を使用しする最合、大場 50 個の値を指定できます。
- 各フィルター基準の属性は AND 演算子として評価されます。同じ属性の複数の値は AND/OR として評価されます。

検出結果をフィルタリングするには (コンソール)

1. GuardDuty 結果の表示されたリストの上にフィルター条件を追加を選択します。
2. 展開された属性のリストで、[Account ID] (アカウント ID) または [Action type] (アクションタイプ) など、フィルターの条件として特定したい属性を選択します。

   > **Note**
   >
   > フィルター基準として指定できる属性の一覧については、このページの フィルター属性 の表を参照してください。

3. 表示されたテキストフィールドで選択された各属性の値を指定し、[Apply] (適用) を選択します。

> **Note**
>
> フィルターを適用したら、フィルター名の左側にある黒いドットを選択し、フィルターに一致する検出結果を除外するようにフィルターを変換できます。これにより、選択した属性に対して [not equals] (等しくない) フィルターが実質的に作成されます。

4. 指定された属性とその値 (フィルター条件) をフィルターとして保存するには、[Save] (保存) を選択します。フィルター名と説明を入力し、[Done] (完了) を選択します。

フィルターの属性

API オペレーションを使用してフィルターを作成したり、検出結果を並べ替える場合は、JSON 中でフィルター基準を特定する必要があります。これらのフィルター基準は、検出結果の詳細 JSON と相関します。次の表にフィルター属性のコンソール表示名と、それに対応する JSON フィールド名のリストを表示します。

コンソールフィールド名	JSON フィールド名
アカウント ID	accountId
検出結果 ID	id
リージョン	region
緊急度	severity 検出結果タイプは、検出結果タイプの重要度レベルに基づいてフィルタリングできます。重要度値の詳細については、「」を参照してください GuardDuty 検出結果の重要度レベル。API、AWS CLI、または `severity`で を使用する場合は AWS CloudFormation、数値が割り当てられます。詳細については、「Amazon GuardDuty API リファレンス」のfindingCriteria」を参照してください。
検出結果タイプ	type

コンソールフィールド名	JSON フィールド名
更新時刻	updatedAt
アクセスキー ID	リソースaccessKeyDetails。accessKeyId
プリンシパル ID	resource.accessKeyDetails.principalId
ユーザーネーム	resource.accessKeyDetails.userName
ユーザーのタイプ	resource.accessKeyDetails.userType
IAM インスタンスプロファイル ID	resource.instanceDetails .iamInstanceProfile.id
インスタンス ID	resource.instanceDetails.instanceId
インスタンスイメージ ID	resource.instanceDetails.imageId
インスタンスのタグキー。	resource.instanceDetails.tags.key
インスタンスのタグ値。	resource.instanceDetails.tags.value
IPv6 アドレス	resource.instanceDetails.networkInterfaces.ipv6Addresses
プライベート IPv4 アドレス	resource.instanceDetails.networkInterfaces.privateIpAddressesprivateIpAddress
パブリック DNS 名	resource.instanceDetails.networkInterfaces.publicDnsName
パブリック IP	resource.instanceDetails.networkInterfaces.publicIp
セキュリティグループ ID	resource.instanceDetails.networkInterfaces.securityGroups.groupId
セキュリティグループ名	resource.instanceDetails.networkInterfaces.securityGroups.groupName

コンソールフィールド名	JSON フィールド名
サブネット ID	resource.instanceDetails.networkInterfaces.subnetId
VPC ID	resource.instanceDetails.networkInterfaces.vpcId
Outpost ARN	resource.instanceDetails.outpostARN
リソースタイプ	resource.resourceType
バケット許可	resource.s3BucketDetails.publicAccess.effectivePermission
バケット名	resource.s3BucketDetails.name
バケットタグキー	resource.s3BucketDetails.tags.key
バケットタグ値	resource.s3BucketDetails.tags.value
バケットタイプ	resource.s3BucketDetails.type
アクションタイプ	service.action.actionType
呼び出された API	service.action.awsApiCallAction.api
API 発信者のタイプ	service.action.awsApiCallAction.callerType
API エラーコード	service.action.awsApiCallAction.errorCode
API 発信者の都市	service.action.awsApiCallAction.remoteIpDetails.city.cityName
API 発信者の国	service.action.awsApiCallAction.remoteIpDetails.country.countryName
API 発信者の IPv4 アドレス	service.action.awsApiCallAction.remoteIpDetails.ipAddressV4

コンソールフィールド名	JSON フィールド名
API 発信者 IPv6 アドレス	service.action.awsApiCallAction.remoteIpDetails.ipAddressV6
API 発信者の ASN ID	service.action.awsApiCallAction.remoteIpDetails.organization.asn
API 発信者の ASN 名	service.action.awsApiCallAction.remoteIpDetails.organization.asnOrg
API 発信者のサービス名	service.action.awsApiCallAction.serviceName
DNS リクエストドメイン	service.action.dnsRequestAction.domain
DNS リクエストドメインサフィックス	service.actiondnsRequestAction。domainWithSuffix
ブロック済みのネットワーク接続	service.action.networkConnectionAction.blocked
ネットワーク接続の方向	service.action.networkConnectionAction.connectionDirection
ネットワーク接続のローカルポート	service.action.networkConnectionActionlocalPortDetails.port
ネットワーク接続プロトコル	service.action.networkConnectionAction.protocol
ネットワーク接続の都市	service.action.networkConnectionActionremoteIpDetails.city.cityName
ネットワーク接続の国	service.action.networkConnectionActionremoteIpDetails.country.countryName
ネットワーク接続のリモート IPv4 アドレス	service.action.networkConnectionActionremoteIpDetails.ipAddressV4

コンソールフィールド名	JSON フィールド名
ネットワーク接続リモート IPv6 アドレス	service.action.networkConnectionActionremoteIpDetails.ipAddressV6
ネットワーク接続のリモート IP ASN ID	service.action.networkConnectionActionremoteIpDetails.organization.asn
ネットワーク接続のリモート IP ASN 名	service.action.networkConnectionActionremoteIpDetails.organization.asnOrg
ネットワーク接続のリモートポート	service.action.networkConnectionAction.remotePortDetails.port
関連するリモートアカウント	service.action.awsApiCallActionremoteAccountDetails.Related
Kubernetes API 発信者の IPv4 アドレス	service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV4
Kubernetes API 発信者 IPv6 アドレス	service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV6
Kubernetes 名前空間	service.action.kubernetesApiCallAction.namespace
Kubernetes API 発信者 ASN ID	service.action.kubernetesApiCallAction.remoteIpDetails.organization.asn
Kubernetes API 呼び出しリクエスト URI	service.action.kubernetesApiCallAction.requestUri
Kubernetes API ステータスコード	service.action.kubernetesApiCallAction.statusCode
ネットワーク接続のローカル IPv4 アドレス	service.action.networkConnectionActionlocalIpDetails.ipAddressV4
ネットワーク接続のローカル IPv6 アドレス	service.action.networkConnectionActionlocalIpDetails.ipAddressV6

コンソールフィールド名	JSON フィールド名
[プロトコル]	service.action.networkConnectionAction.protocol
API 呼び出しのサービス名	service.action.awsApiCallAction.serviceName
API 発信者アカウント ID	service.action.awsApiCallAction.remoteAccountDetails.accountId
脅威リスト名	service.additionalInfo。threatListName
リソースロール	service.resourceRole
EKS クラスター名	resource.eksClusterDetails.name
Kubernetes ワークロード名	resource.kubernetesDetails .kubernetesWorkloadDetails.name
Kubernetes ワークロード名前空間	resource.kubernetesDetails .kubernetesWorkloadDetails.namespace
Kubernetes ユーザー名	resource.kubernetesDetails .kubernetesUserDetails.username
Kubernetes コンテナイメージ	resource.kubernetesDetails .kubernetesWorkloadDetails.containers.image
Kubernetes コンテナイメージのプレフィックス	resource.kubernetesDetails .kubernetesWorkloadDetails.containers.imagePrefix
[Scan ID] (スキャン ID)	service.ebsVolumeScanDetails.scanId
EBS ボリュームスキャンの脅威名	service.ebsVolumeScanDetails.scanDetections .threatDetectedByName.threatNames.name
S3 オブジェクトスキャンの脅威名	service.malwareScanDetails.threats.name

コンソールフィールド名	JSON フィールド名
脅威の重要度	service.ebsVolumeScanDetails.scanDetections .threatDetectedByName.threatNames.severity
SHA ファイル	service.ebsVolumeScanDetails.scanDetections .threatDetectedByName.threatNames.filePaths.hash
ECS クラスター名	resource.ecsClusterDetails.name
ECS コンテナイメージ	resource.ecsClusterDetails.taskDetails.containers.image
ECS タスク定義 ARN	resource.ecsClusterDetails.taskDetails.definitionArn
スタンドアロンコンテナのイメージ	resource.containerDetails.image
データベースインスタンス ID	resource.rdsDbInstanceDetails。dbInstanceIdentifier
データベースクラスター ID	resource.rdsDbInstanceDetails。dbClusterIdentifier
データベースエンジン	resource.rdsDbInstanceDetails.engine
データベースユーザー	resource.rdsDbUserDetails.user
データベースインスタンスのタグキー	resource.rdsDbInstanceDetails.tags.key
データベースインスタンスのタグ値	resource.rdsDbInstanceDetails.tags.value
実行可能ファイル SHA-256	service.runtimeDetails.process.executableSha256
プロセス名	service.runtimeDetails.process.name
実行可能ファイルのパス	service.runtimeDetails.process.executablePath

コンソールフィールド名	JSON フィールド名
Lambda 関数の名前	resource.lambdaDetails.functionName
Lambda 関数の ARN	resource.lambdaDetails.functionArn
Lambda 関数タグキー	resource.lambdaDetails.tags.key
Lambda 関数タグ値	resource.lambdaDetails.tags.value
DNS リクエストドメイン	service.actiondnsRequestAction。domainWithSuffix

抑制ルール

抑制ルールは、フィルター属性と値の組み合わせで構成される基準のセットで、指定した条件に一致する新しい検出結果を自動的にアーカイブして検出結果をフィルタリングするために使用する条件のセットのことです。抑制ルールを使用して、重要ではない検出結果、誤検出の検出結果、対応を行わない脅威をフィルタリングすることにより、環境に最も影響があるセキュリティの脅威を認識しやすくなります。

抑制ルールを作成すると、その抑制ルールが適用されている限り、ルールで定義された条件に一致する新しい検出結果が自動的にアーカイブされます。既存のフィルターを使用して抑制ルールを作成したり、定義した新しいフィルターから抑制ルールを作成することもできます。検出結果タイプ全体を抑制するよう抑制ルールを設定したり、特定の検出結果タイプの特定のインスタンスのみを抑制する、よりきめ細かいフィルター条件を定義したりできます。抑制ルールはいつでも編集できます。

抑制された検出結果は AWS Security Hub、、Amazon Simple Storage Service、Amazon Detective、または Amazon に送信されないため EventBridge、Security Hub、サードパーティー SIEM、またはその他のアラートおよびチケット発行アプリケーションを介して検出 GuardDuty 結果を使用する場合、検出結果のノイズレベルが低下します。を有効にした場合GuardDuty EC2 のマルウェア保護、抑制された GuardDuty 検出結果はマルウェアスキャンを開始しません。

GuardDuty は、抑制ルールと一致しても検出結果を生成し続けますが、それらの検出結果はアーカイブされた として自動的にマークされます。アーカイブされた検出結果は 90 GuardDuty 日間 に保存され、その期間中いつでも表示できます。抑制された検出結果を GuardDuty コンソールで表示するには、検出結果テーブルからアーカイブするか、 GuardDuty API を使用して true にservice.archived等しいfindingCriteria基準で ListFindings API を使用します。

> **Note**
>
> マルチアカウント環境では、 GuardDuty 管理者のみが抑制ルールを作成できます。

抑制ルールの一般的ユースケースとその例

次の検出結果タイプには、抑制ルールを適用するための一般的なユースケースがあります。検出結果名を選択すると、その検出結果の詳細が表示されます。ユースケースの説明を確認して、その検出結果タイプの抑制ルールを構築するかどうかを決定します。

> **Important**
>
> GuardDuty では、環境で誤検出を繰り返し特定した検出結果に対してのみ、抑制ルールを事後的に構築することをお勧めします。

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS - VPC のインターネットゲートウェイからではなく、オンプレミスのゲートウェイからインターネットへのトラフィックをルーティングするように VPC ネットワークが設定されている場合に、生成された検出結果を自動的にアーカイブするために抑制ルールを使用します。

  この検出結果が生成されるのは、VPC インターネットゲートウェイ (IGW) からではなく、オンプレミスのゲートウェイから排出され、インターネットトラフィックがルーティングされるように、ネットワークが構成されている場合です。AWS Outposts や VPC VPN 接続などの一般的な構成では、このようにトラフィックがルーティングされる可能性があります これが予想される動作である場合は、抑制ルールを使用して、2 つのフィルター条件で構成されるルールを作成することをお勧めします。1 つ目の条件では、[finding type] (結果タイプ) に `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` を使用します。2 番目のフィルター条件は、オンプレミスインターネットゲートウェイの IP アドレスまたは CIDR 範囲を持つ [API caller IPv4 address] (API 発信者の IPv4 アドレス) です。次の例は、API 発信者の IP アドレスに基づいてこの検出結果タイプを抑制するために使用するフィルターを示しています。

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
 API caller IPv4 address: 198.51.100.6
```

> **Note**
>
> 複数の API 発信者の IP を含めるには、それぞれに新しい API 発信者 IPv4 アドレスフィルターを追加します。

- Recon:EC2/Portscan - 脆弱性評価アプリケーションを使用する場合に、検出結果を自動的にアーカイブするために抑制ルールを使用します。

  抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `Recon:EC2/Portscan` という値を使用します。2 番目のフィルター条件は、これらの脆弱性評価ツールをホストする 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可能な条件に応じて、[Instance image ID] (インスタンスイメージ ID) 属性または [Tag] (タグ) 値の属性のいずれかを使用できます。次の例は、特定の AMI を持つインスタンスに基づいてこの検出結果タイプを抑制するために使用するフィルターを示しています。

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce - 踏み台インスタンスをターゲットとする場合に、検出結果を自動的にアーカイブするために抑制ルールを使用します。

  ブルートフォース試行のターゲットが踏み台ホストの場合、これは AWS 環境に対して予想される動作を表す可能性があります。このような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `UnauthorizedAccess:EC2/SSHBruteForce` という値を使用します。2 番目のフィルター条件は、要塞ホストとして機能する 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可能な条件に応じて、[Instance image ID] (インスタンスイメージ ID) 属性または [Tag] (タグ) 値の属性のいずれかを使用できます。次の例は、特定のタグ値を持つインスタンスに基づいてこの検出結果タイプを抑制するために使用するフィルターを示しています。

  ```
  Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
  ```

- Recon:EC2/PortProbeUnprotectedPort - 意図的に公開しているインスタンスをターゲットとする場合に、検出結果を自動的にアーカイブするために抑制ルールを使用します。

  インスタンスがウェブサーバーをホストしている場合など、インスタンスが意図的に公開されている場合があります。ご使用の AWS 環境でその場合は、この検出結果の抑制ルールを設定するこ

とをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、[Finding type] (結果タイプ) 属性に `Recon:EC2/PortProbeUnprotectedPort` という値を使用します。2 番目のフィルター条件は、要塞ホストとして機能する 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可能な条件に応じて、[Instance image ID] (インスタンスイメージ ID) 属性または [Tag] (タグ) 値の属性のいずれかを使用できます。次の例は、コンソール内の特定のタグキーを持つインスタンスに基づいてこの検出結果タイプを抑制するために使用するフィルターを示しています。

```
Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
```

Runtime Monitoring の検出結果の推奨抑制ルール

- PrivilegeEscalation:Runtime/DockerSocketAccessed はコンテナ内のプロセスが Docker ソケットと通信するときに生成されます。環境内に、正当な理由で Docker ソケットにアクセスする必要があるコンテナが存在する可能性があります。このようなコンテナからアクセスすると、PrivilegeEscalation:Runtime/DockerSocketAccessed 検出結果が生成されます。ご使用の AWS 環境でこれが当てはまる場合は、この検出結果タイプの抑制ルールを設定することをお勧めします。1 つ目の条件では、値が `PrivilegeEscalation:Runtime/DockerSocketAccessed` に等しい [検出結果タイプ] フィールドを使用する必要があります。2 番目のフィルター条件は、生成された検出結果のプロセスの `executablePath` と同じ値を持つ [実行可能ファイルのパス] フィールドです。別の方法として、2 番目のフィルター条件では、生成された検出結果のプロセスの `executableSha256` と同じ値を持つ [実行可能ファイル SHA-256] フィールドを使用できます。
- Kubernetes クラスターは、独自の DNS サーバーを `coredns` などのポッドとして実行します。したがって、ポッドからの DNS ルックアップごとに、 は 2 つの DNS イベント GuardDuty をキャプチャします。1 つはポッドから、もう 1 つはサーバーポッドから取得します。これにより、以下の DNS 検出結果に重複が生じる可能性があります。
  - Backdoor:Runtime/C&CActivity.B!DNS
  - CryptoCurrency:Runtime/BitcoinTool.B!DNS
  - Impact:Runtime/AbusedDomainRequest.Reputation
  - Impact:Runtime/BitcoinDomainRequest.Reputation
  - Impact:Runtime/MaliciousDomainRequest.Reputation
  - Impact:Runtime/SuspiciousDomainRequest.Reputation
  - Trojan:Runtime/BlackholeTraffic!DNS

- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

重複した検出結果には、DNS サーバーポッドに対応するポッド、コンテナ、プロセスの詳細が含まれます。これらのフィールドを使用して、重複検出結果を抑制する抑制ルールをセットアップできます。最初のフィルター条件では、このセクションで前述した検出結果リストの DNS 検出結果タイプと同じ値の [検出結果タイプ] フィールドを使用する必要があります。2 つ目のフィルター条件は、お使いの DNS サーバー `executablePath` と同じ値の [実行可能ファイルのパス] か、生成された検出結果の DNS サーバー `executableSHA256` と同じ値の [実行可能ファイル SHA-256] のいずれかです。オプションの 3 番目のフィルター条件として、生成された検出結果に含まれる DNS サーバーポッドのコンテナイメージと同じ値の [Kubernetes コンテナイメージ] フィールドを使用できます。

抑制ルールを作成する

任意のアクセス方法を選択して、 GuardDuty 検出結果タイプの抑制ルールを作成します。

Console

GuardDuty コンソールを使用して、抑制ルールを視覚化、作成、管理できます。抑制ルールはフィルターと同じ方法で生成され、既存の保存済みフィルターを抑制ルールとして使用できます。フィルター作成の詳細については、「検出結果のフィルタリング」を参照してください。

コンソールを使用して抑制ルールを作成するには

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. [Findings] (検出結果) ページで、[Suppress findings] (検出結果の抑制) をクリックして、抑制ルールパネルを開きます。
3. フィルター基準メニューを開くには、[Add filter criteria] (フィルター基準を追加) に **`filter criteria`** を入力します。リストから基準を選択できます。選択した基準の有効な値を入力します。

> **Note**
>
> 有効な値を判断するには、検出結果テーブルを表示して、抑制する結果を選択します。検出結果パネルで詳細を確認します。

複数のフィルター基準を追加して、抑制したい検出結果のみがテーブルに表示されるようにすることができます。

4. 抑制ルールの [Name] (名前) と [Description] (説明) を入力します。有効な文字は、英数字、ピリオド (.)、ダッシュ (-)、アンダースコア (_)、空白スペースです。
5. [保存] を選択します。

また、既存の保存済みフィルターから抑制ルールを作成できます。フィルター作成の詳細については、「検出結果のフィルタリング」を参照してください。

保存済みフィルターから抑制ルールを作成するには、次の手順を実行します。

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. [Findings] (検出結果) ページで、[Suppress findings] (検出結果の抑制) をクリックして、抑制ルールパネルを開きます。
3. [Saved rules] (保存済みのルール) ドロップダウンの一覧から、保存したフィルターを選択します。
4. 新しいフィルター基準を追加することもできます。フィルター基準を追加する必要がない場合は、この手順をスキップします。

   フィルター基準メニューを開くには、[Add filter criteria] (フィルター基準を追加) に **filter criteria** を入力します。リストから基準を選択できます。選択した基準の有効な値を入力します。

   > **Note**
   >
   > 有効な値を判断するには、検出結果テーブルを表示して、抑制する結果を選択します。検出結果パネルで詳細を確認します。

5. 抑制ルールの [Name] (名前) と [Description] (説明) を入力します。有効な文字は、英数字、ピリオド (.)、ダッシュ (-)、アンダースコア (_)、空白スペースです。

6. [保存] を選択します。

API/CLI

API を使用して抑制ルールを作成するには

1. 抑制ルールは、CreateFilter API を使用して作成できます。これを行うには、次に示す例の形式に従って JSON ファイルでフィルター条件を指定します。次の例では、test.example.com ドメインへの DNS リクエストが行われた未アーカイブの重要度の低い検出結果を抑制します。重要度が中の検出結果の場合、入力リストは ["4", "5", "7"] になります。重要度が高の検出結果の場合、入力リストは ["6", "7", "8"] になります。リスト内の任意の 1 つの値に基づいてフィルターすることもできます。

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

JSON のフィールド名とそれに相当するコンソールのフィールド名の一覧については、「フィルターの属性」を参照してください。

フィルター基準をテストするには、ListFindings API で同じ JSON 基準を使用し、正しい検出結果が選択されていることを確認します。を使用してフィルター条件をテストするには、独自の detectorId と .json ファイルを使用して例 AWS CLI に従います。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. 抑制ルールとして使用するフィルターを CreateFilter API を使用してアップロードするか、AWS CLI で次の例に従って独自のディテクター ID、抑制ルール名、.json ファイルを使用してアップロードします。

   アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

   ```
   aws guardduty create-filter --action ARCHIVE --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
    file://criteria.json
   ```

ListFilter API を使用して、プログラムでフィルターのリストを表示できます。GetFilter API にフィルター名を指定すると、個々のフィルターの詳細を表示できます。UpdateFilter API を使用してフィルターを更新するか、DeleteFilter API を使用してフィルターを削除します。

抑制ルールを削除する

任意のアクセス方法を選択して、 GuardDuty 検出結果タイプの抑制ルールを削除します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. [Findings] (検出結果) ページで、[Suppress findings] (検出結果の抑制) をクリックして、抑制ルールパネルを開きます。

3. [Saved rules] (保存済みのルール) ドロップダウンの一覧から、保存したフィルターを選択します。
4. [ルールを削除] を選択します。

API/CLI

DeleteFilter API を実行します。特定のリージョンのフィルター名と関連付けられたディテクター ID を指定します。

または、*##*の でフォーマットされた値を置き換えることで、次の AWS CLI 例を使用することもできます。

```
aws guardduty delete-filter --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

信頼できる IP リストと 脅威リストの使用

Amazon は、VPC フローログ、 AWS CloudTrail イベントログ、DNS ログを分析して処理することで、 AWS 環境のセキュリティを GuardDuty モニタリングします。独自の信頼された IPs リストから信頼された IP のアラートを停止し、独自の脅威リストから既知の悪意のある IPs をアラート GuardDuty するように を設定することで、このモニタリング範囲をカスタマイズできます。

信頼できる IP リストと脅威リストは、パブリックにルーティング可能な IP アドレスを宛先とするトラフィックにのみ適用されます。リストの効果はすべての VPC フローログと CloudTrail 検出結果に適用されますが、DNS 検出結果には適用されません。

GuardDuty は、次のタイプのリストを使用するように設定できます。

信頼できる IP リスト

信頼できる IP リストは、 AWS インフラストラクチャやアプリケーションとの安全な通信のために信頼できる IP アドレスで構成されます。 は、信頼できる IP GuardDuty リストの IP アドレス

の VPC フローログや CloudTrail 検出結果を生成しません。単一の信頼できる IP リストには、最大 2000 の IP アドレスと CIDR 範囲を含めることができます。どの時点でも、信頼できる IP リストのアップロード数は各リージョンの AWS アカウントにつき 1 つに限られます。

脅威 IP リスト

脅威リストは、悪意のある既知の IP アドレスで構成されます。このリストは、サードパーティの脅威インテリジェンスによって提供されるか、あるいは組織専用に特別に生成することができます。は、潜在的に疑わしいアクティビティのために検出結果を生成するだけでなく、これらの脅威リストに基づいて検出結果 GuardDuty も生成します。最大 250,000 個の IP アドレスと CIDR 範囲を 1 つの脅威リストに含めることができます。 は、脅威リスト内の IP アドレスと CIDR 範囲を含むアクティビティのみに基づいて検出結果 GuardDuty を生成します。検出結果はドメイン名に基づいて生成されません。どの時点でも、各リージョンごとに AWS アカウント ごとに最大 6 つの脅威リストをアップロードできます。

> **Note**
>
> 信頼できる IP リストと脅威リストの両方に同じ IP を含めると、それは最初に信頼できる IP リストによって処理され、検出結果は生成されません。

マルチアカウント環境では、 GuardDuty 管理者アカウントアカウントのユーザーのみが、信頼できる IP リストと脅威リストを追加および管理できます。管理者アカウントによってアップロードされる信頼された IP リストと脅威リストは、メンバーアカウントの GuardDuty 機能に適用されます。つまり、メンバーアカウントでは、管理者アカウントの脅威リストから既知の悪意のある IP アドレスを含むアクティビティに基づいて検出 GuardDuty 結果を生成し、管理者アカウントの信頼できる IP リストから IP アドレスを含むアクティビティに基づいて検出結果を生成しません。詳細については、「Amazon での複数のアカウントの管理 GuardDuty」を参照してください。

リストフォーマット

GuardDuty は、次の形式のリストを受け入れます。

信頼できる IP リストまたは脅威 IP リストをホストする各ファイルの最大サイズは 35 MB です。信頼できる IP リストと脅威 IP リストで、IP アドレスおよび CIDR 範囲を 1 行に 1 つずつ表示する必要があります。IPv4 アドレスのみ受け入れられます。

- プレーンテキスト (TXT)

このフォーマットは、CIDR ブロックと個々の IP アドレスの両方をサポートします。次のサンプルリストはプレーンテキスト (TXT) フォーマットを使用しています。

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- 脅威情報構造化記述形式 (STIX)

  このフォーマットは、CIDR ブロックと個々の IP アドレスの両方をサポートします。次のサンプルリストは STIX フォーマットを使用しています。

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
```

```
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- Open Threat Exchange (OTX)™ CSV

  このフォーマットは、CIDR ブロックと個々の IP アドレスの両方をサポートします。次のサンプルリストは OTX™ CSV フォーマットを使用しています。

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye™ iSIGHT 脅威インテリジェンス CSV

このフォーマットは、CIDR ブロックと個々の IP アドレスの両方をサポートします。次のサンプルリストは FireEye™ CSV フォーマットを使用しています。

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,
 subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,
 md5, sha1, sha256, description, fileType, packer, userAgent, registry,
 fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,
 networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,
 url, malwareFamily, malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- Proofpoint™ ET Intelligence Feed CSV

  このフォーマットは、個々の IP アドレスのみをサポートします。次のサンプルリストは Proofpoint CSV フォーマットを使用しています。ports パラメータはオプションです。ポートをスキップする場合は、末尾のカンマ (,) を必ず残してください。

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVault™ 評価フィード

このフォーマットは、個々の IP アドレスのみをサポートします。次のサンプルリストは AlienVault フォーマットを使用しています。

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

信頼できる IP リストと 脅威リストをアップロードするために必要な許可

さまざまな IAM ID には、 で信頼できる IP リストと脅威リストを操作するための特別なアクセス許可が必要です GuardDuty。AmazonGuardDutyFullAccess マネージドポリシーがアタッチされている ID のみがアップロードされた信頼できる IP リストと脅威リストの名前を変更および無効化できます。

さまざまな ID に、信頼できる IP リストと脅威リストの操作 (名前の変更および非アクティブ化に加えて、リストの追加、アクティブ化、削除や、リストの場所または名前の更新が含まれます) を行うためのフルアクセスを付与するには、次のアクションがユーザー、グループ、またはロールにアタッチされた許可ポリシーに存在することを確認してください。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> これらのアクションは AmazonGuardDutyFullAccess マネージドポリシーに含まれていません。

信頼できる IP リストと脅威リストに対するサーバー側の暗号化の使用

GuardDuty では、SSE-AES256 と SSE-KMS のリストの暗号化タイプがサポートされています。SSE-C はサポートされていません。S3 サーバー側暗号化の使用の詳細については、「サーバーサイドの暗号化でデータを保護する」を参照してください。

リストがサーバー側の暗号化 SSE-KMS を使用して暗号化されている場合は、リストをアクティブ化するためにファイルを復号化するAWSServiceRoleForAmazonGuardDutyアクセス許可を GuardDuty サービスにリンクされたロールに付与する必要があります。KMS キーポリシーに次のステートメントを追加し、アカウント ID を独自のステートメントに置き換えます。

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

信頼されている IP リストまたは脅威 IP リストの追加とアクティブ化

次のアクセス方法のいずれかを選択して、信頼されている IP リストまたは脅威 IP リストを追加してアクティブ化します。

Console

(オプション) ステップ 1: リストの場所の URL を取得する

1. https://console.aws.amazon.com/s3/でAmazon S3 コンソールを開きます。
2. ナビゲーションペインで、バケットを選択します。
3. 追加する特定のリストを含む Amazon S3 バケット名を選択します。
4. オブジェクト (リスト) 名を選択すると、その詳細が表示されます。
5. [プロパティ] タブで、このオブジェクトの S3 URI をコピーします。

ステップ 2: 信頼されている IP リストまたは脅威リストを追加する

> **Important**
>
> デフォルトでは、どの時点においても、持つことのできる信頼されている IP リストは 1 つのみです。同様に、最大 6 つの脅威リストを作成できます。

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[リスト] を選択します。
3. [List management] (リスト管理) ページで、[Add a trusted IP list] (信頼されている IP リストの追加) または [Add a threat list] (脅威リストを追加) を選択します。
4. 選択内容に基づいて、ダイアログボックスが表示されます。次のステップを実行します。

   a. [リスト名] で、リストの名前を入力します。

      リストの命名に関する制約 – リストの名前には、小文字、大文字、数字、ダッシュ (-)、アンダースコア (_) を含めることができます。

   b. [場所] で、リストをアップロードした場所を指定します。まだ持っていない場合は、「Step 1: Fetching location URL of your list」を参照してください。

      場所の URL の形式

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3-aws-region.amazonaws.com/file.txt
      - s3://bucket.name/file.txt

   c. [I agree] (同意します) チェックボックスをオンにします。

   d. [Add list] (リストを追加) を選択します。デフォルトでは、追加されたリストの [ステータス] は [非アクティブ] です。リストを有効にするには、リストをアクティブ化する必要があります。

ステップ 3: 信頼されている IP リストまたは脅威リストをアクティブ化する

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

2. ナビゲーションペインで、[リスト] を選択します。
3. [リスト管理] ページで、アクティブ化するリストを選択します。
4. [アクション] を選択し、[アクティブ化] を選択します。リストが有効になるまでに最大 15 分かかる場合があります。

API/CLI

信頼されている IP リストの場合

- CreateIPSet を実行します。この信頼されている IP リストを作成するメンバーアカウントの `detectorId` を必ず指定してください。

  リストの命名に関する制約 – リストの名前には、小文字、大文字、数字、ダッシュ (-)、アンダースコア (_) を含めることができます。

  - または、次の AWS Command Line Interface コマンドを実行してこれを行うこともできます。このとき、`detector-id` を、信頼されている IP リストを更新するメンバーアカウントのディテクター ID に置き換えてください。

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

脅威リストの場合

- CreateThreatIntelSet を実行します。この脅威リストを作成するメンバーアカウントの `detectorId` を必ず指定してください。
  - または、次の AWS Command Line Interface コマンドを実行してこれを行うことができます。脅威リストを作成するメンバーアカウントの `detectorId` を必ず指定してください。

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

> **Note**
>
> IP リストをアクティブ化または更新した後、リストの同期に最大 15 分かかる GuardDuty 場合があります。

信頼できる IP リストと脅威リストの更新

リストの名前、または既に追加およびアクティブ化されているリストに追加された IP アドレスを更新できます。リストを更新する場合は、 がリストの最新バージョン GuardDuty を使用するには、リストを再度アクティブ化する必要があります。

いずれかのアクセス方法を選択して、信頼されている IP リストまたは脅威リストを更新します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[リスト] を選択します。
3. [リスト管理] ページで、更新する信頼されている IP セットまたは脅威リストを選択します。
4. [Actions] (アクション) を選択して、[Edit] (編集) を選択します。
5. [リストを更新] ダイアログボックスで、必要に応じて情報を更新します。

   リストの命名に関する制約 – リストの名前には、小文字、大文字、数字、ダッシュ (-)、アンダースコア (_) を含めることができます。
6. [同意します] チェックボックスをオンにし、[リストを更新] を選択します。[ステータス] 列の値が [非アクティブ] に変わります。
7. 更新されたリストを再アクティブ化する

   a. [リスト管理] ページで、再びアクティブ化するリストを選択します。
   b. [アクション] を選択し、[アクティブ化] を選択します。

API/CLI

1. UpdateIPSet を実行して、信頼されている IP リストを更新します。
   - あるいは、次の AWS CLI コマンドを実行して信頼されている IP リストを更新し、`detector-id` を、信頼されている IP リストを更新するメンバーアカウントのディテクター ID に置き換えることもできます。

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
activate
```

2. UpdateThreatIntelSet を実行して、脅威リストを更新する
   - あるいは、次の AWS CLI コマンドを実行して脅威リストを更新し、detector-id を、脅威リストを更新するメンバーアカウントのディテクター ID に置き換えることもできます。

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

信頼されている IP リストまたは脅威リストの非アクティブ化または削除

(コンソールを使用して) 信頼されている IP リストもしくは脅威リストを削除するか、または (API/CLI を使用して) 非アクティブ化する、いずれかのアクセス方法を選択します。

Console

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[リスト] を選択します。
3. [リスト管理] ページで、削除するリストを選択します。
4. [アクション] を選択し、[削除] を選択します。
5. アクションを確認して、[削除] を選択します。特定のリストはテーブルで使用できなくなります。

API/CLI

1. 信頼されている IP リストの場合

   UpdateIPSet を実行して、信頼されている IP リストを更新します。
   - あるいは、次の AWS CLI コマンドを実行して信頼されている IP リストを更新し、detector-id を、信頼されている IP リストを更新するメンバーアカウントのディテクター ID に置き換えることもできます。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、ListDetectors API を実行します。

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
no-activate
```

2. 脅威リストの場合

   UpdateThreatIntelSet を実行して、脅威リストを更新する

   - あるいは、次の AWS CLI コマンドを実行して信頼されている IP リストを更新し、detector-id を、脅威リストを更新するメンバーアカウントのディテクター ID に置き換えることもできます。

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --no-activate
```

検出結果のエクスポート

GuardDuty は、生成された検出結果を 90 日間保持します。 はアクティブな検出結果を Amazon EventBridge () に GuardDuty エクスポートしますEventBridge。必要に応じて、生成された検出結果を Amazon Simple Storage Service (Amazon S3) バケットにエクスポートできます。これにより、アカウント内の潜在的に疑わしいアクティビティの履歴データを追跡し、推奨される修復ステップが成功したかどうかを評価するのに役立ちます。

が GuardDuty 生成する新しいアクティブな検出結果は、検出結果が生成されてから約 5 分以内に自動的にエクスポートされます。アクティブな検出結果の更新を にエクスポートする頻度を設定できます EventBridge。選択した頻度は、既存の検出結果の新しい出現を 、S3 バケット (設定されている場合 ） EventBridge、Detective (統合されている場合) にエクスポートする場合に適用されます。が既存の検出結果の複数の出現を GuardDuty 集約する方法については、「」を参照してくださいGuardDuty 結果の集約。

検出結果を Amazon S3 バケットにエクスポートするように設定する場合、 は AWS Key Management Service （ AWS KMS) GuardDuty を使用して S3 バケットの検出結果データを暗号化し

ます。そのためには、S3 バケットと AWS KMS キーにアクセス許可を追加して、 GuardDuty がそれらを使用してアカウントで検出結果をエクスポートできるようにする必要があります。

内容

考慮事項

検出結果をエクスポートするための前提条件とステップに進む前に、次の主要な概念を考慮してください。

- エクスポート設定はリージョン別 – を使用する各リージョンでエクスポートオプションを設定する必要があります GuardDuty。
- 異なる AWS リージョン （ クロスリージョン) の Amazon S3 バケットに結果をエクスポートする – 次のエクスポート設定 GuardDuty をサポートします。
  - Amazon S3 バケットまたはオブジェクト、 AWS KMS キーは同じ に属している必要がありますAWS リージョン。
  - 商用リージョンで生成された検出結果については、これらの検出結果を任意の商用リージョンの S3 バケットにエクスポートすることを選択できます。ただし、これらの検出結果をオプトインリージョンの S3 バケットにエクスポートすることはできません。
  - オプトインリージョンで生成された検出結果については、これらの検出結果を生成されたのと同じオプトインリージョンまたは任意の商用リージョンにエクスポートすることを選択できます。ただし、あるオプトインリージョンから別のオプトインリージョンに結果をエクスポートすることはできません。
- 検出結果をエクスポートするアクセス許可 – アクティブな検出結果をエクスポートするための設定を構成するには、S3 バケットにオブジェクトのアップロード GuardDuty を許可するアクセス許可が必要です。また、 GuardDuty が検出結果の暗号化に使用できる AWS KMS キーも必要です。
- アーカイブされた検出結果はエクスポートされない – デフォルトの動作は、抑制された検出結果の新しいインスタンスを含むアーカイブされた検出結果はエクスポートされないことです。

GuardDuty 結果がアーカイブされた として生成される場合は、アーカイブを解除する必要があります。これにより、フィルター検出結果のステータスがアクティブに変更されます。 の設定方法に基づいて、アーカイブされていない既存の検出結果に更新が GuardDuty エクスポートされますステップ 5 – 検出結果のエクスポート頻度。

- GuardDuty 管理者アカウントは、関連付けられたメンバーアカウントで生成された結果をエクスポートできます。管理者アカウントでエクスポートの結果を設定すると、同じリージョンで生成された関連付けられたメンバーアカウントからのすべての結果も、管理者アカウント用に設定したのと同じ場所にエクスポートされます。詳細については、「GuardDuty 管理者アカウントとメンバーアカウントの関係を理解する」を参照してください。

ステップ 1 — 検出結果をエクスポートするために必要なアクセス許可

検出結果をエクスポートするための設定を行うときは、検出結果を保存できる Amazon S3 バケットと、データの暗号化に使用する AWS KMS キーを選択します。 GuardDuty 検出結果をエクスポートする設定を正常に設定するには、 アクションのアクセス許可に加えて、以下のアクションに対するアクセス許可も必要です。

- `s3:GetBucketLocation`
- `s3:PutObject`
- `s3:ListBucket`

ステップ 2 – KMS キーにポリシーをアタッチする

GuardDuty は、 を使用してバケット内の検出結果データを暗号化します AWS Key Management Service。設定を正常に設定するには、まず KMS キーを使用するアクセス GuardDuty 許可を付与する必要があります。KMS キーにポリシーを添付することで、許可を付与することができます。

別のアカウントの KMS キーを使用する場合は、キーを所有 AWS アカウント する にログインしてキーポリシーを適用する必要があります。検出結果をエクスポートするように設定する場合、キーを所有するアカウントからのキー ARN も必要です。

の KMS キーポリシーを変更 GuardDuty して エクスポートされた結果を暗号化するには

1. https://console.aws.amazon.com/kms で AWS KMS コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。

3. 既存の KMS キーを選択するか、「 デベロッパーガイド」の「新しいキーを作成する」の手順を実行します。このキーは、エクスポートされた検出結果の暗号化に使用します。 AWS Key Management Service

> **Note**
>
> KMS キーと Amazon S3 バケット AWS リージョン の は同じである必要があります。

同じ S3 バケットと KMS キーペアを使用して、該当するリージョンから結果をエクスポートできます。詳細については、考慮事項「」でリージョン間での結果のエクスポートを参照してください。

4. [Key policy] (キーポリシー) セクションで、[Edit] (編集) を選択します。

ポリシービューに切り替え が表示されている場合は、キーポリシー を表示するように選択し、編集 を選択します。

5. 次のポリシーブロックを KMS キーポリシーにコピーして、キーを使用するアクセス GuardDuty 許可を付与します。

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. ポリシーの例で#でフォーマットされている次の値を置き換えて、ポリシーを編集します。

1. *KMS ## ARN* を KMS キーの Amazon リソースネーム (ARN) に置き換えます。キー ARN を見つけるには、「 AWS Key Management Service デベロッパーガイド」の「キー ID と ARN の検索」を参照してください。
2. *123456789012* を、 AWS アカウント 結果をエクスポートする GuardDuty アカウントを所有する ID に置き換えます。
3. *Region2* を、 AWS リージョン GuardDuty 検出結果を生成する に置き換えます。
4. *SourceDetectorID* を、結果が生成された特定のリージョンの`detectorID` GuardDuty アカウントの に置き換えます。

   アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

> **Note**
>
> オプトインリージョン GuardDuty で を使用している場合は、「Service」の値をそのリージョンのリージョンエンドポイントに置き換えます。例えば、中東 (バーレーン) (me-south-1) リージョン GuardDuty で を使用している場合は、 を `"Service": "guardduty.amazonaws.com"`に置き換えます`"Service": "guardduty.me-south-1.amazonaws.com"`。各オプトインリージョンのエンドポイントの詳細については、GuardDuty 「 エンドポイントとクォータ」を参照してください。

7. 最後のステートメントの前にポリシーステートメントを追加した場合は、このステートメントを追加する前にカンマを追加します。KMS キーポリシーの JSON 構文が有効であることを確認します。

   [保存] を選択します。
8. (オプション) キー ARN をメモ帳にコピーして、後の手順で使用します。

ステップ 3 – Amazon S3 バケットにポリシーをアタッチする

がオブジェクトをこの S3 バケットにアップロードできるように、検出結果をエクスポートする Amazon S3 バケットにアクセス許可を追加します。 GuardDuty アカウントに属する Amazon S3 バケットを使用するか、別の で使用するかにかかわらず AWS アカウント、これらのアクセス許可を追加する必要があります。

いずれかの時点で別の S3 バケットに結果をエクスポートすることを決定した場合、結果をエクスポートし続けるには、その S3 バケットにアクセス許可を追加し、結果のエクスポート設定を再度設定する必要があります。

これらの結果をエクスポートする Amazon S3 バケットがまだない場合は、「Amazon Amazon S3 ユーザーガイド」の「バケットの作成」を参照してください。

S3 バケットポリシーにアクセス許可をアタッチするには

1. Amazon S3 ユーザーガイド」の「バケットポリシーを作成または編集するには」のステップを、「バケットポリシーの編集」ページが表示されるまで実行します。
2. このポリシー例は、Amazon S3 バケットに結果をエクスポートする GuardDuty アクセス許可を付与する方法を示しています。エクスポート結果の設定後にパスを変更する場合は、新しい場所にアクセス許可を付与するようにポリシーを変更する必要があります。

   次のポリシー例をコピーし、バケットポリシーエディタ に貼り付けます。

   最後のステートメントの前にポリシーステートメントを追加した場合は、このステートメントを追加する前にカンマを追加します。KMS キーポリシーの JSON 構文が有効であることを確認します。

   S3 バケットポリシーの例

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": "Amazon S3 bucket ARN",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
```

```
                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "DenyUnencryptedUploadsThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "DenyIncorrectHeaderThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
```

```
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
                }
            }
        },
        {
            "Sid": "DenyNon-HTTPS",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. ポリシーの例で#でフォーマットされている次の値を置き換えて、ポリシーを編集します。

   1. *Amazon S3 #### ARN* を Amazon S3 バケットの Amazon リソースネーム (ARN) に置き換えます。バケット ARN は、https://console.aws.amazon.com/s3/ コンソールのバケットポリシーの編集ページで確認できます。
   2. *123456789012* を、 AWS アカウント 結果をエクスポートする GuardDuty アカウントを所有する ID に置き換えます。
   3. *Region2* を、 AWS リージョン GuardDuty 結果が生成されている に置き換えます。
   4. *SourceDetectorID* を、結果が生成された特定のリージョンのdetectorID GuardDuty アカウントの に置き換えます。

      アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。
   5. S3 バケット ARN の *############* 部分/[オプションのプレフィックス] プレースホルダー値を、検出結果をエクスポートするオプションのフォルダの場所に置き換えます。 *S3* プレフィックスの使用の詳細については、Amazon S3 ユーザーガイド」の「プレフィックスを使用したオブジェクトの整理」を参照してください。

まだ存在しないオプションのフォルダの場所を指定すると、 GuardDuty は S3 バケットに関連付けられたアカウントが検出結果をエクスポートするアカウントと同じである場合にのみ、その場所を作成します。別のアカウントに属する S3 バケットに結果をエクスポートする場合、フォルダの場所は既に存在している必要があります。

6. *KMS ## ARN* を、S3 バケットにエクスポートされた検出結果の暗号化に関連付けられた KMS キーの Amazon リソースネーム (ARN) に置き換えます。キー ARN を見つけるには、「AWS Key Management Service デベロッパーガイド」の「キー ID と ARN の検索」を参照してください。

> **Note**
>
> オプトインリージョン GuardDuty で を使用している場合は、「Service」の値をそのリージョンのリージョンエンドポイントに置き換えます。例えば、中東 (バーレーン) (me-south-1) リージョン GuardDuty で を使用している場合は、 を `"Service": "guardduty.amazonaws.com"`に置き換えます`"Service": "guardduty.me-south-1.amazonaws.com"`。各オプトインリージョンのエンドポイントの詳細については、GuardDuty 「 エンドポイントとクォータ」を参照してください。

4. [保存] を選択します。

ステップ 4 - S3 バケットに結果をエクスポートする (コンソール)

GuardDuty では、別の の既存のバケットに結果をエクスポートできます AWS アカウント。

新しい S3 バケットを作成するとき、またはアカウント内の既存のバケットを選択するときは、オプションのプレフィックスを追加できます。エクスポート結果を設定すると、 は検出結果用の新しいフォルダを S3 バケットに GuardDuty 作成します。プレフィックスは、 が GuardDuty 作成したデフォルトのフォルダ構造に追加されます。例えば、オプションのプレフィックス の形式です`/AWSLogs/123456789012/GuardDuty/Region`。

S3 オブジェクトのパス全体が になります`DOC-EXAMPLE-BUCKET/prefix-name/UUID.jsonl.gz`。UUID はランダムに生成され、ディテクター ID または検出結果 ID を表すものではありません。

> **Important**
>
> KMS キーおよび S3 バケットは同じリージョンにある必要があります。

これらのステップを完了する前に、KMS キーと既存の S3 バケットにそれぞれのポリシーがアタッチされていることを確認してください。

エクスポート結果を設定するには

1. https://console.aws.amazon.com/guardduty/ で GuardDuty 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. 「設定」ページの「検出結果のエクスポートオプション」で、S3 バケット に対して「今すぐ設定」 (または必要に応じて を編集) を選択します。
4. S3 バケット ARN には、 を入力します**`bucket ARN`**。バケット ARN を確認するには、「Amazon S3 ユーザーガイド」の「S3 バケットのプロパティの表示」を参照してください。 Amazon S3 https://console.aws.amazon.com/guardduty/ コンソールの関連付けられたバケットのプロパティページのアクセス許可タブ。
5. KMS キー ARN には、 を入力します**`key ARN`**。キー ARN を見つけるには、「 AWS Key Management Service デベロッパーガイド」の「キー ID と ARN の検索」を参照してください。
6. ポリシーをアタッチする

   - S3 バケットポリシーをアタッチするステップを実行します。詳細については、「ステップ 3 – Amazon S3 バケットにポリシーをアタッチする」を参照してください。

   - KMS キーポリシーをアタッチするステップを実行します。詳細については、「ステップ 2 – KMS キーにポリシーをアタッチする」を参照してください
7. 保存を選択します。

ステップ 5 – 更新されたアクティブな検出結果をエクスポートする頻度を設定する

環境に応じて、更新されたアクティブな検出結果をエクスポートする頻度を設定します。デフォルトでは、更新された検出結果は 6 時間ごとにエクスポートされます。つまり、最新のエクスポート後に更新された検出結果が、次のエクスポートに含まれます。更新された検出結果が 6 時間ごとに工

クスポートされ、エクスポートが 12:00 に発生した場合、12:00 以降に更新した検出結果が 18:00 にエクスポートされます。

頻度を設定するには

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. [設定] を選択します。
3. [Findings export options] (結果のエクスポートオプション) セクションで、[Frequency for updated findings] (更新された結果の頻度) を選択します。これにより、更新されたアクティブ検出結果を EventBridge と Amazon S3 の両方にエクスポートする頻度が設定されます。次から選択できます。
   - 15 分ごとに EventBridge と S3 を更新する
   - 1 時間ごとに EventBridge と S3 を更新する
   - [Update CWE and S3 every 6 hours (default)] (CWE と S3 を 6 時間ごとに更新 (デフォルト))
4. [変更の保存] を選択します。

Amazon CloudWatch Events を使用した GuardDuty 結果へのカスタムレスポンスの作成

GuardDuty は、結果に変更があったときに Amazon CloudWatch Events のイベントを作成します。CloudWatch イベントを作成する変更には、新しく生成された結果や新しく集約された結果が含まれます。イベントは、ベストエフォートベースで発生します。

すべての GuardDuty 結果には結果 ID が割り当てられます。 は、一意の結果 ID を持つすべての結果に対して CloudWatch イベント GuardDuty を作成します。その後に発生した既存の検出結果は、すべて元の検出結果に集約されます。詳細については、「GuardDuty 結果の集約」を参照してください。

> **Note**
>
> アカウントが GuardDuty 委任された管理者である場合、 CloudWatch イベントはアカウントだけでなく、結果が生成されたメンバーアカウントにも発行されます。

で CloudWatch イベントを使用すると GuardDuty、タスクを自動化して、 GuardDuty 検出結果によって明らかになったセキュリティ問題に対応できます。

CloudWatch イベントに基づいて GuardDuty 検出結果に関する通知を受信するには、 CloudWatch イベントルールと のターゲットを作成する必要があります GuardDuty。このルールにより CloudWatch 、 は、 が GuardDuty 生成する検出結果の通知を、ルールで指定されたターゲットに送信できます。詳細については、「の CloudWatch イベントルールとターゲットの作成 GuardDuty (CLI)」を参照してください。

トピック

CloudWatch のイベント通知頻度 GuardDuty

一意の調査結果 ID を含む新しく生成された結果の通知

GuardDuty は、検出結果から 5 分以内に CloudWatch イベントに基づいて通知を送信します。このイベント (およびこの通知) には、この検出結果が一意の ID を伴って生成されてから最初の 5 分に発生したこの検出結果のそれ以降のすべての発生も含まれています。

> **Note**
>
> デフォルトでは、新しく生成された検出結果に関する通知の頻度は 5 分です。この頻度は更新できません。

以降に検出結果が見つかった場合の通知

デフォルトでは、一意の検出結果 ID を持つすべての検出結果について、 は 6 時間間隔内で発生した特定の検出結果タイプの後続のすべての出現を 1 つのイベントに GuardDuty 集約します。GuardDuty その後、このイベントに基づいてこれらの後続の発生に関する通知を送信します。デフォルトでは、既存の検出結果の後続の発生について、 は 6 時間ごとに CloudWatch イベントに基づいて通知 GuardDuty を送信します。

管理者アカウントアカウントのみが、その後の検出結果の発生に関する通知のデフォルトの頻度を CloudWatch イベントにカスタマイズできます。メンバーアカウントのユーザーはこの頻度を

カスタマイズできません。自分のアカウントで管理者アカウントによって設定された頻度値は、すべてのメンバーアカウントの機能に適用されます GuardDuty。管理者アカウントのユーザーがこの頻度値を 1 時間に設定すると、すべてのメンバーアカウントは、それ以降の結果に関する通知を受け取る頻度も 1 時間になります。詳細については、「Amazon での複数のアカウントの管理 GuardDuty」を参照してください。

> **Note**
>
> 管理者アカウントは、その後の検出結果の発生に関する通知のデフォルトの頻度をカスタマイズできます。有効な値は、15 分、1 時間、またはデフォルトの 6 時間です。これらの通知の頻度の設定については、ステップ 5 – 更新されたアクティブな検出結果をエクスポートする頻度を設定する を参照してください。

CloudWatch イベントによるアーカイブされた GuardDuty検出結果のモニタリング

手動でアーカイブされた検出結果の場合、これらの検出結果の最初の発生とその後のすべての発生 (アーカイブ完了後に生成された) は、上記の頻度ごとに CloudWatch イベントに送信されます。

自動アーカイブされた検出結果の場合、これらの検出結果の最初の出現とそれ以降のすべての出現 (アーカイブの完了後に生成された) は CloudWatch イベントに送信されません。

CloudWatch の イベント形式 GuardDuty

の CloudWatch イベント GuardDuty は次の形式です。

```
{
 "version": "0",
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

> **Note**
>
> 詳細値は、配列内で複数の検出結果をサポートできる「検出結果」値を返すのとは対照的に、単一の検出結果の JSON の詳細をオブジェクトとして返します。

`GUARDDUTY_FINDING_JSON_OBJECT` に含まれているすべてのパラメータの完全なリストについては、「GetFindings」を参照してください。`GUARDDUTY_FINDING_JSON_OBJECT` に表示される `id` パラメータは、上記で説明した検出結果 ID です。

GuardDuty 結果を通知する CloudWatch イベントルールの作成 (コンソール)

で CloudWatch イベントを使用して GuardDuty 、結果イベントをメッセージングハブに送信 GuardDutyすることで自動結果アラートを設定し、 GuardDuty 結果の可視性を高めることができます。このトピックでは、SNS トピックを設定し、そのトピックを CloudWatch イベントイベントルールに接続して、E メール、Slack、または Amazon Chime に検出結果アラートを送信する方法について説明します。

Amazon SNS トピックおよびエンドポイントの設定

まず、Amazon Simple Notification Service でトピックを設定し、エンドポイントを追加する必要があります。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「はじめに」を参照してください。

この手順では、 GuardDuty 検出結果データの送信先を設定します。SNS トピックは、 CloudWatch イベントルールの作成中または作成後にイベントイベントイベントルールに追加できます。

Email setup

SNS トピックの作成

1. https://console.aws.amazon.com/sns/v3/home で Amazon SNS コンソール にサインインします。
2. ナビゲーションペインから [Topics] (トピック) を選択し、[Create Topic] (トピックの作成) を選択します。
3. [Create topic] (トピックの作成) セクションで [Standard] (スタンダード) を選択します。次に、トピックの名前を入力します (例: **`GuardDuty_to_Email`**)。その他の詳細はオプションです。

4. [Create Topic] (トピックの作成) を選択します。新しいトピックのトピック詳細が開きます。
5. [Subscriptions] (サブスクリプション) セクションで、[Create Subscription] (サブスクリプションの作成) を選択します。
6. a. [Protocol] (プロトコル) メニューから [Email] (E メール) を選択します。

   b. [Endpoint] (エンドポイント) フィールドに、通知を受信する E メールアドレスを追加します。

   > **Note**
   >
   > 作成後、E メールクライアントを通じてサブスクリプションを確認する必要があります。

   c. [Create subscription] (サブスクリプションの作成) を選択します。
7. 受信トレイでサブスクリプションのメッセージを確認し、[Confirm Subscription] (サブスクリプションの確認) を選択します。

Slack setup

SNS トピックの作成

1. https://console.aws.amazon.com/sns/v3/home で Amazon SNS コンソール にサインインします。
2. ナビゲーションペインから [Topics] (トピック) を選択し、[Create Topic] (トピックの作成) を選択します。
3. [Create topic] (トピックの作成) セクションで [Standard] (スタンダード) を選択します。次に、トピックの名前を入力します (例: **`GuardDuty_to_Slack`**)。その他の詳細はオプションです。[Create topic] (トピックの作成)を選択し、確定します。

AWS Chatbot クライアントの設定

1. AWS Chatbot コンソールに移動します。
2. [Configured clients] (設定されたクライアント) パネルから [Configure new client] (新しいクライアントを設定) を選択します。
3. Slack を選択し、[Configure] (設定) で確認します。

> **Note**
>
> Slack を選択するときは、[allow] (許可) を選択してチャンネルにアクセスするために、AWS Chatbot のための許可を確認する必要があります。

4. [Configure new channel] (新しいチャンネルを設定)を選択し、設定の詳細ペインを開きます。

   a. チャンネルの名前を入力します。

   b. [Slack channel] (Slack チャンネル) で、使用したいチャネルを選択します。AWS Chatbot を用いてプライベート Slack チャンネルを使用するには、[Private channel] (プライベートチャンネル) を選択します。

   c. Slack で、チャンネル名を右クリックして [Copy Link] (リンクのコピー) を選択して、コピーのリンクを選択することでプライベートチャンネルのチャンネル ID をコピーします。

   d. AWS Chatbot ウインドウの AWS マネジメントコンソールで、Slack からコピーした ID を [Private channel ID] (プライベートチャンネル ID) フィールドに貼り付けます。

   e. [Permissions] (許可)で、まだロールを持っていない場合は、テンプレートを使用して IAM ロールを作成することを選択します。

   f. [Policy] (ポリシー) テンプレートで、[Notification permissions] (通知の許可) を選択します。これは AWS Chatbot のためのIAM ポリシーテンプレートです。 CloudWatch アラーム、イベント、ログ、および Amazon SNS トピックに必要な読み取りおよび一覧表示のアクセス許可を提供します。

   g. 以前に SNS トピックを作成したリージョンを選択し、Slack チャンネルに通知を送信するために作成した Amazon SNS トピックを選択します。

5. [Configure] (設定) を選択します。

Chime setup

SNS トピックの作成

1. https://console.aws.amazon.com/sns/v3/home で Amazon SNS コンソール にサインインします。
2. ナビゲーションペインから [Topics] (トピック) を選択し、[Create Topic] (トピックの作成) を選択します。

3. [Create topic] (トピックの作成) セクションで [Standard] (スタンダード) を選択します。次に、トピックの名前を入力します (例: **`GuardDuty_to_Chime`**)。その他の詳細はオプションです。[Create topic] (トピックの作成)を選択し、確定します。

AWS Chatbot クライアントの設定

1. AWS Chatbot コンソールに移動します。
2. [Configured clients] (設定されたクライアント) パネルから [Configure new client] (新しいクライアントを設定) を選択します。
3. Chime を選択し、[Configure] (設定) で確認します。
4. [Configuration details] (設定の詳細) ペインから、チャンネルの名前を入力します。
5. Chime で目的のチャットルームを開きます。
   a. 右上の歯車アイコンを選択してから、[Manage webhooks and bots] (ウェブフックとボットの管理) を選択します。
   b. [Copy URL] (URL をコピー)を選択し、Webhook URL をクリップボードにコピーします。
6. AWS Chatbot ウィンドウのリポジトリの AWS マネジメントコンソール上で、コピーした URL を [Webhook URL] (ウェブフック URL) フィールドに貼り付けてください。
7. [Permissions] (許可)で、まだロールを持っていない場合は、テンプレートを使用して IAM ロールを作成することを選択します。
8. [Policy] (ポリシー) テンプレートで、[Notification permissions] (通知の許可) を選択します。これは AWS Chatbot のためのIAM ポリシーテンプレートです。 CloudWatch アラーム、イベント、ログ、および Amazon SNS トピックに必要な読み取りおよび一覧表示のアクセス許可を提供します。
9. 以前に SNS トピックを作成したリージョンを選択し、Chime ルームに通知を送信するために作成した Amazon SNS トピックを選択します。
10. [Configure] (設定) を選択します。

検出結果の CloudWatch GuardDutyイベントを設定する

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインから [Rules] (ルール) を選択し、[Create Rule] (ルールの作成) を選択します。

3. サービス名 メニューから を選択しますGuardDuty。
4. イベントタイプメニューから、 GuardDuty の検索を選択します。
5. [Event Pattern Preview] (イベントパターンのプレビュー) の [Edit] (編集) を選択します。
6. 以下の JSON コードを [Event Pattern Preview] (イベントパターンプレビュー) に貼り付け、[Save] (保存) を選択します。

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
```

```
      6.4,
      6.5,
      6.6,
      6.7,
      6.8,
      6.9,
      7,
      7.0,
      7.1,
      7.2,
      7.3,
      7.4,
      7.5,
      7.6,
      7.7,
      7.8,
      7.9,
      8,
      8.0,
      8.1,
      8.2,
      8.3,
      8.4,
      8.5,
      8.6,
      8.7,
      8.8,
      8.9
    ]
  }
}
```

> **Note**
>
> 上記のコードでは、[Medium] (中)～[High] (高) の検出結果が警告されます。

7. [Targets] (ターゲット) セクションで、[Add Target] (ターゲットの追加) をクリックします。
8. [Select Targets] (ターゲットの選択) メニューから、[SNS Topic] (SNS トピック) を選択します。
9. [Select Topic] (トピックの選択) で、ステップ 1 で作成した SNS トピックの名前を選択します。
10. イベントの入力を設定します。

- Chime または Slack の通知をステップ 11 にスキップするように設定している場合、タイプデフォルトを [Matched event] (一致したイベント) に入力します。
- SNS 経由でメールの通知を設定する場合は、次のステップで示されるとおりに、以下のステップに従って受信トレイに送信されるメッセージをカスタマイズします。

a. [Configure input] (入力の設定) を展開して、[Input Transformer] (インプットトランスフォーマー) を閉じます。

b. 次のコードをコピーして、[Input Path] (入力パス) フィールドに貼り付けます。

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

c. 次のコードをコピーして [Input Template] (入力テンプレート) フィールドに貼り付け、E メールをフォーマットします。

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. [Configure Details] (詳細の設定) をクリックします。
12. [Configure rule details] (ルール詳細の設定) ページでルールの [Name] (名前) と [Description] (説明) を入力してから、[Create Rule] (ルールの作成) を選択してルールを有効化します。

の CloudWatch イベントルールとターゲットの作成 GuardDuty (CLI)

次の手順は、 AWS CLI コマンドを使用して の CloudWatch イベントルールとターゲットを作成する方法を示しています GuardDuty。具体的には、 が GuardDuty を生成し、 AWS Lambda関数をルールのターゲットとして追加するすべての検出結果のイベント CloudWatch を送信できるようにするルールを作成する方法を示します。

> **Note**
>
> Lambda 関数に加えて、 GuardDuty は、Amazon EC2 インスタンス、Amazon Kinesis ストリーム、Amazon ECS タスク、AWS Step Functionsステートマシン、 run コマンド、組み込みターゲットのターゲットタイプ CloudWatch をサポートします。

CloudWatch イベントコンソール GuardDuty を使用して、 の CloudWatch イベントルールとターゲットを作成することもできます。詳細と詳細な手順については、CloudWatch 「イベント でトリガーするイベントルールの作成」を参照してください。[Event Source] (イベントソース) セクションで、[Service name] (サービス名) のための **GuardDuty** と [Event Type] (イベントタイプ) のための **GuardDuty Finding** を選択します。

ルールおよびターゲットを作成するには

1. が生成する GuardDutyすべての検出結果のイベント CloudWatch を送信できるようにするルールを作成するには、次の CloudWatch CLI コマンドを実行します。

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > ルールをさらにカスタマイズして、 GuardDutyによって生成された結果のサブセットに対してのみイベントを送信する CloudWatch ように に指示できます。このサブセットは、ルールで指定されている検出結果の属性に基づきます。例えば、次の CLI コマンドを使用して、 CloudWatch が重要度が 5 または 8 の検出 GuardDuty 結果のイベントのみを送信できるようにするルールを作成します。
   >
   > ```
   > AWS events put-rule --name Test --event-pattern "{\"source\":
   > [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],
   > \"detail\":{\"severity\":[5,8]}}"
   > ```

この目的のために、JSON で利用可能な任意のプロパティ値を GuardDuty 結果に使用できます。

2. ステップ 1 で作成したルールのターゲットとして Lambda 関数をアタッチするには、次の CloudWatch CLI コマンドを実行します。

```
AWS events put-targets --rule Test --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

> **Note**
>
> 上記のコマンドの <your_function> を GuardDuty イベントの実際の Lambda 関数に置き換えてください。

3. ターゲットを呼び出す上で必要な許可を追加するには、次の Lambda CLI コマンドを実行します。

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

> **Note**
>
> 上記のコマンドの <your_function> を GuardDuty イベントの実際の Lambda 関数に置き換えてください。

> **Note**
>
> 上記の手順では、 CloudWatch イベントをトリガーするルールのターゲットとして Lambda 関数を使用しています。他のAWSリソースをターゲットとして設定して、 CloudWatch イベントをトリガーすることもできます。詳細については、「PutTargets」を参照してください。

CloudWatch GuardDuty マルチアカウント環境のイベント

アカウントの GuardDuty 管理者 CloudWatch イベントルールは、メンバーアカウントからの該当する結果に基づいてトリガーされます。つまり、前のセクションで説明したように、管理者アカウント

で CloudWatch イベントを通じて検出結果通知を設定すると、自分のものに加えて、メンバーアカウントによって生成された重要度の高い検出結果と中程度の検出結果の通知が届きます。

GuardDuty 結果の JSON 詳細の `accountId`フィールドを使用して、結果の発生元のメンバーアカウントを特定できます。

コンソールで環境内の特定のメンバーアカウントのカスタムイベントルールの作成を開始するには、新しいルールを作成し、イベントパターンプレビューに次のテンプレートを貼り付け、イベントをトリガーしたいメンバーアカウントのアカウント ID を追加します。

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> この例では、リストされたアカウント ID のすべての検出結果に対してトリガーします。複数の ID を JSON 構文の後にカンマで区切って追加できます。

Malware Protection for EC2 スキャン中にリソースをスキップする CloudWatch ログと理由を理解する

GuardDuty Malware Protection for EC2 は、Amazon CloudWatch ロググループ /aws/guardduty/malware-scan-events にイベントを発行します。マルウェアスキャンに関連する各イベントについて、影響を受けるリソースのステータスとスキャン結果を監視できます。特定の Amazon EC2 リソースと Amazon EBS ボリュームは、EC2 の Malware Protection スキャン中にスキップされている可能性があります。

Malware Protection for EC2 GuardDuty での CloudWatch ログの監査

/aws/guardduty/malware-scan-events CloudWatch log グループでは、3 種類のスキャンイベントがサポートされています。

EC2 スキャンイベント名の Malware Protection	説明
EC2_SCAN_STARTED	GuardDuty Malware Protection for EC2 が EBS ボリュームのスナップショットを作成する準備など、マルウェアスキャンのプロセスを開始したときに作成されます。
EC2_SCAN_COMPLETED	影響を受けたリソースの少なくとも 1 つの EBS ボリュームの GuardDuty Malware Protection for EC2 スキャンが完了したときに作成されます。このイベントには、スキャンされた EBS ボリュームに属する snapshotId も含まれます。スキャンが完了すると、スキャン結果は、CLEAN、THREATS_FOUND 、または NOT_SCANNED のいずれかになります。
EC2_SCAN_SKIPPED	GuardDuty Malware Protection for EC2 スキャンが、影響を受けるリソースのすべての EBS ボリュームをスキップしたときに作成されます。スキップ理由を特定するには、対応するイベントを選択し、詳細を表示します。スキップの理由の詳細については、以下の「マルウェアスキャン中にリソースをスキップする理由」を参照してください。

> **Note**
>
> を使用している場合 AWS Organizations、Organizations のメンバーアカウントからの CloudWatch ログイベントは、管理者アカウントとメンバーアカウントのロググループの両方に発行されます。

任意のアクセス方法を選択して、 CloudWatch イベントを表示およびクエリします。

Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[Logs] (ログ)、[Log groups] (ロググループ) の順に選択します。Malware Protection for EC2 のスキャンイベントを表示するには、/aws/guardduty/malware-scan-events GuardDuty ロググループを選択します。

   クエリを実行するには、[Log Insights] (ログのインサイト) を選択してください

   クエリの実行の詳細については、「Amazon ユーザーガイド」の「Logs Insights を使用した CloudWatch ログデータの分析」を参照してください。 CloudWatch
3. [Scan ID] (スキャン ID) を選択して、影響を受けたリソースとマルウェアの検出結果の詳細を監視します。例えば、次のクエリを実行して、 を使用して CloudWatch ログイベントをフィルタリングできますscanId。ご自身の有効な *Scan-ID* を使用してください。

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- ロググループを使用するには、「Amazon ユーザーガイド」の「 を使用してログエントリを検索する AWS CLI」を参照してください。 CloudWatch

  Malware Protection for EC2 のスキャンイベントを表示するには、/aws/guardduty/malware-scan-events GuardDuty ロググループを選択します。
- ログイベントを表示およびフィルタリングするには、「Amazon CloudWatch API リファレンス」のFilterLogEventsGetLogEvents「」と「」をそれぞれ参照してください。

GuardDuty EC2 ログ保持の Malware Protection

/aws/guardduty/malware-scan-events ロググループのデフォルトのログ保持期間は 90 日です。その後、ログイベントは自動的に削除されます。ロググループの CloudWatch ログ保持ポリシーを変更するには、「Amazon ユーザーガイド」の CloudWatch 「ログでのログデータ保持の変更」、ま

たはPutRetentionPolicy「Amazon CloudWatch API リファレンス」の「」を参照してください。CloudWatch

マルウェアスキャン中にリソースをスキップする理由

マルウェアスキャンに関連するイベントでは、特定の EC2 リソースと EBS ボリュームがスキャンプロセス中にスキップされた可能性があります。次の表に、 GuardDuty Malware Protection for EC2 がリソースをスキャンしない理由を示します。該当する場合は、提案されたステップを使用してこれらの問題を解決し、次に GuardDuty Malware Protection for EC2 がマルウェアスキャンを開始したときにこれらのリソースをスキャンします。その他の問題は、イベントの経過を知らせるために使用されるものであり、対応不要です。

スキップの理由	説明	提案されるステップ	
`RESOURCE_NOT_FOUND`	オンデマンドのマルウェアスキャンを開始する にresourceArn 提供された は、AWS 環境で見つかりませんでした。	Amazon EC2 インスタンスの resourceArn またはコンテナのワークロードを検証して、もう一度試してください。	
`ACCOUNT_INELIGIBLE`	オンデマンドのマルウェアスキャンを開始しようとした AWS アカウント ID が を有効にしていません GuardDuty。	この AWS アカウントで GuardDuty が有効になっていることを確認します。 新しい GuardDuty でを有効にすると、同期に最大 20 分かかる AWS リージョン 場合があります。	
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty Malware Protection for EC2 は、暗号化されていないボリュームと、カスタマーマネージドキーで暗号化され	暗号化キーをカスタマーマネージドキーに置き換えます。が GuardDuty サポートする暗号化のタイプの詳細について	

スキップの理由	説明	提案されるステップ	
	たボリュームの両方をサポートします。Amazon EBS 暗号化を使用して暗号化された EBS ボリュームのスキャンはサポートされていません。 現在、このスキップ理由が適用されない地域的な違いがあります。これらの の詳細については AWS リージョン、「」を参照してくださいリージョン固有機能の可用性。	は、「」を参照してくださいマルウェアスキャンでサポートされている Amazon EBS ボリューム。	

スキップの理由	説明	提案されるステップ	
EXCLUDED_BY_SCAN_SETTINGS	EC2 インスタンスまたは EBS ボリュームは、マルウェアスキャン中に除外されました。2 つの可能性があります。タグが対象リストに追加されたが、リソースがこのタグに関連付けられていないか、タグが除外リストに追加され、リソースがそのタグに関連付けられている、または、GuardDuty Excluded タグがそのリソースに対し true に設定されています。	スキャンオプションまたは Amazon EC2 リソースに関連付けられているタグを更新します。詳細については、「ユーザー定義タグ付きのスキャンオプション」を参照してください。	
UNSUPPORTED_VOLUME_SIZE	ボリュームが 2048 GB を超えています。	実用的ではありません。	
NO_VOLUMES_ATTACHED	GuardDuty Malware Protection for EC2 は、アカウント内のインスタンスを検出しましたが、スキャンを続行するためにこのインスタンスに EBS ボリュームがアタッチされていません。	実用的ではありません。	

スキップの理由	説明	提案されるステップ	
UNABLE_TO_SCAN	内部サービスエラー。	実用的ではありません。	
SNAPSHOT_NOT_FOUND	EBS ボリュームから作成され、サービスアカウントと共有されているスナップショットは見つかりませんでした。EC2 の GuardDuty Malware Protection はスキャンを続行できませんでした。	スナップショットが意図的に削除されていない CloudTrail ことを確認します。	
SNAPSHOT_QUOTA_REACHED	各リージョンのスナップショットに許可されている最大ボリュームに達しました。これにより、スナップショットの保持だけでなく、新しいスナップショットの作成もできなくなります。	古いスナップショットを削除するか、クォータの増加をリクエストできます。リージョンごとのスナップショットのデフォルト制限と、クォータの増加をリクエストする方法については、「AWS 全般のリファレンスガイド」の「サービスクォータ」を参照してください。	

スキップの理由	説明	提案されるステップ	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	EC2 インスタンスに 11 個を超える EBS ボリュームがアタッチされました。EC2 の GuardDuty マルウェア保護は、アルファベット順にソートして取得した最初の 11 個の EBS deviceName ボリュームをスキャンしました。	実用的ではありません。	
UNSUPPORTED_PRODUCT_CODE_TYPE	GuardDuty は、 を productCode とするインスタンスのスキャンをサポートしていませんmarketplace 。詳細については、「Amazon EC2 ユーザーガイドAMIs」を参照してください。Amazon EC2 productCode の詳細については、「Amazon EC2 API リファレンス」の「ProductCode」を参照してください。	実用的ではありません。	

Malware Protection for EC2 GuardDuty での誤検出の報告

GuardDuty EC2 スキャンの Malware Protection は、Amazon EC2 インスタンスまたはコンテナワークロード内の無害なファイルを悪意のあるファイルまたは有害なファイルとして識別する場合があります。Malware Protection for EC2 と GuardDuty サービスの使用体験を向上させるために、スキャン中に悪意のあるファイルまたは有害であると特定されたファイルにマルウェアが実際に含まれていないと思われる場合は、誤検出結果を報告できます。

誤検出ファイル提出

1. https://console.aws.amazon.com/guardduty/ コンソールにログインします。
2. 誤検出の結果と思われるものを特定したら、 AWS Support に連絡して誤検出ファイルの送信プロセスを開始します。
3. [Malware Scans] (マルウェアのスキャン) を選択します。
4. スキャンを選択してその [Finding ID] (検出結果 ID) を表示します。
5. [Finding ID] (検出結果 ID) を指定します。ファイルの SHA-256 ハッシュを指定する必要があります。これは、 GuardDuty Malware Protection for EC2 が正しいファイルを受信していることを確認するために必要です。
6. AWS Support チームは、ファイルと SHA-256 ハッシュのアップロードに使用できる Amazon Simple Storage Service (S3) URL を提供します。ファイルが正常にアップロードされたら、AWS Support チームに通知します。

> **Warning**
>
> ファイルまたは SHA-256 ハッシュを直接 AWS Supportに送らないでください。指定された URL を介してのみ、ファイルとハッシュを Amazon S3 にアップロードする必要があります。URL を受け取ってから 7 日以内にファイルとハッシュをアップロードしないと、無効になります。URL が無効になった場合は、 に連絡して新しい URL AWS Support を受け取る必要があります。

GuardDuty は、ファイルを 30 日以内に保持します。 GuardDuty チームメンバーは送信を分析し、Malware Protection for EC2 と サービスの使用体験を向上させるための適切な措置を講じます GuardDuty。

によって検出されたセキュリティ問題の修復 GuardDuty

Amazon は、潜在的なセキュリティ問題を示す検出結果 GuardDuty を生成します。のこのリリースでは GuardDuty、潜在的なセキュリティ問題は、侵害された EC2 インスタンスまたはコンテナワークロード、または AWS 環境内の一連の侵害された認証情報のいずれかを示します。次のセクションでは、これらのシナリオにおいて推奨される修復ステップについて説明します。代替修復シナリオがある場合は、その特定の検出結果タイプのエントリで説明されます。検出結果タイプに関する完全な情報にアクセスするには、[Active findings types table] (アクティブな検出結果タイプテーブル) を選択します。

内容

侵害された可能性のある Amazon EC2 インスタンスの修復

環境内の侵害された可能性のある EC2 インスタンスを修正するには、以下の推奨ステップに従います AWS 。

1. 侵害された可能性のある Amazon EC2 インスタンスを特定する

   マルウェアに侵害された可能性のあるインスタンスを調査し、検出されたマルウェアを削除します。オンデマンドのマルウェアスキャン を使用して、侵害された可能性のある EC2 インスタンス内のマルウェアを特定したり、AWS Marketplace でマルウェアを特定して削除するのに役立つパートナー製品があるかどうかを確認したりできます。
2. 侵害された可能性のある Amazon EC2 インスタンスを分離する

可能であれば、次のステップを使用して、侵害された可能性のあるインスタンスを分離します。

1. 専用の分離セキュリティグループを作成します。
2. アウトバウンドルールのすべてのトラフィック0.0.0.0/0 (0-65535)に対して の単一のルールを作成します。

   このルールが適用されると、既存の (および新しい) アウトバウンドトラフィックがすべて追跡されていない状態に変換され、確立されたアウトバウンドセッションがブロックされます。詳細については、「未追跡の接続」を参照してください。
3. 侵害された可能性のあるインスタンスから、現在のセキュリティグループの関連付けをすべて削除します。
4. 分離セキュリティグループをこのインスタンスに関連付けます。

   関連付け後、分離セキュリティグループのアウトバウンドルールから0.0.0.0/0 (0-65535)すべてのトラフィックのルールを削除します。

3. 疑わしいアクティビティのソースを特定する

   マルウェアが検出された場合は、アカウント内の検出結果のタイプに基づいて、EC2 インスタンスでの不正なアクティビティの可能性を特定して停止します。これには、開いているポートを閉じる、アクセスポリシーを変更する、脆弱性を修正するためにアプリケーションをアップグレードするなどのアクションが必要になる場合があります。

   侵害された可能性のある EC2 インスタンスで不正なアクティビティを特定して停止できない場合は、侵害された EC2 インスタンスを終了し、必要に応じて新しいインスタンスに置き換えることをお勧めします。EC2 インスタンスを保護するための追加リソースを次に示します。

   - 「Amazon EC2 のベストプラクティス」の「セキュリティ」と「ネットワーク」のセクション。
   - 「Linux インスタンス用の Amazon EC2 セキュリティグループ」および「Windows インスタンス用の Amazon EC2 セキュリティグループ」
   - Amazon EC2 でのセキュリティ
   - EC2 インスタンスのセキュリティを確保するためのヒント (Linux)
   - AWS セキュリティのベストプラクティス
   - のインフラストラクチャドメインインシデント AWS
4. 参照 AWS re:Post

   詳細については、AWS re:Post「」を参照してください。

5. テクニカルサポートリクエストを送信する

   プレミアムサポートパッケージのサブスクライバーは、テクニカルサポートをリクエストできます。

侵害された可能性のある S3 バケットの修復

環境内の侵害された可能性のある Amazon S3 バケットを修正するには、以下の推奨ステップに従います AWS 。

1. 侵害された可能性のある S3 リソースを特定します。

   S3 GuardDuty の結果は、関連する S3 バケット、その Amazon リソースネーム (ARN)、およびその所有者を結果の詳細に一覧表示します。
2. 疑わしいアクティビティのソースと使用された API コールを特定します。

   使用された API コールは、検出結果の詳細に API として表示されます。ソースは IAM プリンシパル (IAM ロール、ユーザーまたはアカウント) で、識別情報が検出結果に表示されます。ソースタイプに応じて、リモート IP アドレスまたはソースドメイン情報が利用可能になり、ソースが承認されたかどうかを評価するのに役立ちます。検出結果に Amazon EC2 インスタンスの認証情報が含まれている場合、そのリソースの詳細も含まれます。
3. コールソースが、識別されたリソースへのアクセスを許可されたかどうかを確認します。

   例えば、次の事項を検討します。
   - IAM ユーザーが関係していた場合、認証情報が侵害された可能性がありますか？ 詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。
   - API が、このタイプの API を呼び出した履歴がないプリンシパルから呼び出された場合、このソースはこのオペレーションのアクセス権を必要としますか? バケットの許可をさらに制限することはできますか?
   - ユーザー名 ANONYMOUS_PRINCIPAL とユーザータイプ AWSAccount のアクセスがあった場合、これは、バケットがパブリックであり、アクセスされたことを示します。このバケットはパブリックであるべきですか? そうでない場合は、S3 リソースを共有する代替ソリューションについて、以下のセキュリティに関するレコメンデーションを確認してください。
   - ユーザータイプ AWSAccount のユーザー名 ANONYMOUS_PRINCIPAL から見た PreflightRequest コールが成功した場合、これはバケットにクロスオリジンリソース共有 (CORS) ポリシーが設定されていることを示します。このバケットには CORS ポリシーが必要ですか? そうでない場合は、バケットが不用意に公開されないようにし、S3 リソースを共

有する代替ソリューションについて、以下のセキュリティに関するレコメンデーションを確認してください。CORS の詳細については、「S3 ユーザーガイド」の「Cross-Origin Resource Sharing (CORS) の使用」を参照してください。

4. S3 バケットに機密データが含まれているかどうか判断します。

   Amazon Macie を使用して、S3 バケットに個人を特定できる情報 (PII)、財務データ、認証情報などの機密データが含まれているかどうかを判断します。Macie アカウントで機密データの自動検出が有効になっている場合は、S3 バケットの詳細を確認して S3 バケットのコンテンツをよりよく理解してください。Macie アカウントでこの機能が無効になっている場合、評価を早めるために有効にすることをおすすめします。または、機密データ検出ジョブを作成して実行し、S3 バケットのオブジェクトに機密データがないかを検査することもできます。詳細については、「機密ログデータをマスキングで保護する」を参照してください。

アクセスが許可されている場合は、検出結果を無視できます。https://console.aws.amazon.com/guardduty/ コンソールでは、個々の結果を表示しないように完全に抑制するルールを設定できます。詳細については、「抑制ルール」を参照してください。

S3 データが権限のない当事者によって公開またはアクセスされたと判断した場合は、次の S3 セキュリティに関する推奨事項を確認して、アクセス許可を厳しくし、アクセスを制限します。適切な修復ソリューションは、特定の環境のニーズによって異なります。

特定の S3 バケットアクセスのニーズに基づく推奨事項

次のリストは、特定の Amazon S3 バケットアクセスのニーズに基づく推奨事項を示しています。

- S3 データ使用へのパブリックアクセスを一元的に制限するために、S3 はパブリックアクセスをブロックします。ブロックパブリックアクセス設定は、アクセスポイント、バケット、 AWS アカウントに対して 4 つの異なる設定で有効にして、アクセスの粒度を制御できます。「S3 Block Public Access Settings」(S3 ブロックパブリックアクセス設定) を参照してください。
- AWS アクセスポリシーを使用して、IAM ユーザーがリソースにアクセスする方法やバケットにアクセスする方法を制御できます。詳細については、「バケットポリシーとユーザーポリシーの使用」を参照してください。

  S3 バケットポリシーで仮想プライベートクラウド (VPC) エンドポイントを使用して、特定の VPC エンドポイントへのアクセスを制限することもできます。詳細については、「Example Bucket Policies for VPC Endpoints for Amazon S3」(Amazon S3 の VPC エンドポイント用のバケットポリシーの例) を参照してください。

- アカウント外の信頼できるエンティティへの S3 オブジェクトへのアクセスを一時的に許可するには、S3 を使用して署名済み URL を作成します。このアクセスは、アカウントの認証情報を使用して作成され、使用される認証情報に応じて 6 時間から 7 日間使用できます。詳細については、「Generating presigned URLs with S3」(S3 で署名済み URL を生成する) を参照してください。
- 異なるソース間で S3 オブジェクトを共有する必要があるユースケースでは、S3 アクセスポイントを使用して、プライベートネットワーク内のオブジェクトのみへのアクセスを制限する許可セットを作成できます。詳細については、「Amazon S3 Access Points を使用したデータアクセスの管理」を参照してください。
- 他の AWS アカウントに S3 リソースへのアクセスを安全に付与するには、アクセスコントロールリスト (ACL) を使用できます。詳細については、「ACL による S3 アクセスの管理 ACLs」を参照してください。

S3 セキュリティオプションの詳細については、S3 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。

悪意のある可能性のある S3 オブジェクトの修復

S3 検出結果タイプの Malware Protection が で生成されると AWS アカウント、潜在的に悪意のあるリソースタイプは S3Objectです。

生成された検出結果を修正するには、以下の推奨ステップを使用します。

1. 検出結果に関連付けられた S3 をチェックして、悪意のある可能性のある S3ObjectDetails オブジェクトを特定します。
2. 影響を受けた S3 オブジェクトを分離します。関連付けられた Amazon S3 バケットの Malware Protection for S3 を有効にしたときにタグ付けを有効にしていた場合、 はこのオブジェクトに悪意のあるタグを割り当てている GuardDuty 必要があります。 Amazon S3 タグベースのアクセスコントロール (TBAC) を使用して、この S3 オブジェクトへのアクセスを制限します。詳細については、「タグベースのアクセスコントロール (TBAC) の使用」を参照してください。

   または、このオブジェクトが不要になった場合は、削除することも、分離された S3 バケットに移動することもできます。S3 オブジェクトの削除に関する考慮事項については、「Amazon S3 ユーザーガイド」の「オブジェクトの削除」を参照してください。 Amazon S3

侵害された可能性のある ECS クラスターの修復

環境内の侵害された可能性のある Amazon ECS クラスターを修正するには、以下の推奨ステップに従います AWS 。

1. 侵害された可能性のある ECS クラスターを特定します。

   ECS の EC2 検出結果の GuardDuty Malware Protection は、検出結果の詳細パネルに ECS クラスターの詳細を提供します。

2. マルウェアの発生源を評価する

   検出されたマルウェアがコンテナのイメージに存在していたかどうかを評価します。マルウェアがイメージに存在していた場合は、このイメージを使用して実行されている他のすべてのタスクを特定します。タスクの実行の詳細については、「」を参照してくださいListTasks。

3. 影響を受ける可能性のあるタスクを分離する

   タスクへの送受信トラフィックをすべて拒否して、影響を受けたタスクを分離します。すべてのトラフィックルールを拒否すると、タスクへのすべての接続を切断することで、すでに進行中の攻撃を停止するのに役立ちます。

アクセスが許可されている場合は、検出結果を無視できます。https://console.aws.amazon.com/guardduty/ コンソールでは、個々の結果を表示しないように完全に抑制するルールを設定できます。詳細については、「抑制ルール」を参照してください。

侵害された可能性のある AWS 認証情報の修正

環境内の侵害された可能性のある認証情報を修正するには、以下の推奨ステップに従います AWS 。

1. 侵害された可能性のある IAM エンティティと使用された API コールを特定します。

   使用された API コールは、検出結果の詳細に API として表示されます。IAM エンティティ (IAM ロールまたはユーザー) とその識別情報は、検出結果の詳細のリソースセクションに一覧表示されます。関連する IAM エンティティのタイプは、[User Type] (ユーザータイプ) フィールドで特定できます。IAM エンティティの名前は、[User name] (ユーザー名) フィールドに表示されます。検出結果に関連する IAM エンティティのタイプは、使用された [Access key ID] (アクセスキー ID) でも特定できます。

`AKIA` で始まるキーの場合:

このタイプのキーは、IAM ユーザーまたは AWS アカウントのルートユーザーに関連付けられているカスタマーマネージドの長期の認証情報です。IAM ユーザーのアクセスキーの管理については、「IAM ユーザーのアクセスキーの管理」を参照してください。

`ASIA` で始まるキーの場合:

このタイプのキーは、 AWS Security Token Serviceによって生成される短期の一時的な認証情報です。これらのキーは短時間だけ存在し、 AWS マネジメントコンソールで表示または管理することはできません。IAM ロールは常に AWS STS 認証情報を使用しますが、IAM ユーザー用に生成することもできます。詳細については、「IAM: 一時的なセキュリティ認証情報 AWS STS 」を参照してください。

ロールが使用された場合、[User name] (ユーザー名) フィールドには使用されたロールの名前が表示されます。 CloudTrail ログエントリの `sessionIssuer`要素を調べる AWS CloudTrail ことで、 でキーがどのようにリクエストされたかを特定できます。詳細については、「IAM」および AWS STS 「」の情報 CloudTrailを参照してください。

2. IAM エンティティの許可を確認します。

   [IAM コンソール] を開きます。使用するエンティティのタイプに応じて、ユーザーまたはロールタブを選択し、識別された名前を検索フィールドに入力して、影響を受けるエンティティを見つけます。[Permission] (許可) タブと [Access Advisor] (アクセスアドバイザー) タブを使用して、そのエンティティの有効な許可を確認します。

3. IAM エンティティの認証情報が正当に使用されたかどうかを確認します。

   アクティビティが意図的なものであったかどうかを確認するには、認証情報のユーザーに問い合わせます。

   例えば、ユーザーが次のことを行ったかどうかを確認します。

   - GuardDuty 検出結果にリストされている API オペレーションを呼び出しました
   - 検出結果にリストされている時点で API オペレーションを GuardDuty呼び出しました
   - GuardDuty 検出結果にリストされている IP アドレスから API オペレーションを呼び出しました

このアクティビティが AWS 認証情報の正当な使用である場合は、 GuardDuty 結果を無視できます。https://console.aws.amazon.com/guardduty/ コンソールでは、個々の結果を表示しないように完全に抑制するルールを設定できます。詳細については、「抑制ルール」を参照してください。

このアクティビティが正当な使用であるかどうかが確認できない場合は、特定のアクセスキー、IAM ユーザーのサインイン認証情報、または 全体に対する侵害の結果である可能性があります AWS アカウント。認証情報が侵害された疑いがある場合は、「My AWS アカウント may be compromised」の記事の情報を確認して、この問題を修正してください。

侵害された可能性のあるスタンドアロンコンテナの修復

1. 侵害された可能性のあるコンテナを分離する

   次のステップは、潜在的に悪意のあるコンテナワークロードを特定するのに役立ちます。

   - https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
   - 検出結果ページで、対応する検出結果を選択して検出結果パネルを表示します。
   - 検出結果パネルの [Resource affected] (影響を受けるリソース) セクションで、コンテナの [ID] と [Name] (名前) を表示できます。

   このコンテナを他のコンテナワークロードから分離します。

2. コンテナを一時停止する

   コンテナ内のすべてのプロセスを一時停止します。

   コンテナをフリーズする方法については、「コンテナを一時停止する」を参照してください。

   コンテナを停止する

   上記のステップが失敗し、コンテナが一時停止しない場合は、コンテナの実行を停止します。スナップショットの保持 この機能を有効にした場合、 GuardDuty はマルウェアを含む EBS ボリュームのスナップショットを保持します。

   コンテナの停止については、「コンテナの停止」を参照してください。

3. マルウェアの有無の評価

   マルウェアがコンテナのイメージに存在したかどうかを評価します。

アクセスが許可されている場合は、検出結果を無視できます。https://console.aws.amazon.com/guardduty/ コンソールでは、個々の結果を表示しないように完全に抑制するルールを設定できます。GuardDuty コンソールでは、個々の検出結果が表示されないように完全に抑制するルールを設定できます。詳細については、「抑制ルール」を参照してください。

EKS 監査ログのモニタリング検出結果の修正

Amazon は、アカウントで EKS 監査ログのモニタリングが有効になっている場合に、Kubernetes セキュリティの潜在的な問題を示す結果 GuardDuty を生成します。詳細については、「EKS 監査ログのモニタリング」を参照してください。次のセクションでは、これらのシナリオにおいて推奨される修復ステップについて説明します。特定の修復アクションは、その特定の検出結果タイプのエントリで説明されています。検出結果タイプに関する完全な情報にアクセスするには、[Active findings types table] (アクティブな検出結果タイプテーブル) を選択します。

EKS Audit Log Monitoring の結果タイプのいずれかが予想どおりに生成された場合は、今後アラートが発生しないように 抑制ルール を追加することを検討してください。

さまざまなタイプの攻撃や設定の問題により、 GuardDuty Kubernetes の検出結果がトリガーされる可能性があります。このガイドでは、クラスターに対する GuardDuty 検出結果の根本原因を特定し、適切な修復ガイダンスの概要を説明します。 GuardDuty Kubernetes の検出結果につながる主な根本原因は次のとおりです。

- 設定の潜在的な問題
- 侵害された可能性のある Kubernetes ユーザーの修復
- 侵害された可能性のある Kubernetes ポッドの修復
- 侵害された可能性のある Kubernetes ノードの修復
- 侵害された可能性のあるコンテナイメージの修復

> **Note**
>
> Kubernetes バージョン 1.14 より前のバージョンでは、`system:unauthenticated`グループは`system:basic-user`ClusterRolesデフォルトで `system:discovery`および に関連付けられていました。これは、匿名ユーザーからの意図しないアクセスを許可する場合があります。クラスターの更新では、これらの許可は取り消されません。つまり、クラスターをバージョン 1.14 以降に更新した場合でも、これらの許可は引き続き有効である可能性があります。これらの許可の関連付けを `system:unauthenticated` グループから解除することをお勧めします。
> これらのアクセス許可の削除の詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS 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。

設定の潜在的な問題

検出結果で設定の問題が示されている場合、その特定の問題の解決に関するガイダンスについては、その検出結果の修復セクションを参照してください。詳細については、設定上の問題を示す次の検出結果タイプを参照してください。

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- で終わる結果 SuccessfulAnonymousAccess

侵害された可能性のある Kubernetes ユーザーの修復

GuardDuty 検出結果で識別されたユーザーが予期しない API アクションを実行した場合、検出結果は侵害された Kubernetes ユーザーを示している可能性があります。ユーザーは、コンソールの検出結果の詳細の [Kubernetes user details] (Kubernetes ユーザー詳細) セクション、または検出結果の JSON の `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` で識別できます。これらのユーザーの詳細には、`user name`、`uid`、およびユーザーが属する Kubernetes グループが含まれます。

ユーザーが IAM エンティティを使用してワークロードにアクセスしていた場合は、この `Access Key details` セクションを使用して、IAM ロールまたはユーザーの詳細を識別できます。次のユーザータイプとその修復ガイダンスを参照してください。

> **Note**
>
> Amazon Detective を使用して、検出結果で特定された IAM ロールまたはユーザーをさらに調査できます。 GuardDuty コンソールで検出結果の詳細を表示しながら、Detective で調査を選択します。次に、リストされた項目から AWS ユーザーまたはロールを選択して、Detective で調査します。

組み込みの Kubernetes 管理者 – クラスターを作成した IAM アイデンティティに Amazon EKS によって割り当てられたデフォルトのユーザー。このユーザータイプは、ユーザー名 `kubernetes-admin` で識別されます。

組み込みの Kubernetes 管理者のアクセスを取り消すには:

- `Access Key details` セクションから `userType` を識別します。
  - `userType` が [Role] (ロール) であり、ロールが EC2 インスタンスロールに属している場合:
    - そのインスタンスを特定し、「侵害された可能性のある Amazon EC2 インスタンスの修復」の手順に従います。
  - `userType` が [User] (ユーザー) の場合、またはユーザーが引き受けた [Role] (ロール) の場合:
    1. そのユーザーのアクセスキーをローテーションします。
    2. ユーザーがアクセス権を有していたシークレットをローテーションします。
    3. 詳細については、「マイ AWS アカウントが侵害されている可能性がある」の情報を確認してください。

OIDC 認証済みユーザー – OIDC プロバイダーを通じてアクセス権を付与されたユーザー。通常、OIDC ユーザーは、ユーザー名としてメールアドレスを持っています。次のコマンドを使用して、クラスターが OIDC を使用しているかどうかを確認できます: `aws eks list-identity-provider-configs --cluster-name your-cluster-name` 。

OIDC 認証済みユーザーのアクセスを取り消すには:

1. OIDC プロバイダーでそのユーザーの認証情報をローテーションします。
2. ユーザーがアクセス権を有していたシークレットをローテーションします。

-AWSAuth ConfigMap defined user – AWS-auth を通じてアクセス権を付与された IAM ユーザー ConfigMap。詳細については、「&EKS; ユーザーガイド」の「クラスターのユーザーまたは IAM ロールの管理」を参照してください。次のコマンドを使用して、許可を確認できます: `kubectl edit configmaps aws-auth --namespace kube-system`。

ユーザーのアクセス AWS ConfigMapを取り消すには :

1. 次のコマンドを使用して、 を開きます ConfigMap。

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. mapRoles または mapUsers セクションのロールまたはユーザーエントリを、 GuardDuty 検出結果の Kubernetes ユーザーの詳細セクションで報告されたものと同じユーザー名で特定します。次の例を参照してください。ここでは、管理者ユーザーが検出結果で特定されています。

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. そのユーザーを から削除します ConfigMap。管理者ユーザーが削除された次の例を参照してください。

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. userType が [User] (ユーザー) の場合、またはユーザーが引き受けた [Role] (ロール) の場合:

a. そのユーザーのアクセスキーをローテーションします。

b. ユーザーがアクセス権を有していたシークレットをローテーションします。

c. 詳細については、「マイ AWS アカウントが侵害されている可能性がある」の情報を確認してください。

検出結果に `resource.accessKeyDetails` セクションがない場合、ユーザーは Kubernetes サービスアカウントです。

サービスアカウント – サービスアカウントはポッドのアイデンティティを提供し、次の形式のユーザー名で識別できます: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*。

サービスアカウントへのアクセス権を取り消すには:

1. サービスアカウントの認証情報をローテーションします。
2. 次のセクションでポッドの侵害に関するガイダンスを確認します。

侵害された可能性のある Kubernetes ポッドの修復

が `resource.kubernetesDetails.kubernetesWorkloadDetails`セクション内でポッドまたはワークロードリソースの詳細 GuardDuty を指定すると、そのポッドまたはワークロードリソースが侵害された可能性があります。 GuardDuty 検出結果は、1 つのポッドが侵害されたこと、または上位レベルのリソースを介して複数のポッドが侵害されたことを示している可能性があります。侵害されたポッドを特定する方法のガイダンスについては、次の侵害シナリオを参照してください。

単一のポッドの侵害

`resource.kubernetesDetails.kubernetesWorkloadDetails` セクション内の `type` フィールドが [Pod] (ポッド) である場合、検出結果は単一のポッドを特定します。名前フィールドはポッドの `name` であり、`namespace` フィールドはその名前空間です。

ポッドを実行しているワーカーノードを識別する方法については、「問題のあるポッドとワーカーノードの特定」を参照してください。

ワークロードリソースを通じて侵害されたポッド

`type` セクション内の `resource.kubernetesDetails.kubernetesWorkloadDetails` フィールドが、`Deployment` などの [Workload Resource] (ワークロードリソース) を識別している場合、そのワークロードリソース内のすべてのポッドが侵害されている可能性があります。

ワークロードリソースのすべてのポッドとそれらが実行されているノードを識別する方法については、「ワークロード名 を使用して問題のあるポッドとワーカーノードを特定する」を参照してください。

サービスアカウントを通じて侵害されたポッド

GuardDuty 検出結果によって `resource.kubernetesDetails.kubernetesUserDetails`セクションでサービスアカウントが特定された場合、識別されたサービスアカウントを使用するポッドが侵害されている可能性があります。検出結果によって報告されたユーザー名は、次の形式の場合はサービスアカウントです: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*。

サービスアカウントを使用してすべてのポッドを識別し、ポッドが実行されているノードを識別する方法については、「サービスアカウント名 を使用して問題のあるポッドとワーカーノードを特定する」を参照してください。

侵害されたすべてのポッドとそれらが実行されているノードを特定したら、「Amazon EKS ベストプラクティスガイド」を参照して、ポッドを分離し、その認証情報をローテーションし、フォレンジック分析のためにデータを収集します。

侵害された可能性のあるポッドを修復するには :

1. ポッドを侵害した脆弱性を特定します。
2. その脆弱性の修復を実装し、新しい代替ポッドを起動します。
3. 脆弱なポッドを削除します。

   詳細については、「侵害されたポッドまたはワークロードリソースを再デプロイする」を参照してください。

ポッドが他の AWS リソースにアクセスできるようにする IAM ロールがワーカーノードに割り当てられている場合は、それらのロールをインスタンスから削除して、攻撃によるさらなる損害を防ぎます。同様に、ポッドに IAM ロールが割り当てられている場合は、他のワークロードに影響を与えることなく、ロールから IAM ポリシーを安全に削除できるかどうかを評価します。

侵害された可能性のあるコンテナイメージの修復

GuardDuty 検出結果がポッドの侵害を示している場合、ポッドの起動に使用されるイメージは、潜在的に悪意のあるものであるか、侵害されている可能性があります。 GuardDuty 検出結果は、`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image`フィー

ルド内のコンテナイメージを識別します。マルウェアがないかを調べるためにスキャンして、イメージが悪意のあるものであるかどうかを判断できます。

侵害された可能性のあるコンテナイメージを修復するには：

1. 直ちにイメージの使用を停止し、イメージリポジトリから削除します。
2. 侵害された可能性のあるイメージを使用して、すべてのポッドを特定します。

   詳細については、「脆弱性または侵害された可能性のあるコンテナイメージとワーカーノードを持つポッドを特定する」を参照してください。
3. 侵害された可能性のあるポッドを分離し、認証情報をローテーションして、分析のためにデータを収集します。詳細については、「Amazon EKS ベストプラクティスガイド」を参照してください。
4. 侵害された可能性のあるイメージを使用して、すべてのポッドを削除します。

侵害された可能性のある Kubernetes ノードの修復

GuardDuty 検出結果で識別されたユーザーがノード ID を表す場合、または検出結果が特権コンテナの使用を示している場合、検出結果はノードの侵害を示している可能性があります。

[username] (ユーザーネーム) フィールドの形式が次の場合、ユーザーアイデンティティはワーカーノードです: `system:node:node name`。例えば、`system:node:ip-192-168-3-201.ec2.internal` です。これは、攻撃者がノードへのアクセスを取得し、ノードの認証情報を使用して Kubernetes API エンドポイントと通信していることを示すものです。

検出結果では、検出結果にリストされている 1 つ以上のコンテナの `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` 検出結果フィールドが `True` に設定されている場合に、特権コンテナの使用を示します。

侵害された可能性のあるノードを修復するには：

1. ポッドを分離し、認証情報をローテーションして、フォレンジック分析のためにデータを収集します。

   詳細については、「Amazon EKS ベストプラクティスガイド」を参照してください。
2. 侵害された可能性のあるノードで実行されているすべてのポッドが使用するサービスアカウントを特定します。許可を確認し、必要に応じてサービスアカウントをローテーションします。

3. 侵害された可能性のあるノードを終了します。

Runtime Monitoring 検出結果の修正

アカウントのランタイムモニタリングを有効にすると、Amazon GuardDuty Runtime Monitoring の検出結果タイプ AWS は環境内の潜在的なセキュリティ問題を示す情報を生成する場合があります。潜在的なセキュリティ問題は、侵害された Amazon EC2 インスタンスもしくはコンテナワークロード、Amazon EKS クラスター、またはご利用の AWS 環境での侵害された認証情報セットを示します。セキュリティエージェントは、複数のリソースタイプからのランタイムイベントを監視します。侵害の可能性があるリソースを特定するには、 GuardDuty生成された結果の詳細でリソースタイプをコンソールに表示します。次のセクションでは、リソースのタイプごとに推奨される修復手順について説明します。

Instance

検出結果の [リソースタイプ] が [インスタンス] の場合は、EC2 インスタンスまたは EKS ノードのいずれかが侵害されている可能性があることを示しています。

- 侵害された EKS ノードを修復するには、「侵害された可能性のある Kubernetes ノードの修復」を参照してください。
- 侵害された EC2 インスタンスを修正するには、「侵害された可能性のある Amazon EC2 インスタンスの修復」を参照してください。

EKSCluster

検出結果の詳細の [リソースタイプ] が [EKSCluster] の場合は、EKS クラスター内のポッドまたはコンテナが危険にさらされている可能性があることを示しています。

- 侵害されたポッドを修復するには、「侵害された可能性のある Kubernetes ポッドの修復」を参照ください。
- 侵害されたコンテナイメージを修復するには、「侵害された可能性のあるコンテナイメージの修復」を参照してください。

ECSCluster

検出結果の詳細の [リソースタイプ] が [ECSCluster] の場合は、ECS タスク内の ECS タスクまたはコンテナが危険にさらされている可能性があることを示しています。

1. 影響を受ける ECS クラスターを特定します

   GuardDuty ランタイムモニタリングの結果では、結果の詳細パネルまたは結果の JSON `resource.ecsClusterDetails` のセクションに ECS クラスターの詳細が表示されます。

2. 影響を受ける ECS タスクを特定

   GuardDuty ランタイムモニタリングの結果では、結果の詳細パネルまたは結果の JSON `resource.ecsClusterDetails.taskDetails` のセクションに ECS タスクの詳細が表示されます。

3. 影響を受けるタスクを分離

   タスクへの送受信トラフィックをすべて拒否して、影響を受けたタスクを分離します。すべてのトラフィックを拒否するルールは、タスクへのすべての接続を切断することによって、すでに進行中の攻撃を阻止するのに役立ちます。

4. 侵害されたタスクを修復

   a. タスクを侵害した脆弱性を特定します。

   b. その脆弱性に対する修正を実装し、代替タスクを新たに開始します。

   c. 脆弱なタスクを停止します。

Container

検出結果の詳細の [リソースタイプ] が [コンテナ] の場合は、スタンドアロンコンテナが危険にさらされている可能性があることを示しています。

- 修正するには、「侵害された可能性のあるスタンドアロンコンテナの修復」を参照してください。
- 同じコンテナイメージを使用して複数のコンテナにわたって検出結果が生成される場合は、「侵害された可能性のあるコンテナイメージの修復」を参照してください。
- コンテナが基盤となる EC2 ホストにアクセスした場合、関連するインスタンスの認証情報が侵害されている可能性があります。詳細については、「侵害された可能性のある AWS 認証情報の修正」を参照してください。
- 潜在的に悪意のある攻撃者が基盤となる EKS ノードまたは EC2 インスタンスにアクセスした場合は、[EKSCluster] タブと [インスタンス] タブで推奨される修復方法を参照してください。

侵害されたコンテナイメージの修復

GuardDuty 検出結果からタスクの侵害が判明した場合、そのタスクを起動するために使用されるイメージが悪意のあるものであるか、侵害されている可能性があります。 GuardDuty 検出結果によって、`resource.ecsClusterDetails.taskDetails.containers.image`フィールド内のコンテナイメージが特定されます。マルウェアの有無を調べるためにスキャンして、イメージが悪意のあるものであるかどうかを判断できます。

侵害されたコンテナイメージを修復

1. 直ちにイメージの使用を停止し、イメージリポジトリから削除します。
2. このイメージを使用しているタスクをすべて特定します。
3. 侵害されたイメージを使用しているすべてのタスクを停止します。侵害されたイメージの使用を停止するよう、タスクの定義を更新します。

侵害された可能性のあるデータベースの修復

GuardDuty サポートされているデータベースを有効にすると、 での疑わしいログイン動作や異常なログイン動作RDS Protection の検出結果タイプを示す が生成されますGuardDuty RDS Protection。RDS ログインアクティビティを使用して、 はログイン試行の異常なパターンを特定することで脅威 GuardDuty を分析し、プロファイリングします。

> **Note**
>
> 検出結果タイプに関する完全な情報にアクセスするには、検出結果の表 から選択します。

ご利用の AWS 環境で侵害された可能性のある Amazon Aurora データベースを修復するには、以下の推奨ステップに従います。

トピック

- ログインイベントの成功により、侵害された可能性のあるデータベースの修復
- ログインイベントの失敗により、侵害された可能性のあるデータベースの修正
- 漏えいした可能性のある認証情報の修正
- ネットワークアクセスを制限する

ログインイベントの成功により、侵害された可能性のあるデータベースの修復

以下の推奨手順は、ログインイベントの成功に関連して異常な動作をする、侵害された可能性のある Aurora データベースを修復する際に役に立ちます。

1. 影響を受けたデータベースとユーザーを特定します。

   生成された GuardDuty 検出結果には、影響を受けるデータベースの名前と対応するユーザーの詳細が表示されます。詳細については、「検出結果の詳細」を参照してください。
2. この動作が予期されるものであるか、または予期されないものであるかを確認します。

   次のリストは、 が検出結果を生成する原因 GuardDuty となった可能性のあるシナリオを示しています。

   - 長い時間が経過した後にデータベースにログインするユーザー。
   - データベースにときどきログインするユーザー (四半期ごとにログインする財務アナリストなど)。
   - ログイン試行に成功し、データベースを侵害した可能性がある疑わしい攻撃者。
3. 予期しない動作が発生した場合は、このステップを開始してください。

   1. データベースアクセスを制限する

      疑わしいアカウントおよびこのログインアクティビティのソースによるデータベースへのアクセスを制限します。詳細については、漏えいした可能性のある認証情報の修正およびネットワークアクセスを制限するを参照してください。
   2. 影響を評価し、アクセスされた情報を特定します。

      - 可能であれば、監査ログを確認して、アクセスされた可能性のある情報を特定します。詳細については、「Amazon Aurora ユーザーガイド」の「Amazon Aurora DB クラスターでの、イベント、ログ、およびストリーミングのモニタリング」を参照してください。
      - 機密情報または保護された情報にアクセスされたか、または変更が加えられたかどうかを確認します。

ログインイベントの失敗により、侵害された可能性のあるデータベースの修正

以下の推奨手順は、ログインイベントの失敗に関連して異常な動作をする、侵害された可能性がある Aurora データベースを修復する際に役に立ちます。

1. 影響を受けたデータベースとユーザーを特定します。

   生成された GuardDuty 検出結果には、影響を受けるデータベースの名前と対応するユーザーの詳細が表示されます。詳細については、「検出結果の詳細」を参照してください。

2. ログインに失敗したソースを特定します。

   生成された GuardDuty 検出結果は、検出結果パネルのアクターセクションの下に IP アドレスと ASN 組織 (パブリック接続の場合) を提供します。

   自律システム (AS) は、1 つ以上のネットワークオペレーターによって実行される 1 つ以上の IP プレフィックス (ネットワーク上でアクセス可能な IP アドレスのリスト) のグループで、明確に定義された単一のルーティングポリシーを維持します。ネットワークオペレーターには、ネットワーク内のルーティングを制御したり、他のインターネットサービスプロバイダー (ISP) とルーティング情報を交換したりするための AS 番号 (ASN) が必要です。

3. この動作が予期しないものであることを確認します。

   このアクティビティが、データベースへのさらなる不正アクセスを試みているものかどうかを次のように検証します。

   - ソースが内部にある場合は、アプリケーションが誤って設定されていないかどうかを調べて、接続が繰り返し試行されていないかを確認します。
   - これが外部の攻撃者である場合は、該当するデータベースが一般公開されているかどうか、または設定が誤っていないかどうか調べ、悪意のある攻撃者が一般的なユーザー名に対してブルートフォース攻撃を仕掛けられるようになっていないかを確認します。

4. 予期しない動作が発生した場合は、このステップを開始してください。

   1. データベースアクセスを制限する

      疑わしいアカウントおよびこのログインアクティビティのソースによるデータベースへのアクセスを制限します。詳細については、漏えいした可能性のある認証情報の修正およびネットワークアクセスを制限するを参照してください。

2. 根本原因を分析し、このアクティビティを引き起こした可能性のあるステップを特定します。

   アクティビティによってネットワークポリシーが変更され、安全でない状態になったときに通知を受けるようにアラートを設定します。詳細については、「AWS Network Firewall デベロッパーガイド」の「AWS Network Firewallにおけるファイアウォールポリシー」を参照してください。

漏えいした可能性のある認証情報の修正

GuardDuty 検出結果は、検出結果で識別されたユーザーが予期しないデータベース操作を実行したときに、影響を受けたデータベースのユーザー認証情報が侵害されたことを示している可能性があります。ユーザーを特定するには、コンソールの検出結果パネル内の [RDS DB user details] (RDS DB ユーザー詳細) セクション、または検出結果 JSON の `resource.rdsDbUserDetails` を確認します。これらのユーザーの詳細には、ユーザー名、使用したアプリケーション、アクセスしたデータベース、SSL バージョン、認証方法が含まれます。

- 検出結果に関係する特定のユーザーのアクセス権限を取り消したり、パスワードを変更したりするには、「Amazon Aurora ユーザーガイド」の「Amazon Aurora MySQL でのセキュリティ」または「Amazon Aurora PostgreSQL でのセキュリティ」を参照してください。
- を使用して AWS Secrets Manager 、Amazon Relational Database Service (RDS) データベースのシークレットを安全に保存し、自動的にローテーションします。詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager のチュートリアル」を参照してください。
- IAM データベース認証を使用すると、パスワードなしでデータベースユーザーのアクセスを管理できます。詳細については、「Amazon Aurora ユーザーガイド」の「IAM データベース認証」を参照してください。

  詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS 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。

ネットワークアクセスを制限する

GuardDuty 検出結果は、データベースがアプリケーションや Virtual Private Cloud (VPC) の外部からアクセスできることを示している場合があります。検出結果に示されているリモート IP アドレスが予期しない接続元である場合は、セキュリティグループを監査してください。データベースにアタッチされたセキュリティグループのリストは、https://

console.aws.amazon.com/rds/ コンソールの [セキュリティグループ]、または検出結果 JSON の `resource.rdsDbInstanceDetails.dbSecurityGroups` で確認できます。セキュリティグループの設定については、「Amazon RDS ユーザーガイド」の「セキュリティグループによるアクセス制御」を参照してください。

ファイアウォールを使用している場合は、ネットワークアクセスコントロールリスト (NACL) を再設定して、データベースへのネットワークアクセスを制限します。詳細については、「AWS Network Firewall デベロッパーガイド」の「AWS Network Firewallのファイアウォール」を参照してください。

侵害された可能性のある Lambda 関数の修復

が Lambda Protection の検出結果 GuardDuty を生成し、アクティビティが予期しない場合、Lambda 関数が侵害されている可能性があります。侵害された Lambda 関数を修正するには、以下の手順を実行することをお勧めします。

Lambda Protection の検出結果を修正するには

1. 侵害された可能性のある Lambda 関数のバージョンを特定します。

   Lambda Protection の検出 GuardDuty 結果には、検出結果の詳細にリストされている Lambda 関数に関連付けられた名前、Amazon リソースネーム (ARN)、関数のバージョン、およびリビジョン ID が表示されます。
2. 潜在的に疑わしいアクティビティのソースを特定します。

   a. 検出結果に含まれる Lambda 関数のバージョンに関連するコードを確認してください。
   b. インポートされたライブラリと、検出結果に関係する Lambda 関数バージョンのレイヤーを確認します。
   c. Amazon Inspector で AWS Lambda 関数のスキャンを有効にしている場合は、検出結果に関係する Lambda 関数に関連する Amazon Inspector の検出結果を確認します。
   d. AWS CloudTrail ログを確認して、関数の更新の原因となったプリンシパルを特定し、アクティビティが承認または予期されたことを確認します。
3. 侵害された可能性のある Lambda 関数 を修正します。

   a. 検出結果に関係する Lambda 関数の実行トリガーを無効にします。詳細については、「」を参照してくださいDeleteFunctionEventInvokeConfig。
   b. Lambda コードを確認し、ライブラリのインポートと Lambda 関数レイヤーを更新して、潜在的に疑わしいライブラリとレイヤーを削除します。

c. 検出結果に関係した Lambda 関数に関連する Amazon Inspector の検出結果を軽減します。

Amazon での複数のアカウントの管理 GuardDuty

AWS 環境に複数のアカウントがある場合は、1 つのアカウントを管理者 AWS アカウントとして指定することで管理できます。その後、他のアカウント AWS をメンバーアカウントとしてこの管理者アカウントに関連付けることができます。この指定された GuardDuty 管理者アカウントは、保護プランを設定できます。 アカウントを管理者アカウントに関連付けるには、 を使用して組織を作成する方法 AWS Organizations と、この組織に属している管理者アカウントと 1 つ以上のメンバーアカウントの両方を作成する方法、または を介して AWS アカウントに招待を送信する方法の 2 GuardDuty つがあります GuardDuty。

GuardDuty では、 AWS Organizations メソッドの使用を推奨しています。組織の設定については、「AWS Organizations ユーザーガイド」の「組織の作成」を参照してください。

を使用した複数のアカウントの管理 AWS Organizations

GuardDuty 管理者アカウントとして指定するアカウントが の組織の一部である場合は AWS Organizations、そのアカウントを の組織の委任管理者として指定できます GuardDuty。委任された管理者として登録されているアカウントは自動的に GuardDuty 管理者アカウントになります。

この管理者アカウントを使用して、メンバーアカウントとしてそのアカウントを追加するときに、組織 AWS アカウント 内の任意の GuardDuty に対して を有効におよび管理できます。

招待によってメンバーアカウントが関連付けられている GuardDuty 管理者アカウントがすでにある場合は、そのアカウントを組織の GuardDuty 委任管理者として登録できます。これを行うと、現在関連付けられているすべてのメンバーアカウントがメンバーのままになり、 でアカウントを管理するという追加機能を最大限に活用できます GuardDuty AWS Organizations。

組織 GuardDuty を通じて で複数のアカウントをサポートする方法の詳細については、「」を参照してくださいによる GuardDuty アカウントの管理 AWS Organizations。

招待による複数のアカウントの管理

関連付けるアカウントが組織の一部でない場合は、 で管理者アカウントを指定 GuardDuty し、管理者アカウントを使用して他の を AWS アカウント メンバーアカウントに招待できます。招待されたアカウントが招待を受け入れると、そのアカウントは管理者アカウントに関連付けられた GuardDuty メンバーアカウントになります。

招待による複数のアカウントのサポートの詳細については、 GuardDuty 「」を参照してください招待による GuardDuty アカウントの管理。

GuardDuty 管理者アカウントとメンバーアカウントの関係を理解する

GuardDuty マルチアカウント環境で を使用すると、管理者アカウントはメンバーアカウント GuardDuty に代わって の特定の側面を管理できます。管理者アカウントが実行できる主な機能は次のとおりです。

- 関連付けられたメンバーアカウントを追加および削除する。このためのプロセスは、アカウントが組織を通じて関連付けられているか、招待によって関連付けられているかによって異なります。
- の有効化と停止など、関連するメンバーアカウント GuardDuty 内の のステータスを管理します GuardDuty。

> **Note**
>
> で管理される委任された管理者アカウントは、メンバーとして追加されたアカウント GuardDuty で AWS Organizations 自動的に を有効にします。

- 抑制ルール、信頼できる IP リスト、脅威リストの作成と管理を通じて、 GuardDuty ネットワーク内の検出結果をカスタマイズします。マルチアカウント環境では、これらの機能の設定は委任された GuardDuty 管理者アカウントでのみ使用できます。メンバーアカウントはこの設定を更新できません。

次の表は、 GuardDuty 管理者アカウントとメンバーアカウントの関係の詳細を示しています。

この表で以下の点に注意してください。

- 自己 – アカウントは、自分のアカウントに対してのみ、リストされたアクションを実行できます。
- 任意 – アカウントは、関連付けられたアカウントに対してリストされたアクションを実行できます。
- すべて – アカウントはリストされたアクションを実行でき、関連付けられたすべてのアカウントに適用されます。通常、このアクションを実行するアカウントは指定された GuardDuty 管理者アカウントです。

ダッシュ (—) が付いたテーブルセルは、アカウントがリストされたアクションを実行できないことを示します。

[アクション]	経由 AWS Organizations		招待により	
	委任 GuardDuty 管理者アカウント	関連付けられたメンバーアカウント	委任 GuardDuty 管理者アカウント	関連付けられたメンバーアカウント
を有効にする GuardDuty	すべて	–	自分	自分
組織全体で GuardDuty を自動的に有効にする (ALL、NEW、NONE)	すべて	–	–	–
GuardDuty ステータスに関係なく、すべての Organizations メンバーアカウントを表示する	すべて	–	–	–
検出結果サンプルを生成する	Self	自分	自分	自分
すべての GuardDuty 結果を表示する	すべて	Self	すべて	Self
GuardDuty 結果のアーカイブ	すべて	–	任意	–
抑制ルールを適用する	すべて	–	すべて	–

信頼できる IP リストまたは脅威リストを作成する	すべて	–	すべて	–
信頼できる IP リストまたは脅威リストを更新する	すべて	–	すべて	–
信頼できる IP リストまたは脅威リストを削除する	すべて	–	すべて	–
EventBridge 通知頻度を設定する	すべて	–	すべて	自分
検出結果をエクスポートする Amazon S3 の場所を設定する	すべて	–	すべて	自分
組織全体で 1 つ以上のオプションの保護プランを有効にする (ALL、NEW、NONE) これには、Malware Protection for S3 は含まれません。	すべて	–	–	–

個々のアカウントの GuardDuty 保護プランを有効にする これには、Malware Protection for S3 は含まれません。	すべて	–	すべて	Self
S3 のマルウェア保護	–	自分	–	自分
メンバーアカウントの関連付けを解除する	すべて	–	すべて	–
管理者アカウントとの関連付けを解除する	–	セルフ [#]	–	自分
関連付けが解除されたメンバーアカウントを削除する	すべて	–	すべて	–
一時停止 GuardDuty	任意[*]	–	任意[*]	–
無効化 GuardDuty	任意[*]	–	任意[*]	–

[#]委任 GuardDuty 管理者アカウントがALL組織メンバーに対して自動有効化設定を設定していない場合にのみ、アカウントがこのアクションを実行できることを示します。

[*]このアカウントに対して実行する前に、関連するすべてのアカウントに対してこのアクションを実行する必要があることを示します。これらのアカウントの関連付けを解除したら、削除する必要があ

ります。組織でこれらのタスクを実行する方法の詳細については、「」を参照してください内の組織の維持 GuardDuty。

による GuardDuty アカウントの管理 AWS Organizations

AWS 組織 GuardDuty で を使用する場合、その組織の管理アカウントは、組織内の任意のアカウントを委任された GuardDuty 管理者アカウントとして指定できます。この管理者アカウントでは、GuardDuty は指定された でのみ自動的に有効になります AWS リージョン。このアカウントには、そのリージョン内の組織内のすべてのアカウント GuardDuty に対して を有効化および管理するためのアクセス許可もあります。管理者アカウントは、 のメンバーを表示し、この AWS 組織にメンバーを追加できます。

招待によって関連付けられたメンバーアカウントを持つ GuardDuty 管理者アカウントをすでに設定していて、そのメンバーアカウントが同じ組織の一部である場合、組織の委任 GuardDuty 管理者アカウントを設定すると、そのタイプは招待によって組織経由で変わります。委任された GuardDuty 管理者アカウントが同じ組織に属していない招待によって以前にメンバーを追加した場合、そのタイプは招待によって のままになります。どちらの場合も、以前に追加されたアカウントは、組織の委任 GuardDuty 管理者アカウントに関連付けられているメンバーアカウントです。

組織外にいる場合でも、引き続きアカウントをメンバーとして追加できます。詳細については、招待によるアカウントの追加と管理または GuardDuty コンソールを使用した委任 GuardDuty 管理者アカウントの指定とメンバーの管理を参照してください。

内容

- 委任 GuardDuty 管理者アカウントを指定する際の考慮事項と推奨事項
- 委任された GuardDuty 管理者アカウントを指定するために必要なアクセス許可
- GuardDuty コンソールを使用した委任 GuardDuty 管理者アカウントの指定とメンバーの管理
- API を使用した GuardDuty 委任 GuardDuty 管理者アカウントの指定とメンバーの管理
- 内の組織の維持 GuardDuty
- 委任 GuardDuty 管理者アカウントの変更

委任 GuardDuty 管理者アカウントを指定する際の考慮事項と推奨事項

以下の考慮事項と推奨事項は、委任された GuardDuty 管理者アカウントが でどのように動作するかを理解するのに役立ちます GuardDuty。

委任 GuardDuty 管理者アカウントは、最大 50,000 人のメンバーを管理できます。

委任 GuardDuty 管理者アカウントあたり 50,000 のメンバーアカウントに制限があります。これには、 を通じて追加されたメンバーアカウント AWS Organizations 、または GuardDuty 管理者アカウントの組織への招待を受け入れたメンバーアカウントが含まれます。ただし、 AWS 組織内に 50,000 を超えるアカウントが存在する可能性があります。

メンバーアカウントの上限である 50,000 を超えると、 から通知が送信され CloudWatch AWS Health Dashboard、指定された委任 GuardDuty 管理者アカウントに E メールが送信されます。

委任 GuardDuty 管理者アカウントはリージョン別です。

とは異なり AWS Organizations、 はリージョンサービス GuardDuty です。委任された GuardDuty 管理者アカウントとそのメンバーアカウントは、 GuardDuty 有効にした各リージョン AWS Organizations で を通じて追加する必要があります。組織管理アカウントが米国東部 (バージニア北部) でのみ委任された GuardDuty 管理者アカウントを指定している場合、委任された GuardDuty 管理者アカウントは、そのリージョンの組織に追加されたメンバーアカウントのみを管理します。 GuardDuty が利用可能なリージョンの機能パリティの詳細については、「」を参照してくださいリージョンとエンドポイント。

オプトインリージョンの特殊なケース

- 委任された GuardDuty 管理者アカウントがオプトインリージョンをオプトアウトすると、組織 GuardDuty で自動有効化設定が新しいメンバーアカウントのみ (NEW) またはすべてのメンバーアカウント () に設定されている場合でもALL、 GuardDuty現在 GuardDuty 無効になっている組織内のメンバーアカウントに対して有効にすることはできません。メンバーアカウントの設定については、GuardDuty コンソールのナビゲーションペインでアカウントを開くか、ListMembers API を使用します。
- GuardDuty 自動有効化設定を に設定する場合はNEW、次のシーケンスが満たされていることを確認してください。

  1. メンバーアカウントはオプトインリージョンにオプトインします。
  2. のメンバーアカウントを の組織に追加します AWS Organizations。

  これらのステップの順序を変更すると、メンバーアカウントNEWが組織に新しくなくなるため、 で GuardDuty の自動有効化設定は特定のオプトインリージョンでは機能しません。GuardDuty には、次の 2 つの代替ソリューションがあります。

  - 新規および既存のメンバーアカウントALLを含む GuardDuty 自動有効化設定を に設定します。この場合、これらのステップの順序は関係ありません。

- メンバーアカウントが既に組織の一部である場合は、 GuardDuty コンソールまたは API を使用して、特定のオプトインリージョンでこのアカウントの設定を個別に管理 GuardDuty します。

すべての で同じ委任 GuardDuty 管理者アカウントを持つように AWS 組織に対して推奨されます AWS リージョン。

を有効に AWS リージョン したすべての で、同じ委任 GuardDuty 管理者アカウントを組織に指定することをお勧めします GuardDuty。あるリージョンでアカウントを委任 GuardDuty 管理者アカウントとして指定する場合は、他のすべてのリージョンで委任 GuardDuty 管理者アカウントと同じアカウントを使用することをお勧めします。

新しい委任 GuardDuty 管理者アカウントはいつでも指定できます。既存の委任 GuardDuty 管理者アカウントの削除の詳細については、「」を参照してください委任 GuardDuty 管理者アカウントの変更。

組織の管理アカウントを委任 GuardDuty 管理者アカウントとして設定することはお勧めしません。

組織の管理アカウントは、委任された GuardDuty 管理者アカウントとすることができます。ただし、 AWS のセキュリティのベストプラクティスは最小特権の原則に従っており、この設定は推奨されていません。

委任された GuardDuty 管理者アカウントを変更しても、メンバーアカウントの GuardDuty は無効になりません。

委任された GuardDuty 管理者アカウントを削除すると、 はこの委任された GuardDuty 管理者アカウントに関連付けられているすべてのメンバーアカウント GuardDuty を削除します。GuardDuty 保持は、これらのすべてのメンバーアカウントに対して有効のままです。

委任された GuardDuty 管理者アカウントを指定するために必要なアクセス許可

委任された GuardDuty 管理者アカウントを委任する場合、 GuardDuty および特定の AWS Organizations API アクションを有効にするアクセス許可が必要です。IAM ポリシーの最後に次のステートメントを追加することで、これらの許可を付与できます。

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
```

```
            "organizations:EnableAWSServiceAccess",
            "organizations:RegisterDelegatedAdministrator",
            "organizations:ListDelegatedAdministrators",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:DescribeOrganizationalUnit",
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListAccounts"
        ],
        "Resource": "*"
}
```

さらに、 AWS Organizations 管理アカウントを委任された GuardDuty 管理者アカウントとして指定する場合、 GuardDutyそのエンティティには を初期化するためのCreateServiceLinkedRoleアクセス許可が必要です GuardDuty。これを行うには、次のステートメントを IAM ポリシーに追加し、*111122223333* を組織の管理アカウントの AWS アカウント ID に置き換えます。

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

GuardDuty コンソールを使用した委任 GuardDuty 管理者アカウントの指定とメンバーの管理

内容

ステップ 1 – 組織の委任 GuardDuty 管理者アカウントを指定する

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

   ログインするには、 AWS Organizations 組織の管理者アカウントの認証情報を使用します。
2. 管理アカウント GuardDuty に対して を既に有効にしている場合は、このステップをスキップして次のステップに従います。

   GuardDuty まだ を有効にしていない場合は、「開始方法」を選択し、「ようこそ GuardDuty」ページで委任 GuardDuty 管理者アカウントを指定します。

   > **Note**
   >
   > 委任 GuardDuty 管理者アカウントがそのアカウント GuardDuty で を有効にして管理できるように、管理アカウントには GuardDuty サービスにリンクされたロール (SLR) が必要です。管理アカウントのリージョン GuardDuty で を有効にすると、この SLR が自動的に作成されます。
3. 管理アカウント GuardDuty で を有効にした後、このステップを実行します。 GuardDuty コンソールのナビゲーションペインで、設定 を選択します。設定ページで、組織の委任 GuardDuty 管理者アカウントとして指定するアカウントの 12 桁の AWS アカウント ID を入力します。

   新しく指定した委任 GuardDuty 管理者アカウント GuardDuty に対して を有効にしてください。有効にしないと、何も実行できません。
4. [委任] を選択します。
5. (推奨) 前のステップを繰り返して、 GuardDuty 有効に AWS リージョン した各 の委任 GuardDuty 管理者アカウントを指定します。

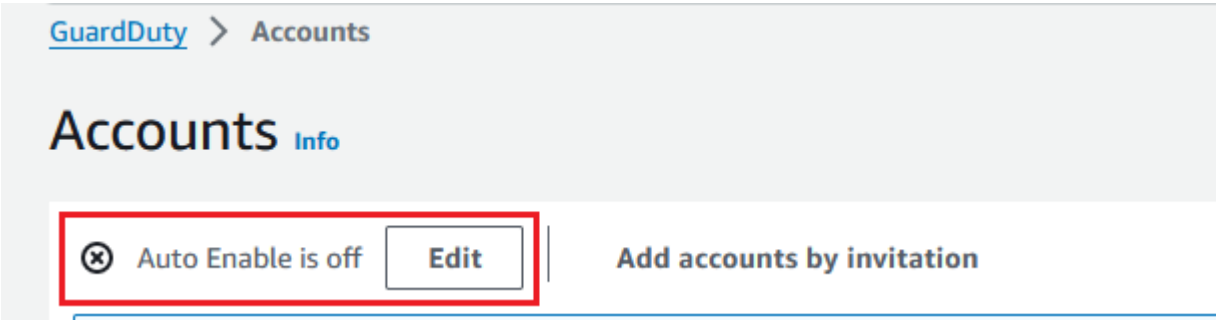
ステップ 2 – 組織の自動有効化設定を構成する

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

   サインインするには、 GuardDuty 管理者アカウントの認証情報を使用します。
2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

   アカウントページには、組織に属するメンバーアカウントに代わって、自動有効化 GuardDuty するための設定オプションとオプションの保護プランが GuardDuty 管理者アカウントに表示されます。

3. 既存の自動有効化設定を更新するには、編集 を選択します。



このサポートは、 GuardDuty でサポートされているすべてのオプション保護プランを設定するために利用できます AWS リージョン。メンバーアカウント GuardDuty に代わって、 の次の設定オプションのいずれかを選択できます。

- すべてのアカウントで を有効にする (**ALL**) — 選択すると、組織内のすべてのアカウントに対応するオプションが有効になります。これには、組織に参加した新しいアカウントと、組織から一時停止または削除された可能性のあるアカウントが含まれます。これには、委任された GuardDuty 管理者アカウントも含まれます。

  > **Note**
  >
  > すべてのメンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

- 新しいアカウントで自動有効化 (**NEW**) – 組織への新規メンバーアカウントのみに対して、GuardDuty を有効にするか、オプションの保護プランを自動的に有効にするかを選択します。
- (**NONE**) を有効にしない – 組織内の新しいアカウントに対応するオプションを有効にしないように を選択します。この場合、 GuardDuty 管理者アカウントは各アカウントを個別に管理します。

  自動有効化設定を ALLまたは から NEWに更新してもNONE、このアクションは既存のアカウントに対応するオプションを無効にしません。この設定は、組織に参加する新しいアカウントに適用されます。自動有効化設定を更新すると、対応するオプションが有効になっている新しいアカウントはありません。

> **Note**
>
> 委任された GuardDuty 管理者アカウントがオプトインリージョンをオプトアウトすると、組織 GuardDuty で自動有効化設定が新しいメンバーアカウントのみ (NEW) またはすべてのメンバーアカウント () に設定されている場合でもALL、 GuardDuty現在 GuardDuty 無効になっている組織内のメンバーアカウントに対して有効にすることはできません。メンバーアカウントの設定については、GuardDuty コンソールのナビゲーションペインでアカウントを開くか、 ListMembers API を使用します。

4. [変更の保存] を選択します。
5. (オプション) 各リージョンで同じ設定を使用する場合は、サポートされている各リージョンで設定を個別に更新します。

   一部のオプションの保護プランは、 AWS リージョン GuardDuty が利用可能なすべての で利用できない場合があります。詳細については、「リージョンとエンドポイント」を参照してください。

ステップ 3 – アカウントをメンバーとして組織に追加する

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

   ログインするには、委任された GuardDuty 管理者アカウントの認証情報を使用します。
2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

   アカウントテーブルには、[Organizations 経由] (AWS Organizations) または [招待による] のいずれかで追加されたすべてのアカウントが表示されます。メンバーアカウントが組織の GuardDuty 管理者アカウントに関連付けられていない場合、このメンバーアカウントのステータスはメンバー ではありません。
3. メンバーとして追加する 1 つまたは複数のアカウント ID を選択します。これらのアカウント ID の [タイプ] は [Organizations 経由] である必要があります。

   招待を通じて追加されたアカウントは、組織の一部ではありません。このようなアカウントは個別に管理できます。詳細については、「招待によるアカウントの管理」を参照してください。
4. [アクション] ドロップダウンを選択し、[メンバーを追加] を選択します。このアカウントをメンバーとして追加すると、自動有効化 GuardDuty 設定が適用されます。の設定に基づいてthe

section called “ステップ 1 – 組織の委任 GuardDuty 管理者アカウントを指定する”、これらのアカウントの設定が GuardDuty変更される場合があります。

5. ステータス列の下矢印を選択して、アカウントをメンバーステータスではないでソートし、現在のリージョンで GuardDuty が有効になっていない各アカウントを選択できます。

   アカウントテーブルにリストされているアカウントがまだメンバーとして追加されていない場合は、現在のリージョン GuardDuty ですべての組織アカウントに対して を有効にできます。ページ上部のバナーで [有効にする] を選択します。このアクションは、組織に参加する新しいアカウントに対して GuardDuty が有効になるように、自動有効化 GuardDuty 設定を自動的にオンにします。

6. アカウントをメンバーとして追加するには、[確認] を選択します。このアクションでは、選択したすべてのアカウント GuardDuty に対して も有効にします。アカウントの [ステータス] が [有効] に変わります。

7. (推奨) 各 でこれらのステップを繰り返します AWS リージョン。これにより、委任された GuardDuty 管理者アカウントは、 GuardDuty 有効にしたすべてのリージョンのメンバーアカウントの検出結果やその他の設定を管理できます。

   自動有効化機能を使用すると、組織の将来のすべてのメンバー GuardDuty に対して が有効になります。これにより、委任された GuardDuty 管理者アカウントは、 内で作成された、または組織に追加される新しいメンバーを管理できます。メンバーアカウントの数が 50,000 の制限に達すると、自動有効化機能は自動的にオフになります。メンバーアカウントを削除し、メンバーの合計数が 50,000 未満に減少すると、自動有効化機能が再びオンになります。

(オプション) ステップ 4 – 個々のアカウントの保護プランを設定する

[アカウント] ページを通じて個々のアカウントのために保護プランを設定できます。

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

   委任 GuardDuty 管理者アカウントの認証情報を使用します。

2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
3. 保護プランを設定するアカウントを 1 つ以上選択します。設定する保護プランごとに次のステップを繰り返します。

   a. [保護プランを編集] を選択します。
   b. 保護プランのリストから、設定する保護プランを 1 つ選択します。
   c. この保護プランについて実行するいずれかのアクションを選択し、[確認] を選択します。

d. 選択したアカウントについて、設定された保護プランに対応する列で、更新された設定が [有効] または [無効] として表示されます。

API を使用した GuardDuty 委任 GuardDuty 管理者アカウントの指定とメンバーの管理

内容

ステップ 1 – AWS 組織の委任 GuardDuty 管理者アカウントを指定する

1. 組織の管理アカウントの AWS アカウント の認証情報enableOrganizationAdminAccountを使用して を実行します。
   - または、 AWS Command Line Interface を使用してこれを行うことができます。次の AWS CLI コマンドは、現在のリージョンの委任 GuardDuty 管理者アカウントのみを指定します。次の AWS CLI コマンドを実行し、*111111111111* を委任 GuardDuty 管理者アカウントとして指定するアカウントの AWS アカウント ID に置き換えます。

     ```
     aws guardduty enable-organization-admin-account --admin-account-id 111111111111
     ```

     他のリージョンの委任 GuardDuty 管理者アカウントを指定するには、 AWS CLI コマンドでリージョンを指定します。次の例は、米国西部 (オレゴン) で委任 GuardDuty 管理者アカウントを有効にする方法を示しています。*us-west-2* は、 GuardDuty 必ず委任された GuardDuty 管理者アカウントを割り当てるリージョンに置き換えてください。

     ```
     aws guardduty enable-organization-admin-account --admin-account-id 111111111111
      --region us-west-2
     ```

     GuardDuty が利用可能な の詳細については、 AWS リージョン 「」を参照してくださいリージョンとエンドポイント。

GuardDuty が委任された GuardDuty 管理者アカウントに対して有効になっていない場合、アクションを実行することはできません。まだ有効にしていない場合は、新しく指定された委任 GuardDuty 管理者アカウント GuardDuty に対して を有効にしてください。

2. (推奨) 前のステップを繰り返して、 GuardDuty 有効に AWS リージョン した各 の委任 GuardDuty 管理者アカウントを指定します。

ステップ 2 - 組織の自動有効化の詳細設定を構成する

1. 1. 委任された GuardDuty 管理者アカウントの認証情報UpdateOrganizationConfigurationを使用して を実行し、組織のそのリージョンで GuardDuty およびオプションの保護プランを自動的に設定します。

   アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

   > **Note**
   >
   > さまざまな自動有効化設定の詳細については、autoEnableOrganization「メンバー」を参照してください。

   2. リージョンでサポートされているオプションの保護プランの自動有効化の設定を行うには、各保護プランの対応するドキュメントセクションに記載されているステップに従ってください。
   3. 現在のリージョンで組織の詳細設定を検証できます。describeOrganizationConfiguration を実行します。委任 GuardDuty 管理者アカウントのディテクター ID を必ず指定してください。

   > **Note**
   >
   > すべてのメンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。

   - 1. または、次の AWS CLI コマンドを実行して、組織に参加する新しいアカウント (NEW) 、すべてのアカウント ()、または組織内のアカウント (NONE) のいずれも有効または無効にしない GuardDuty リージョンで を自動的に有効ALLまたは無効にするように設

定します。詳細については、autoEnableOrganization「メンバー」を参照してください。必要に応じて、NEW を ALL または NONE に置き換える必要がある場合があります。で保護プランを設定するとALL、委任された GuardDuty 管理者アカウントでも保護プランが有効になります。組織設定を管理する委任 GuardDuty 管理者アカウントのディテクター ID を必ず指定してください。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、ListDetectors API を実行します。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

2. 現在のリージョンで組織の詳細設定を検証できます。委任 GuardDuty 管理者アカウントのディテクター ID を使用して、次の AWS CLI コマンドを実行します。

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0
```

2. （推奨) 委任 GuardDuty 管理者アカウントディテクター ID を使用して、各リージョンで前の手順を繰り返します。

> **Note**
>
> 委任された GuardDuty 管理者アカウントがオプトインリージョンをオプトアウトすると、組織 GuardDuty で自動有効化設定が新しいメンバーアカウントのみ (NEW) またはすべてのメンバーアカウント () に設定されている場合でもALL、 GuardDuty現在 GuardDuty 無効になっている組織内のメンバーアカウントに対して有効にすることはできません。メンバーアカウントの設定については、GuardDuty コンソールのナビゲーションペインでアカウントを開くか、 ListMembers API を使用します。

ステップ 3 – アカウントをメンバーとして組織に追加する

- 前のステップで指定した委任 GuardDuty 管理者アカウントの認証情報CreateMembersを使用して を実行します。

  委任された GuardDuty 管理者アカウントのリージョンレベルのディテクター ID と、GuardDuty メンバーとして追加するアカウントのアカウント詳細 (AWS アカウント IDsと対応

する E メールアドレス) を指定する必要があります。この API オペレーションを使用して 1 名以上のメンバーを作成できます。

組織CreateMembersで を実行すると、新しいメンバーアカウントが組織に参加すると、新しいメンバーの自動有効化設定が適用されます。既存のメンバーアカウントCreateMembersで を実行すると、組織設定は既存のメンバーにも適用されます。これにより、既存のメンバーアカウントの現在の設定が変更される場合があります。

AWS Organizations API リファレンス ListAccountsで を実行して、 AWS 組織内のすべてのアカウントを表示します。

> **Important**
>
> アカウントを GuardDuty メンバーとして追加すると、そのリージョンで が自動的に GuardDuty 有効になります。組織管理アカウントには例外があります。管理アカウントを GuardDuty メンバーとして追加する前に、 GuardDuty が有効になっている必要があります。

- または、 を使用することもできます AWS Command Line Interface。次の AWS CLI コマンドを実行し、必ず自分の有効なディテクター ID、 AWS アカウント ID、およびアカウント ID に関連付けられたメールアドレスを使用してください。

  アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  account-details AccountId=111122223333,Email=guardduty-member-name@amazon.com
  ```

  次の AWS CLI コマンドを実行すると、すべての組織メンバーのリストを表示できます。

  ```
  aws organizations list-accounts
  ```

このアカウントをメンバーとして追加すると、自動有効化 GuardDuty設定が適用されます。

内の組織の維持 GuardDuty

委任 GuardDuty 管理者アカウントとして、サポートされている各 の組織内のすべてのアカウントについて、 の設定 GuardDuty とオプションの保護プランを維持する責任があります AWS リージョン。以下のセクションでは、 GuardDuty またはそのオプションの保護プランの設定ステータスを維持するオプションについて説明します。

各リージョンで組織全体の設定ステータスを維持するには

- GuardDuty コンソールを使用して組織全体の自動有効化設定を設定する – 組織内のすべての (ALL) メンバーまたは組織に参加する新しい (NEW) メンバーに対して自動的に を有効にする GuardDuty か、組織内のメンバーのいずれかを自動有効化しない (NONE) ように選択できます。

  また、 内の保護プランに対して同じ設定または異なる設定を設定することもできます GuardDuty。

  組織内のすべてのメンバーアカウントの設定を更新するには、最大 24 時間かかる場合があります。
- API を使用して自動有効化設定を更新する – を実行してUpdateOrganizationConfiguration、組織のとそのオプションの保護プランを自動的に設定 GuardDutyします。CreateMembers を実行して組織に新しいメンバーアカウントを追加すると、設定された設定が自動的に適用されます。既存のメンバーアカウントCreateMembersで を実行すると、組織設定は既存のメンバーにも適用されます。これにより、既存のメンバーアカウントの現在の設定が変更される場合があります。

  組織内のすべてのアカウントを表示するには、 AWS Organizations API リファレンス ListAccounts で を実行します。

各リージョンのメンバーアカウントの設定ステータスを個別に維持するには

- 組織内のすべてのアカウントを表示するには、 AWS Organizations API リファレンス ListAccounts で を実行します。
- 選択的メンバーアカウントの設定ステータスを変更する場合は、メンバーアカウントUpdateMemberDetectorsごとに を個別に実行します。

  GuardDuty コンソールのアカウントページに移動することで、 GuardDuty コンソールを使用して同じタスクを実行できます。

  コンソールまたは API を使用して個々のアカウントの保護プランを有効にする方法については、対応する保護プランの設定ページを参照してください。

委任 GuardDuty 管理者アカウントの変更

各リージョンで組織の委任 GuardDuty 管理者アカウントを変更し、各リージョンで新しい管理者を委任できます。リージョン内の組織のメンバーアカウントのセキュリティ体制を維持するには、そのリージョンに委任された GuardDuty 管理者アカウントが必要です。

既存の委任 GuardDuty 管理者アカウントの削除

ステップ 1 - 各リージョンの既存の委任 GuardDuty 管理者アカウントを削除するには

1. 既存の委任 GuardDuty 管理者アカウントとして、管理者アカウントに関連付けられているすべてのメンバーアカウントを一覧表示します。ListMembers で を実行しますOnlyAssociated=false。
2. GuardDuty またはオプションの保護プランの自動有効化設定が に設定されている場合はALL、UpdateOrganizationConfigurationを実行して組織設定を NEWまたは に更新しますNONE。このアクションは、次のステップですべてのメンバーアカウントの関連付けを解除するときにエラーを防ぐことができます。
3. を実行してDisassociateMembers、管理者アカウントに関連付けられているすべてのメンバーアカウントの関連付けを解除します。
4. DeleteMembers を実行して、管理者アカウントとメンバーアカウント間の関連付けを削除します。
5. 組織管理アカウントとして、 DisableOrganizationAdminAccountを実行して既存の委任 GuardDuty 管理者アカウントを削除します。
6. この委任 GuardDuty 管理者アカウント AWS リージョン がある各 で、これらのステップを繰り返します。

ステップ 2 - で既存の委任 GuardDuty 管理者アカウントの登録を解除するには AWS Organizations (1 回限りのグローバルアクション)

- AWS Organizations API リファレンス DeregisterDelegatedAdministratorで を実行して、 で既存の委任 GuardDuty 管理者アカウントの登録を解除します AWS Organizations。

  または、次の AWS CLI コマンドを実行できます。

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --
service-principal guardduty.amazonaws.com
```

111122223333 を既存の委任 GuardDuty 管理者アカウントに置き換えてください。

古い委任 GuardDuty 管理者アカウントを登録解除したら、新しい委任 GuardDuty 管理者アカウントにメンバーアカウントとして追加できます。

各リージョンで新しい委任 GuardDuty 管理者アカウントを指定する

1. 次のいずれかのアクセス方法を使用して、各リージョンで新しい委任 GuardDuty 管理者アカウントを指定します。

   - GuardDuty コンソールの使用 – ステップ 1 – 組織の委任 GuardDuty 管理者アカウントを指定する。
   - GuardDuty API の使用 – ステップ 1 – AWS 組織の委任 GuardDuty 管理者アカウントを指定する。

2. DescribeOrganizationConfiguration を実行して、組織の現在の自動有効化設定を表示します。

   > **Important**
   >
   > 新しい委任 GuardDuty 管理者アカウントにメンバーを追加する前に、組織の自動有効化設定を確認する必要があります。この設定は、新しい委任 GuardDuty 管理者アカウントと選択したリージョンに固有であり、 には関係ありません AWS Organizations。新しい委任された GuardDuty 管理者アカウントの下に (新規または既存の) 組織メンバーアカウントを追加すると、新しい委任された GuardDuty 管理者アカウントの自動有効化設定は、有効化時 GuardDuty またはそのオプションの保護プランのいずれかに適用されます。

   新しい委任 GuardDuty 管理者アカウントのこの組織設定を変更するには、次のいずれかのアクセス方法を使用します。

   - GuardDuty コンソールの使用 – ステップ 2 – 組織の自動有効化設定を構成する。
   - GuardDuty API の使用 – ステップ 2 - 組織の自動有効化の詳細設定を構成する。

招待による GuardDuty アカウントの管理

組織外のアカウントを管理するには、従来の招待による方法を使用できます。この方法を使用する場合、他のアカウントが招待を承諾してメンバーアカウントになると、アカウントは管理者アカウントとして指定されます。

アカウントが管理者アカウントでない場合は、別のアカウントからの招待を受け入れることができます。招待を承諾すると、自分のアカウントはメンバーアカウントになります。 AWS アカウントは、GuardDuty 管理者アカウントとメンバーアカウントを同時に使用することはできません。

あるアカウントからの招待を受け入れる場合、別のアカウントからの招待を受け入れることはできません。別のアカウントからの招待を受け入れるには、まず既存の管理者アカウントからアカウントの関連付けを解除する必要があります。または、管理者アカウントは、組織からアカウントの関連付けを解除して削除することもできます。

招待によって関連付けられたアカウントは、「」で説明されているように AWS Organizations、によって関連付けられたアカウントと同じ全体的な管理者 account-to-member 関係を持ちます GuardDuty 管理者アカウントとメンバーアカウントの関係を理解する。ただし、招待管理者アカウントのユーザーは、関連付けられたメンバーアカウント GuardDuty に代わって を有効にしたり、AWS Organizations 組織内の他の非メンバーアカウントを表示したりすることはできません。

> **Important**
>
> クロスリージョンデータ転送は、 がこの方法を使用してメンバーアカウント GuardDuty を作成するときに発生する可能性があります。メンバーアカウントの E メールアドレスを検証するために、 は米国東部 (バージニア北部) リージョンでのみ動作する E メール検証サービス GuardDuty を使用します。

招待によるアカウントの追加と管理

いずれかのアクセス方法を選択して、アカウントを追加し、 GuardDuty 管理者アカウントとして GuardDuty メンバーアカウントになるように招待します。

Console

ステップ 1 - アカウントを追加する

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

2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
3. 上部のペインで [招待によってアカウントを追加] を選択します。
4. 「メンバーアカウントの追加」ページの「アカウントの詳細を入力」に、追加するアカウントに関連付けられた AWS アカウント ID と E メールアドレスを入力します。
5. アカウントの詳細を追加する別の行を 1 つずつ追加するには、[別のアカウントを追加] を選択します。[アカウントの詳細を含む.csvファイルをアップロード] を選択して、アカウントを一括で追加することもできます。

   > **Important**
   >
   > 次の例に示すように、.csv ファイルの 1 行目にヘッダー (`Account ID,Email`) を含める必要があります。後続の各行には、有効な AWS アカウント ID とそれに関連付けられた E メールアドレスが 1 つ含まれている必要があります。行の形式は、 AWS アカウント ID が 1 つだけ含まれ、関連する E メールアドレスがカンマで区切られている場合に有効です。
   >
   > ```
   > Account ID,Email
   > 555555555555,user@example.com
   > ```

6. すべてのアカウントの詳細を追加したら、[次へ] を選択します。新しく追加したアカウントは、[アカウント] テーブルに表示されます。これらのアカウントのステータスは [招待未送信] になります。追加したアカウントに招待状を送信する方法については、「Step 2 - Invite an account」を参照してください。

ステップ 2: アカウントを招待する

1. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
2. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
3. Amazon に招待するアカウントを 1 つ以上選択します GuardDuty。
4. [アクション] ドロップダウンメニューから [招待] を選択します。
5. 「招待 GuardDuty」ダイアログボックスに、「 (オプション) 招待メッセージ」を入力します。

   招待されたアカウントが E メールにアクセスできない場合は、[招待先の AWS アカウントのルートユーザーにも E メール通知を送信し、招待先の AWS Health Dashboard にアラートを生成] をクリックします。

6. [Send invitation] (招待の送信) を選択します。招待者が指定された E メールアドレスにアクセスできる場合は、https://console.aws.amazon.com/guardduty/ でコンソールを開くGuardDutyことで招待を表示できます。
7. 招待先が招待を承諾すると、[ステータス] 列の値が [招待済み] に変わります。招待を承諾する方法の詳細については、「Step 3 - Accept an invitation」を参照してください。

ステップ 3 - 招待を受け入れる

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

> **Important**
>
> メンバーシップの招待を表示または承諾 GuardDuty する前に、 を有効にする必要があります。

2. GuardDuty まだ を有効にしていない場合にのみ、次の手順を実行します。有効にしていない場合は、このステップをスキップして次のステップに進むことができます。

   をまだ有効にしていない場合は GuardDuty、Amazon ページで「使用開始」を選択します。GuardDuty

   「ようこそ GuardDuty」ページで、「 を有効にする GuardDuty」を選択します。
3. アカウント GuardDuty で を有効にしたら、次のステップに従ってメンバーシップの招待を承諾します。

   a. ナビゲーションペインで 設定 を選択します。

   b. [アカウント] を選択します。

   c. [アカウント] で、招待元のアカウント所有者を確認してください。[承諾] を選択してメンバーシップへの招待を承諾します。
4. 招待を承諾すると、アカウントは GuardDuty メンバーアカウントになります。所有者が招待を送信したアカウントが GuardDuty 管理者アカウントになります。招待が承諾されたことが管理者アカウントで認識されます。 GuardDuty アカウントのアカウントテーブルが更新されます。メンバーアカウント ID に対応するステータス列の値は、有効 に変更されます。管理者アカウントの所有者は、アカウントに代わって および保護プランの設定を表示 GuardDuty および管理できるようになりました。管理者アカウントは、メンバーアカウントに対して生成された GuardDuty 結果を表示および管理することもできます。

API/CLI

GuardDuty 管理者アカウントを指定し、 API オペレーションを通じて招待によって GuardDuty メンバーアカウントを作成または追加できます。で管理者アカウントとメンバーアカウントを指定するには、次の GuardDuty API オペレーションを実行します GuardDuty。

GuardDuty 管理者アカウントとして AWS アカウント 指定する の認証情報を使用して、次の手順を実行します。

メンバーアカウントの作成または追加

1. GuardDuty が有効になっているアカウントの認証情報 AWS を使用して CreateMembers API オペレーションを実行します。これは、管理者アカウントとして使用する GuardDuty アカウントです。

   現在の AWS アカウントのディテクター ID と、 GuardDuty メンバーにするアカウントのアカウント ID と E メールアドレスを指定する必要があります。この API オペレーションを使用して 1 名以上のメンバーを作成できます。

   コマンド AWS ラインツールを使用して、次の CLI コマンドを実行して管理者アカウントを指定することもできます。自身の有効なディテクター ID、アカウント ID、E メールを使用してください。

   アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. GuardDuty が有効になっている AWS アカウントの認証情報InviteMembersを使用して を実行します。これは、管理者アカウントとして使用する GuardDuty アカウントです。

   現在の AWS アカウントのディテクター ID と、 GuardDuty メンバーにするアカウントのアカウント IDs を指定する必要があります。この API オペレーションにより 1 名以上のメンバーを招待できます。

> **Note**
>
> `message` リクエストパラメータを使用してオプションの招待メッセージを指定することもできます。

を使用して AWS Command Line Interface 、次のコマンドを実行してメンバーアカウントを指定することもできます。招待するアカウントには、自身の有効なディテクター ID と有効なアカウント ID を使用してください。

アカウントと現在のリージョン`detectorId`の を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

招待の受け入れ

GuardDuty メンバー AWS アカウントとして指定する各アカウントの認証情報を使用して、次の手順を実行します。

1. GuardDuty メンバーアカウントに招待され、招待を受け入れるアカウントごとに CreateDetector AWS API オペレーションを実行します。

   サービスを使用して GuardDutyディテクターリソースを有効にするかどうかを指定する必要があります。を運用可能 GuardDuty にするには、ディテクターを作成して有効にする必要があります。招待を受け入れる GuardDuty 前に、まず を有効にする必要があります。

   これを行うには、次の CLI AWS コマンドを使用して コマンドラインツールを使用します。

   ```
   aws guardduty create-detector --enable
   ```

2. その AWS アカウントの認証情報を使用して、メンバーシップの招待を承諾するアカウントごとに AcceptAdministratorInvitation API オペレーションを実行します。

   メンバー AWS アカウントのこのアカウントのディテクター ID、招待を送信した管理者アカウントのアカウント ID、および承諾する招待の招待 ID を指定する必要があります。管理者

アカウントのアカウント ID は、招待メールで見つかります。または、API の ListInvitations オペレーションを使用して検索することもできます。

次の CLI コマンドを実行して、 AWS コマンドラインツールを使用して招待を受け入れることもできます。ディテクター ID、管理者アカウント ID、招待状 ID は必ず有効なものを使用してください。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

GuardDuty 管理者アカウントを単一の組織委任 GuardDuty 管理者アカウントに統合する

GuardDuty では、 を介した関連付けを使用して AWS Organizations 、委任 GuardDuty 管理者アカウントのメンバーアカウントを管理することを推奨しています。以下に示すプロセス例を使用して、組織内の招待によって関連付けられた管理者アカウントとメンバーを 1 つの GuardDuty委任 GuardDuty 管理者アカウントに統合できます。

> **Note**
>
> 委任された GuardDuty 管理者アカウントによって既に管理されているアカウント、または委任された GuardDuty 管理者アカウントに関連付けられているアクティブなメンバーアカウントを、別の委任された GuardDuty 管理者アカウントに追加することはできません。各組織には、リージョンごとに 1 つの委任された GuardDuty 管理者アカウントしか持つことができず、各メンバーアカウントには 1 つの委任された GuardDuty 管理者アカウントしか持つことができません。

いずれかのアクセス方法を選択して、 GuardDuty 管理者アカウントを 1 つの委任 GuardDuty 管理者アカウントに統合します。

Console

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

   ログインするには、組織の管理アカウントの認証情報を使用します。

2. 管理するすべてのアカウントは、組織の一部 GuardDuty である必要があります。組織にアカウントを追加する方法については、「組織への AWS アカウント の招待」を参照してください。

3. すべてのメンバーアカウントが、単一の委任 GuardDuty 管理者アカウントとして指定するアカウントに関連付けられていることを確認します。既存の管理者アカウントにまだ関連付けられているメンバーアカウントの関連付けを解除します。

   次のステップは、メンバーアカウントと既存の管理者アカウントの関連付けを解除するのに役立ちます。

   a. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。
   b. ログインするには、既存の管理者アカウントの認証情報を使用します。
   c. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
   d. [アカウント] ページで、管理者アカウントとの関連付けを解除する 1 つ以上のアカウントを選択します。
   e. [アクション] を選択してから、[アカウントの関連付けを解除する] を選択します。
   f. [確認] を選択してステップを確定します。

4. https://console.aws.amazon.com/guardduty/ で GuardDuty コンソールを開きます。

   ログインするには、管理アカウントの認証情報を使用します。

5. ナビゲーションペインで 設定 を選択します。設定ページで、組織の委任 GuardDuty 管理者アカウントを指定します。

6. 指定された委任 GuardDuty 管理者アカウントにログインします。

7. 組織からメンバーを追加します。詳細については、「による GuardDuty アカウントの管理 AWS Organizations」を参照してください。

API/CLI

1. 管理するすべてのアカウントは、組織の一部 GuardDuty である必要があります。組織にアカウントを追加する方法については、「組織への AWS アカウント の招待」を参照してください。

2. すべてのメンバーアカウントが、単一の委任 GuardDuty 管理者アカウントとして指定するアカウントに関連付けられていることを確認します。

   a. を実行してDisassociateMembers、既存の管理者アカウントにまだ関連付けられているメンバーアカウントの関連付けを解除します。

   b. または、 AWS Command Line Interface を使用して次のコマンドを実行し、*777777777777* をメンバーアカウントの関連付けを解除する既存の管理者アカウントのディテクター ID に置き換えることもできます。*666666666666* を、関連付けを解除するメンバーアカウントの AWS アカウント ID に置き換えます。

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
   ```

3. EnableOrganizationAdminAccount を実行して、 を委任された GuardDuty 管理者アカウント AWS アカウント として委任します。

   または、 AWS Command Line Interface を使用して次のコマンドを実行し、委任された GuardDuty 管理者アカウントを委任することもできます。

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. 組織からメンバーを追加します。詳細については、「Create or add member member accounts using API」を参照してください。

> **Important**
>
> リージョンサービスである の有効性を最大化するには GuardDuty、委任された GuardDuty 管理者アカウントを指定し、すべてのリージョンのすべてのメンバーアカウントを追加することをお勧めします。

複数のアカウント GuardDuty で同時に を有効にする

複数のアカウント GuardDuty で同時に を有効にするには、次の方法を使用します。

Python スクリプトを使用して複数のアカウント GuardDuty で同時に を有効にする

Amazon GuardDuty マルチアカウントスクリプト のサンプルリポジトリのスクリプトを使用して、GuardDuty 複数のアカウントで の有効化または無効化を自動化できます。このセクションのプロセ

スを使用して、Amazon EC2 を使用するメンバーアカウントのリスト GuardDuty に対して を有効にします。disable スクリプトの使用またはローカルでスクリプトを設定する方法については、共有リンクの手順を参照してください。

このenableguardduty.pyスクリプトは、 を有効にし GuardDuty、管理者アカウントから招待を送信し、すべてのメンバーアカウントで招待を受け入れます。その結果、すべてのメンバー GuardDuty アカウントのすべてのセキュリティ検出結果を含む管理者アカウントが作成されます。GuardDuty はリージョンによって分離されているため、各メンバーアカウントの結果は、管理者アカウントの対応するリージョンにロールアップされます。例えば、 GuardDuty 管理者アカウントの us-east-1 リージョンには、関連するすべてのメンバーアカウントのすべての us-east-1 の検出結果のセキュリティ検出結果が含まれています。

これらのスクリプトは、マネージドポリシー AWS マネージドポリシー: AmazonGuardDutyFullAccess を使用する共有 IAM ロールに依存しています。このポリシーは、 へのアクセスをエンティティに許可 GuardDuty し、管理者アカウントと、 を有効にする各アカウントに存在する必要があります GuardDuty。

以下のプロセスでは、使用可能なすべてのリージョン GuardDuty でデフォルトで を有効にします。指定されたリージョン GuardDuty で を有効にするには、オプションの `--enabled_regions`引数を使用し、リージョンのカンマ区切りリストを指定します。オプションで、`enableguardduty.py` を開いて `gd_invite_message` 文字列を編集することで、メンバーアカウントに送信される招待メッセージをカスタマイズすることもできます。

1. GuardDuty 管理者アカウントに IAM ロールを作成し、AWS マネージドポリシー: AmazonGuardDutyFullAccessポリシーをアタッチして を有効にします GuardDuty。
2. GuardDuty 管理者アカウントで管理する各メンバーアカウントに IAM ロールを作成します。このロールは、ステップ 1 で作成したロールと同じ名前にする必要があります。また、管理者アカウントを信頼されたエンティティとして許可し、前述の同じ AmazonGuardDutyFullAccess 管理ポリシーを持つ必要があります。
3. インスタンスがサービスのロールを引き受けることができるようにする次の信頼関係のあるロールをアタッチして、新しい Amazon Linux インスタンスを起動します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 新しいインスタンスにログインし、次のコマンドを実行してそのインスタンスを設定します。

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. ステップ 2 でロールを追加したメンバーアカウントのアカウント ID と E メールのリストを含む CSV ファイルを作成します。次の例のように、アカウントは 1 行に 1 つずつ記述し、アカウント ID と E メールアドレスはカンマで区切る必要があります。

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> CSV ファイルは、enableguardduty.py スクリプトと同じ場所にあることが必要です。次の方法で、既存の CSV ファイルを Amazon S3 から現在のディレクトリにコピーできます。
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. Python スクリプトを実行します。 GuardDuty 管理者アカウント ID、最初のステップで作成したロールの名前、CSV ファイルの名前を引数として指定してください。

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

GuardDuty コストの見積もり

GuardDuty コンソールまたは API オペレーションを使用して、 の 1 日の平均使用コストを見積もることができます GuardDuty。30 日間の無料トライアル期間中、コストの見積もりはトライアル期間後の推定コストを予測します。マルチアカウント環境で運用している場合、 GuardDuty 管理者アカウントはすべてのメンバーアカウントのコストメトリクスをモニタリングできます。

> **Note**
>
> Malware Protection for S3 の使用コストは、 GuardDuty コンソールの Usage には含まれません。詳細については、「Malware Protection for S3 の使用状況とコストの表示」を参照してください。

コストの見積もりは、次のメトリクスを基準にして表示することができます。

- アカウント ID – アカウント、または GuardDuty 管理者アカウントとして運用している場合はメンバーアカウントの推定コストを一覧表示します。
- データソース – VPC フローログ、 CloudTrail 管理ログ、 CloudTrail データイベント、または DNS ログのデータソースタイプについて、指定された GuardDuty データソースの推定コストを一覧表示します。
- 機能 – S3、EKS 監査ログモニタリング、EBS ボリューム GuardDuty CloudTrail データ、RDS ログインアクティビティ、EKS ランタイムモニタリング、Fargate Runtime Monitoring、EC2 Runtime Monitoring、または Lambda Network Activity Monitoring のデータイベントに関する、指定されたデータソースの推定コストを一覧表示します。
- S3 バケット - 指定したバケットの S3 データイベントまたは環境内のアカウントで最も高価なバケットの推定コストをリスト化します。

> **Note**
>
> S3 バケット統計は、アカウントで S3 Protection が有効になっている場合にのみ使用できます。詳細については、「Amazon での Amazon S3 Protection GuardDuty」を参照してください。

が使用コスト GuardDuty を計算する方法を理解する

GuardDuty コンソールに表示される見積りは、 AWS Billing and Cost Management コンソールの見積りと若干異なる場合があります。次のリストでは、 が使用コストを GuardDuty 見積もる方法を説明します。

- GuardDuty 使用量の見積もりは、現在のリージョンのみを対象としています。
- GuardDuty 使用コストは、過去 30 日間の使用量に基づきます。
- 試用コストの見積もりには、現在トライアル期間中の基本的なデータソースと機能の見積もりが含まれます。内の各機能とデータソース GuardDuty には独自のトライアル期間がありますが、 の GuardDutyトライアル期間または同時に有効になった別の機能と重複する可能性があります。
- GuardDuty 使用量の見積もりには、Amazon GuardDuty 料金ページで説明されているように、リージョンあたりの GuardDuty ボリューム料金割引が含まれますが、ボリューム料金階層を満たす個々のアカウントのみを対象とします。ボリュームの割引料金は、組織内のアカウント間の合計使用量の見積もりには含まれません。組み合わせ使用量の割引料金の詳細については、「AWS 請求: ボリューム割引」を参照してください。
- 組織 AWS アカウント 内の各 の使用コストの合計は、選択したデータソースの過去 30 日間の推定コストと必ずしも同じとは限りません。料金範囲は、 がより多くのイベントやデータ GuardDuty を処理するにつれて変更される場合があります。詳細については、「 AWS Billing ユーザーガイド」の「 料金範囲」を参照してください。

このシナリオでは、Runtime Monitoring の使用コストの発生を停止するには、Runtime Monitoring 機能と EKS Runtime Monitoring 機能の両方を無効にする必要があります。

GuardDuty は、EKS Runtime Monitoring のコンソールエクスペリエンスを Runtime Monitoring に統合しました。 GuardDuty は EKS Runtime Monitoring 設定ステータスの確認と を推奨しますEKS Runtime Monitoring から Runtime Monitoring への移行。

Runtime Monitoring への移行の一環として、 を必ず に移行してくださいEKS Runtime Monitoring を無効にする。これは、後で Runtime Monitoring を無効にし、EKS Runtime Monitoring を無効にしない場合、EKS Runtime Monitoring の使用コストが引き続き発生するため、重要です。

Runtime Monitoring – EC2 インスタンスからの VPC フローログが使用コストに与える影響

EC2 インスタンスの EKS Runtime Monitoring または Runtime Monitoring でセキュリティエージェントを (手動または を介して GuardDuty) 管理し、現在 Amazon EC2 インスタンスにデプロイされ、このインスタンス収集されたランタイムイベントタイプから を受け取った場合、 GuardDuty はこの Amazon EC2 インスタンスからの VPC フローログの分析 AWS アカウント に対して に課金 GuardDuty しません。これにより、アカウントの 2 倍の使用コスト GuardDuty を回避できます。

が CloudTrail イベントの使用コスト GuardDuty を見積もる方法

を有効にすると GuardDuty、選択した でアカウント用に記録された AWS CloudTrail イベントログの使用が自動的に開始されます AWS リージョン。 はグローバルサービスイベントログを GuardDuty レプリケートし、 GuardDuty 有効にした各リージョンでこれらのイベントを個別に処理します。これにより、各リージョンのユーザープロファイルとロールプロファイル GuardDuty を維持し、異常を特定できます。

CloudTrail 設定は、 GuardDuty 使用コストやイベントログ GuardDuty の処理方法には影響しません。 GuardDuty 使用コストは、 にログ記録される AWS APIs の使用によって影響を受けます CloudTrail。詳細については、「AWS CloudTrail イベントログ」を参照してください。

GuardDuty 使用状況統計の確認

任意のアクセス方法を選択して、アカウント GuardDutyの使用統計を確認します。 GuardDuty 管理者アカウントの場合、次の方法は、すべてのメンバーの使用状況統計を確認するのに役立ちます。

Console

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

   GuardDuty 管理者アカウントアカウントを使用してください。
2. ナビゲーションペインで 使用状況を選択します。
3. 使用状況ページでは、メンバーアカウントを持つ GuardDuty 管理者アカウントが、過去 30 日間の推定組織コストを表示できます。これは、組織の推定総使用コストです。
4. GuardDuty メンバーを持つ 管理者アカウントは、データソース別またはアカウント別に使用コストの内訳を表示できます。個々のアカウントまたはスタンドアロンアカウントは、データソースごとに内訳を表示できます。

メンバーアカウントがある場合は、Accounts テーブルでそのアカウントを選択すると、個々のアカウントの統計を表示できます。

データソース別タブで、使用コストが関連付けられているデータソースを選択すると、アカウントレベルでのコスト内訳の対応する合計が常に同じとは限りません。

API/CLI

GuardDuty 管理者アカウントアカウントの認証情報を使用して GetUsageStatistics API オペレーションを実行します。コマンドを実行するには、次の情報を提供します。

- (必須) 統計を取得するアカウントのリージョンディ GuardDuty テクター ID を指定します。
- (必須) 取得する統計のタイプの 1 つ、SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE を指定します。

  現在、 TOP_ACCOUNTS_BY_FEATUREは の使用統計の取得をサポートしていませんRDS_LOGIN_EVENTS。
- (必須) 使用統計を照会する、データソースまたは特徴量を 1 つ以上提供します。
- (オプション) 使用統計を取得するアカウント ID のリストを提供します。

また、 AWS Command Line Interfaceを使用することもできます 次のコマンドは、アカウントで計算されたすべてのデータソースと機能の使用統計を取得する例です。必ず detector-id をご自身の有効なディテクター ID に置き換えてください。スタンドアロンアカウントの場合、このコマンドはアカウントに対してのみ、過去 30 日間の使用コストを返します。メンバーアカウントを持つ GuardDuty 管理者アカウントの場合、すべてのメンバーのコストがアカウントごとに一覧表示されます。

アカウントと現在のリージョンdetectorIdの を検索するには、https://console.aws.amazon.com/guardduty/ コンソールの設定ページを参照するか、 ListDetectors API を実行します。

使用統計の計算に使用するタイプに SUM_BY_ACCOUNT を置き換えます。

データソースのコストのみを監視

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
```

```
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

特徴量のコストを監視

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
 "EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
 "EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Amazon GuardDuty のセキュリティ

AWS では、クラウドセキュリティを最優先事項としています。AWS の顧客は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWS とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ - AWS は、AWS クラウドで AWS のサービスを実行するインフラストラクチャを保護する責任を負います。また、AWS は、使用するサービスを安全に提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。GuardDuty に適用するコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲の AWS のサービス」、「を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS のサービスに応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、GuardDuty を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。ここでは、セキュリティとコンプライアンスの目標を満たすように GuardDuty を設定する方法を説明します。また、GuardDuty リソースのモニタリングや保護に役立つ、他の AWS のサービスの使用方法についても説明します。

目次

Amazon でのデータ保護 GuardDuty

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

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

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

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

保管中の暗号化

すべての GuardDuty 顧客データは、保管時に暗号化ソリューションを使用して AWS 暗号化されます。

GuardDuty 検出結果などの データは、 が所有するカスタマーマネージドキーを使用して AWS Key Management Service （ AWS KMS) を使用して AWS 保管時に暗号化されます。

転送中の暗号化

GuardDuty は、他の サービスのログデータを分析します。GuardDuty は、これらのサービスから転送中のデータすべてを HTTPS および KMS で暗号化します。がログから必要な情報を GuardDuty 抽出すると、それらは破棄されます。が他の のサービスからの情報 GuardDuty を使用する方法の詳細については、GuardDuty 「 データソース」を参照してください。

GuardDuty データは、サービス間で転送中に暗号化されます。

サービス改善のためのデータ使用をオプトアウトする

オプトアウトポリシーを使用して、 GuardDuty およびその他の AWS セキュリティサービスの開発と改善にデータを使用することを AWS Organizations オプトアウトできます。が現在そのようなデータを収集していない場合でも GuardDuty 、オプトアウトを選択できます。オプトアウトする方法の詳細については、「AWS Organizations ユーザーガイド」の「AI サービスのオプトアウトポリシー」を参照してください。

> **Note**
>
> オプトアウトポリシーを使用するには、 AWS アカウントが によって一元管理されている必要があります AWS Organizations。 AWS アカウント用の組織をまだ作成していない場合は、「 ユーザーガイド」の「組織の作成と管理AWS Organizations 」を参照してください。

オプトアウトには次のような効果があります。

- GuardDuty は、オプトアウトする前に、サービス改善の目的で収集および保存したデータ (存在する場合) を削除します。
- オプトアウトすると、 GuardDuty はサービス改善の目的でこのデータを収集または保存しなくなります。

以下のトピックでは、 の各機能がサービス向上のためにデータをどのように GuardDuty 処理するかについて説明します。

内容

- GuardDuty ランタイムモニタリング

- GuardDuty マルウェア保護

GuardDuty ランタイムモニタリング

GuardDuty Runtime Monitoring は、 AWS 環境内の Amazon Elastic Kubernetes Service (Amazon EKS) クラスター、 AWS Fargate (Fargate) Amazon Elastic Container Service (Amazon ECS) のみ、および Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのランタイム脅威検出を提供します。Runtime Monitoring を有効にし、リソース GuardDuty のセキュリティエージェントをデプロイすると、 はリソースに関連付けられたランタイムイベントのモニタリングと分析 GuardDuty を開始します。これらのランタイムイベントタイプには、プロセスイベント、コンテナイベント、DNS イベントなどが含まれます。詳細については、「が GuardDuty 使用する収集済みランタイムイベントタイプ」を参照してください。

GuardDuty は、ワークロードに転送できるコマンドライン引数を収集しますが、現在、サービス改善の目的でこれらの引数を使用しません (今後使用される場合があります) 。間もなくリリースされる新たな脅威検出ルールや検出結果を見越して、コマンドライン引数の収集を開始しました。信頼、プライバシー、およびコンテンツのセキュリティが当社の最優先事項であり、当社の使用に際してユーザーへの約束に確実に従うことを保証します。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。

GuardDuty マルウェア保護

GuardDuty Malware Protection は、侵害された可能性のある Amazon EC2 インスタンスとコンテナワークロードにアタッチされた EBS ボリュームに含まれるマルウェア、および選択した Amazon S3 バケットに新しくアップロードされたファイルをスキャンして検出します。 GuardDuty Malware Protection が EBS ボリュームファイルまたは S3 ファイルを悪意のある、または有害なものとして識別すると、 GuardDuty Malware Protection はこのファイルを収集して保存し、マルウェア検出と GuardDuty サービスを開発および改善します。このファイルは、他の AWS セキュリティサービスの開発と改善にも使用される場合があります。信頼、プライバシー、およびコンテンツのセキュリティが当社の最優先事項であり、当社の使用に際してユーザーへの約束に確実に従うことを保証します。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。

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

Amazon GuardDuty は、GuardDuty のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供するサービスである AWS CloudTrail と統合されています。CloudTrail は、GuardDuty コンソールからの呼び出しや GuardDuty API へのコード呼び出し

を含む、GuardDuty 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。追跡を作成する場合は、GuardDuty に関するイベントを含めた CloudTrail のイベントの Amazon Simple Storage Service (Amazon S3) バケットへの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、GuardDuty に対するリクエスト、そのリクエストが発信された IP アドレス、リクエストの作成者、リクエスト作成日時、その他の詳細情報などを確認できます。

CloudTrail を設定して有効にする方法などの詳細については、AWS CloudTrail ユーザーガイドを参照してください。

CloudTrail での GuardDuty 情報

CloudTrail は、アカウントを作成すると AWS アカウントで有効になります。サポートされているイベントアクティビティが GuardDuty で発生すると、そのアクティビティは [Event history] (イベント履歴) の他の AWS のサービスのイベントとともに、CloudTrail イベントにレコードされます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail Event 履歴でのイベントの表示」を参照してください。

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

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

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。ID 情報は次の判断に役立ちます。

- リクエストが、ルートユーザーまたは IAM ユーザーのどちらのサインイン認証情報を使用して送信されたか

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

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

CloudTrail の GuardDuty コントロールプレーンイベント

デフォルトでは、CloudTrail は Amazon GuardDuty API リファレンスで提供されているすべての GuardDuty API オペレーションを CloudTrail ファイルにイベントとして記録します。

CloudTrail の GuardDuty データイベント

でのランタイムモニタリング GuardDuty は、Amazon Elastic Kubernetes Service (Amazon EKS) クラスター、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、AWS Fargate Amazon Elastic Container Service (Amazon ECS)タスクにデプロイされた GuardDuty セキュリティエージェントを使用して、AWS ワークロード用に 収集されたランタイムイベントタイプ を収集するアドオン (`aws-guardduty-agent`) を収集し、脅威検出と分析に使用するため、GuardDuty に送信します。

データイベントのログとモニタリング

オプションで、GuardDuty セキュリティエージェントのデータイベントを表示するように AWS CloudTrail ログを設定できます。

CloudTrail を作成して設定するには、「AWS CloudTrail ユーザーガイド」の「データイベント」を参照して、「AWS Management Console の高度なイベントセレクターによるデータイベントのロギング」の手順に従ってください。トレイルを記録するには、以下の変更を実行します。

- [データイベントタイプ] には、[GuardDuty ディテクター] を選択します。
- [ログセレクターテンプレート] では、[すべてのイベントをログに記録する] を選択します。
- 設定の [JSON ビュー] を展開します。次の JSON と同じようになります。

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
```

```
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

トレイルのセレクターを有効にした後、https://console.aws.amazon.com/s3/ にある Amazon S3 コンソールに移動します。CloudTrail ログの設定時に選択した S3 バケットからデータイベントをダウンロードできます。

例: GuardDuty ログアーカイブエントリ

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。CloudTrailのログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrailログファイルは、パブリックAPIコールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次は、データプレーンイベントを示す CloudTrail ログエントリの例です。

```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
```

```
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```


次の例では、CreateIPThreatIntelSet アクション (コントロールプレーンイベント) を示す CloudTrail ログエントリを示しています。


```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

このイベント情報からは、GuardDuty で脅威リスト Example を作成するリクエストが行われたことを判断できます。また、このリクエストは、Alice という名前のユーザーによって 2018 年 6 月 14 日に行われたことも確認できます。

Amazon の Identity and Access Management GuardDuty

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に GuardDuty リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon と IAM GuardDuty の連携方法
- Amazon のアイデンティティベースのポリシーの例 GuardDuty
- Amazon のサービスにリンクされたロールの使用 GuardDuty
- AWS Amazon の マネージドポリシー GuardDuty
- Amazon GuardDuty 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

対象者

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

サービスユーザー – GuardDuty サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの GuardDuty 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。の機能にアクセスできない場合は、GuardDuty「」を参照してくださいAmazon GuardDuty 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。

サービス管理者 – 社内の GuardDuty リソースを担当している場合は、通常、 へのフルアクセスがあります GuardDuty。サービスユーザーがどの GuardDuty 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。会社で IAM を で使用する方法の詳細については、 GuardDuty「」を参照してくださいAmazon と IAM GuardDuty の連携方法。

IAM 管理者 – IAM 管理者は、 へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります GuardDuty。IAM で使用できる GuardDuty 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、「」を参照してくださいAmazon のアイデンティティベースのポリシーの例 GuardDuty。

アイデンティティを使用した認証

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

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

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

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

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

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドのルートユーザー認証情報が必要なタスクを参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がにアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

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

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。

例えば、IAMAdminsという名前のグループを設定して、そのグループにIAM リソースを管理する許可を与えることができます。

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

IAM ロール

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

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(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 Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、IAM ユーザーガイドのAmazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与するを参照してください。

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

ポリシーを使用したアクセスの管理

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

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

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

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

アイデンティティベースのポリシー

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

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

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があ

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

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

アクセスコントロールリスト (ACL)

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

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

その他のポリシータイプ

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

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザーガイドのIAM エンティティのアクセス許可の境界を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を

制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」を参照してください。

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、IAM ユーザーガイドのセッションポリシーを参照してください。

複数のポリシータイプ

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

Amazon と IAM GuardDuty の連携方法

IAM を使用して へのアクセスを管理する前に GuardDuty、 で使用できる IAM 機能について学びます GuardDuty。

Amazon で使用できる IAM の機能 GuardDuty

IAM 機能	GuardDuty サポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	Yes
ACL	なし
ABAC (ポリシー内のタグ)	部分的

IAM 機能	GuardDuty サポート
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	あり
サービスリンクロール	あり

GuardDuty およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」の「IAM AWS と連携する のサービス」を参照してください。

のアイデンティティベースのポリシー GuardDuty

アイデンティティベースポリシーをサポートする	あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベース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。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、IAM ユーザーガイドのIAM JSON ポリシーの要素のリファレンスを参照してください。

のアイデンティティベースのポリシーの例 GuardDuty

GuardDuty 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、「」を参照してくださいAmazon のアイデンティティベースのポリシーの例 GuardDuty。

内のリソースベースのポリシー GuardDuty

リソースベースのポリシーのサポート	なし

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

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

のポリシーアクション GuardDuty

ポリシーアクションに対するサポート	あり

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

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

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

GuardDuty 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 で定義されるアクション GuardDuty」を参照してください。

のポリシーアクションは、アクションの前に次のプレフィックス GuardDuty を使用します。

```
guardduty
```

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。

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

GuardDuty 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、「」を参照してくださいAmazon のアイデンティティベースのポリシーの例 GuardDuty。

のポリシーリソース GuardDuty

ポリシーリソースに対するサポート	あり

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

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

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

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

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

GuardDuty 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、「」を参照してくださいAmazon のアイデンティティベースのポリシーの例 GuardDuty。

のポリシー条件キー GuardDuty

サービス固有のポリシー条件キーのサポート	あり

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

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

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

GuardDuty 条件キー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 の条件キー GuardDuty」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 で定義されるアクション GuardDuty」を参照してください。

GuardDuty 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、「」を参照してくださいAmazon のアイデンティティベースのポリシーの例 GuardDuty。

GuardDuty のアクセスコントロールリスト (ACL)

ACL のサポート	なし

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

を使用した属性ベースのアクセスコントロール (ABAC) GuardDuty

ABAC (ポリシー内のタグ) のサポート	部分的

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、IAM ユーザーガイドのABAC とは?を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、IAM ユーザーガイドの属性に基づくアクセスコントロール (ABAC) を使用するを参照してください。

での一時的な認証情報の使用 GuardDuty

一時的な認証情報のサポート	あり

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、IAM ユーザーガイドのロールへの切り替え (コンソール)を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、IAM の一時的セキュリティ認証情報を参照してください。

のクロスサービスプリンシパル許可 GuardDuty

フォワードアクセスセッション (FAS) をサポート	あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

GuardDuty のサービスロール

サービスロールに対するサポート	あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細につい

ては、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 GuardDuty 機能が破損する可能性があります。が指示する場合以外 GuardDuty は、サービスロールを編集しないでください。

のサービスにリンクされたロール GuardDuty

サービスリンクロールのサポート	あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

GuardDuty サービスにリンクされたロールの作成または管理の詳細については、「」を参照してくださいAmazon のサービスにリンクされたロールの使用 GuardDuty。

サービスリンクロールの作成または管理の詳細については、IAM と提携するAWS のサービスを参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

Amazon のアイデンティティベースのポリシーの例 GuardDuty

デフォルトでは、ユーザーとロールにはリソースを作成または変更 GuardDutyするアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

各リソースタイプの ARN の形式など GuardDuty、 で定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンス」の「Amazon のアクション、リソース、および条件キー GuardDuty」を参照してください。 ARNs

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 GuardDuty 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 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイドのIAM でのポリシーとアクセス許可を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を通じてサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許

可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素:条件) を参照してください。

- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイドのIAM Access Analyzer ポリシーの検証を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドのMFA 保護 API アクセスの設定を参照してください。

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

GuardDuty コンソールを使用する

Amazon GuardDuty コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の GuardDuty リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

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

ユーザーとロールが GuardDuty 引き続きコンソールを使用できるようにするには、エンティティに GuardDuty `ConsoleAccess`または `ReadOnly` AWS 管理ポリシーもアタッチします。詳細については、IAM ユーザーガイドのユーザーへの許可の追加を参照してください。

GuardDuty の有効化に必要なアクセス許可

さまざまな IAM ID (ユーザー、グループ、ロール) が持つ必要があるアクセス許可を付与するには、必要なAWS マネージドポリシー: AmazonGuardDutyFullAccessポリシーをアタッチして を有効にします GuardDuty。

自分の権限の表示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 AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

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

への読み取り専用アクセスを許可するカスタム IAM ポリシー GuardDuty

への読み取り専用アクセスを許可するには GuardDuty 、 AmazonGuardDutyReadOnlyAccessマネージドポリシーを使用できます。

IAM ロール、ユーザー、またはグループに への読み取り専用アクセスを許可するカスタムポリシーを作成するには GuardDuty、次のステートメントを使用できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

GuardDuty 結果へのアクセスを拒否する

次のポリシーを使用して、検出 GuardDuty 結果への IAM ロール、ユーザー、またはグループアクセスを拒否できます。ユーザーは検出結果や検出結果の詳細を表示することはできませんが、他のすべての GuardDuty オペレーションにアクセスできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
```

```
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

カスタム IAM ポリシーを使用して GuardDuty リソースへのアクセスを制限する

ディテクター ID GuardDuty に基づいて へのユーザーのアクセスを定義するには、以下のオペレーションを除くカスタム IAM ポリシーですべての GuardDuty API アクションを使用できます。

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

IAM ポリシーで次のオペレーションを使用して、IPSet ID と ThreatIntelSet ID に基づいて へのGuardDutyユーザーのアクセスを定義します。

- `guardduty:DeleteIPSet`

- guardduty:DeleteThreatIntelSet
- guardduty:GetIPSet
- guardduty:GetThreatIntelSet
- guardduty:UpdateIPSet
- guardduty:UpdateThreatIntelSet

次の例では、前述のオペレーションのいくつかを使用してポリシーを作成する方法を示します。

- このポリシーでは、us-east-1 リージョンでディテクター ID として 1234567 を使用し、guardduty:UpdateDetector オペレーションを実行できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- このポリシーでは、us-east-1 リージョンでディテクター ID として 1234567、および IPSet ID として 000000 を使用し、guardduty:UpdateIPSet オペレーションを実行できます。

> **Note**
>
> 信頼された IP リストと脅威リストへのアクセスに必要なアクセス許可がユーザーに付与されていることを確認します GuardDuty。詳細については、「信頼できる IP リストと 脅威リストをアップロードするために必要な許可」を参照してください。

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

```
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- このポリシーでは、us-east-1 リージョンで任意のディテクター ID、および IPSet ID として 000000 を使用し、guardduty:UpdateIPSet オペレーションを実行できます。

> **Note**
>
> 信頼された IP リストと脅威リストへのアクセスに必要なアクセス許可がユーザーに付与されていることを確認します GuardDuty。詳細については、「信頼できる IP リストと 脅威リストをアップロードするために必要な許可」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- このポリシーでは、us-east-1 リージョンでディテクター ID および任意の IPSet ID を使用し、guardduty:UpdateIPSet オペレーションを実行できます。

> **Note**
>
> 信頼された IP リストと脅威リストへのアクセスに必要なアクセス許可がユーザーに付与されていることを確認します GuardDuty。詳細については、「信頼できる IP リストと 脅威リストをアップロードするために必要な許可」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Amazon のサービスにリンクされたロールの使用 GuardDuty

Amazon GuardDuty 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。サービスにリンクされたロール (SLR) は、 に直接リンクされた一意のタイプの IAM ロールです GuardDuty。サービスにリンクされたロールは、 によって事前定義 GuardDuty されており、ユーザーに代わって他の AWS のサービスを呼び出す GuardDuty ために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールでは、必要なアクセス許可を手動で追加 GuardDuty せずに を設定できます。 は、サービスにリンクされたロールのアクセス許可 GuardDuty を定義します。アクセス許可が別途定義されていない限り、 のみがロールを引き受け GuardDuty ることができます。定義された許可には信頼ポリシーと許可ポリシーが含まれ、そ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。

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

GuardDuty サービスにリンクされたロールは、それが有効なすべてのリージョン GuardDuty で最初に無効にした後にのみ削除できます。これにより、リソースへのアクセス許可が誤って削除されないため、 GuardDuty リソースが保護されます。

サービスにリンクされたロールをサポートするその他のサービスについては、「IAM ユーザーガイド」の「AWS services that work with IAM」を参照し、「Service-Linked Role」列が「Yes」となっているサービスを探してください。そのサービスについて、サービスにリンクされたロールのドキュメントを表示するには、「Yes」を選択します。これにはリンクが設定されています。

のサービスにリンクされたロールのアクセス許可 GuardDuty

GuardDuty は、 という名前のサービスにリンクされたロール (SLR) を使用しますAWSServiceRoleForAmazonGuardDuty。SLR では GuardDuty 、 は次のタスクを実行できます。また GuardDuty 、 は、EC2 インスタンスに属する取得されたメタデータを、潜在的な脅威について生成する GuardDuty 可能性のある検出結果に含めることもできます。AWSServiceRoleForAmazonGuardDuty サービスにリンクされたロールは、ロールを継承するために guardduty.amazonaws.com のサービスを信頼します。

アクセス許可ポリシーは、以下のタスク GuardDuty を実行するのに役立ちます。

- Amazon EC2 アクションを使用して、VPC、サブネット、トランジットゲートウェイなどの EC2 VPCs インスタンス、イメージ、ネットワークコンポーネントに関する情報を管理および取得します。
- Amazon EC2 の自動エージェントで Runtime Monitoring を有効にする場合は、 AWS Systems Manager アクションを使用して Amazon EC2 インスタンスの GuardDuty SSM 関連付けを管理します。 GuardDuty 自動エージェント設定が無効になっている場合、包含タグ (GuardDutyManaged：true) を持つ EC2 インスタンスのみ GuardDuty を考慮します。
- AWS Organizations アクションを使用して、関連するアカウントと組織 ID を記述します。
- Amazon S3 アクションを使用して S3 バケットとオブジェクトに関する情報を取得します。
- AWS Lambda アクションを使用して、Lambda 関数とタグに関する情報を取得します。
- Amazon EKS アクションを使用して、EKS クラスターに関する情報を管理および取得し、EKS クラスター上の Amazon EKS アドオンを管理します。EKS アクションは、 に関連付けられたタグに関する情報も取得します GuardDuty。
- Malware Protection for EC2 が有効になったMalware Protection for EC2 のサービスにリンクされたロールのアクセス許可ら、IAM を使用して を作成します。

- Amazon ECS アクションを使用して、Amazon ECS クラスターの管理や情報を取得し、guarddutyActivate で、Amazon ECS アカウント設定を管理します。Amazon ECS に関連するアクションは、 に関連付けられたタグに関する情報も取得します GuardDuty。

ロールは、AmazonGuardDutyServiceRolePolicy と名付けられた次の AWS マネージドポリシーで構成されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
             "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
             "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
```

```
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/GuardDutyManaged": "*"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateEksAddonPolicy",
            "Effect": "Allow",
            "Action": "eks:CreateAddon",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEksAddonManagementPolicy",
            "Effect": "Allow",
            "Action": [
```

```
                "eks:DeleteAddon",
                "eks:UpdateAddon",
                "eks:DescribeAddon"
            ],
            "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
        },
        {
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
```

```
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
            "Effect": "Allow",
            "Action": [
                "ssm:AddTagsToResource"
            ],
            "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
```

```
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
    ]
}
```

AWSServiceRoleForAmazonGuardDuty サービスにリンクされたロールにアタッチされている信頼ポリシーは次のとおりです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AmazonGuardDutyServiceRolePolicy ポリシーへの更新詳細については、GuardDuty AWS 管理ポリシーの更新 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、ドキュメント履歴 ページの RSS フィードをサブスクライブしてください。

のサービスにリンクされたロールの作成 GuardDuty

AWSServiceRoleForAmazonGuardDuty サービスにリンクされたロールは、 GuardDuty を初めて有効にするか、以前に有効にしていなかったサポートされているリージョン GuardDuty で有効にすると、自動的に作成されます。IAM コンソール、、または IAM API を使用して AWS CLI、サービスにリンクされたロールを手動で作成することもできます。

> **Important**
>
> GuardDuty 委任管理者アカウント用に作成されたサービスにリンクされたロールは、メンバー GuardDuty アカウントには適用されません。

サービスにリンクされたロールの作成、編集、削除をIAM プリンシパル (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要がありま

す。AWSServiceRoleForAmazonGuardDuty サービスにリンクされたロールを正常に作成するには、 GuardDuty で使用する IAM プリンシパルに必要なアクセス許可が必要です。必要なアクセス許可を付与するには、次のポリシーをこの ユーザー、グループ、またはロールにアタッチします。

> **Note**
>
> 次の例のサンプル##### *ID* を実際の AWS アカウント ID に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
```

```
}
```

IAM ロールを手動で作成する方法の詳細は、「IAM ユーザーガイド」の「サービスにリンクされたロールを作成する」を参照してください。

のサービスにリンクされたロールの編集 GuardDuty

GuardDuty では、AWSServiceRoleForAmazonGuardDuty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すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。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。

のサービスにリンクされたロールの削除 GuardDuty

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。これにより、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。

> **Important**
>
> Malware Protection for EC2 を有効にしている場合、 を削除しても は自動的に削除AWSServiceRoleForAmazonGuardDutyされませんAWSServiceRoleForAmazonGuardDutyMalwareProtection。を削除する場合はAWSServiceRoleForAmazonGuardDutyMalwareProtection、「Malware Protection for EC2 のサービスにリンクされたロールの削除」を参照してください。

を削除するには、まず、有効になっているすべてのリージョン GuardDuty で を無効にする必要がありますAWSServiceRoleForAmazonGuardDuty。 GuardDuty サービスにリンクされたロールを削除しようとしたときにサービスが無効になっていない場合、削除は失敗します。詳細については、「一時停止または無効化 GuardDuty」を参照してください。

を無効にすると GuardDuty、 は自動的に削除AWSServiceRoleForAmazonGuardDutyされません。 GuardDuty を再度有効にすると、既存の の使用が開始されますAWSServiceRoleForAmazonGuardDuty。

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、 AWS CLI、または IAM API を使用して、AWSServiceRoleForAmazonGuardDutyサービスにリンクされたロールを削除します。詳細については、IAM ユーザーガイドのサービスにリンクされたロールの削除を参照してください。

サポート対象 AWS リージョン

Amazon は、 AWS リージョン GuardDuty が利用可能なすべてので、AWSServiceRoleForAmazonGuardDutyサービスにリンクされたロールの使用 GuardDuty をサポートしています。 GuardDuty が現在利用可能なリージョンのリストについては、「」の「Amazon GuardDuty エンドポイントとクォータ」を参照してくださいAmazon Web Services 全般のリファレンス。

Malware Protection for EC2 のサービスにリンクされたロールのアクセス許可

Malware Protection for EC2 は、 という名前のサービスにリンクされたロール (SLR) を使用しますAWSServiceRoleForAmazonGuardDutyMalwareProtection。この SLR により、Malware Protection for EC2 はエージェントレススキャンを実行して GuardDuty 、アカウントのマルウェアを検出できます。これにより GuardDuty 、 アカウントで EBS ボリュームスナップショットを作成し、そのスナップショットを GuardDuty サービスアカウントと共有できます。がスナップショット GuardDuty を評価すると、取得した EC2 インスタンスとコンテナワークロードメタデータが Malware Protection for EC2 の検出結果に含まれます。AWSServiceRoleForAmazonGuardDutyMalwareProtection サービスにリンクされたロールは、ロールを継承するために malware-protection.guardduty.amazonaws.com のサービスを信頼します。

このロールのアクセス許可ポリシーは、Malware Protection for EC2 が次のタスクを実行するのに役立ちます。

- Amazon Elastic Compute Cloud (Amazon EC2) アクションを使用して、Amazon EC2 インスタンス、ボリューム、スナップショットに関する情報を取得します。Malware Protection for EC2 は、Amazon EKS および Amazon ECS クラスターメタデータにアクセスするためのアクセス許可も提供します。
- GuardDutyExcluded タグが true に設定されていない EBS ボリュームのスナップショットを作成してください。デフォルトでは、GuardDutyScanId タグを持つスナップショットが作成されます。このタグを削除しないでください。削除しないと、EC2 の Malware Protection はスナップショットにアクセスできません。

> **Important**
>
> GuardDutyExcluded を に設定するとtrue GuardDuty、サービスは今後これらのスナップショットにアクセスできなくなります。これは、このサービスにリンクされたロールの他のステートメントは GuardDuty 、 が GuardDutyExcludedに設定されているスナップショットに対して がアクションを実行できないためですtrue。

- スナップショットの共有と削除を許可するのは、GuardDutyScanId タグが存在し、GuardDutyExcluded タグが true に設定されていない場合のみです。

> **Note**
>
> Malware Protection for EC2 がスナップショットを公開することを許可しません。

- タグが GuardDutyExcludedに設定されているキーを除き、カスタマーマネージドキーにアクセスして を呼び出しtrue、 GuardDuty サービスアカウントと共有される暗号化されたスナップショットから暗号化された EBS ボリュームCreateGrantを作成してアクセスします。各リージョン GuardDuty のサービスアカウントのリストについては、「」を参照してくださいGuardDuty による サービスアカウント AWS リージョン。
- お客様の CloudWatch ログにアクセスしてEC2 ロググループ用の Malware Protection を作成し、マルウェアスキャンイベントログを/aws/guardduty/malware-scan-eventsロググループの下に配置します。
- マルウェアが検出されたスナップショットを自分のアカウントに保持するかどうかをお客様が決定できるようにします。スキャンでマルウェアが検出された場合、サービスにリンクされたロールは、 GuardDuty と の 2 つのタグをスナップショットに追加できますGuardDutyFindingDetectedGuardDutyExcluded。

> **Note**
>
> GuardDutyFindingDetected タグは、スナップショットにマルウェアが含まれていると指定します。

- ボリュームが EBS マネージドキーで暗号化されているかどうかを確認します。 GuardDuty は DescribeKeyアクションを実行して、アカウント内の EBS マネージドキーkey Idの を決定します。

- を使用して暗号化された EBS ボリュームのスナップショットを から取得 AWS アカウント し AWS マネージドキー、 にコピーしますGuardDuty サービスアカウント。この目的のために、 アクセス許可 GetSnapshotBlockと を使用しますListSnapshotBlocks。その後、 GuardDuty はサービスアカウントのスナップショットをスキャンします。現在、 で暗号化された EBS ボリュームのスキャンに対する Malware Protection for EC2 のサポートは、すべての で利用できない AWS マネージドキー 場合があります AWS リージョン。詳細については、「リージョン固有機能の可用性」を参照してください。
- Amazon EC2 が Malware Protection for EC2 AWS KMS に代わって を呼び出し、カスタマーマネージドキーに対して複数の暗号化アクションを実行できるようにします。kms:ReEncryptTo や kms:ReEncryptFrom のようなアクションは、カスタマーマネージドキーで暗号化されたスナップショットを共有するために必要です。GuardDutyExcluded タグが true に設定されていないキーだけがアクセス可能です。

ロールは、AmazonGuardDutyMalwareProtectionServiceRolePolicy と名付けられた次の AWS マネージドポリシーで構成されます。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
```

```
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyScanId"
                }
            }
        },
        {
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "PreventPublicAccessToSnapshotPermission",
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:Add/group": "all"
                }
            }
        },
        {
            "Sid": "CreateGrantPermission",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
```

```
                    "CreateGrant",
                    "GenerateDataKeyWithoutPlaintext",
                    "ReEncryptFrom",
                    "ReEncryptTo",
                    "RetireGrant",
                    "DescribeKey"
                ]
            },
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    },
    {
        "Sid": "ShareSnapshotKMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:ReEncryptTo",
            "kms:ReEncryptFrom"
        ],
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "ec2.*.amazonaws.com"
            },
            "Null": {
                "aws:ResourceTag/GuardDutyExcluded": "true"
            }
        }
    },
    {
        "Sid": "DescribeKeyPermission",
        "Effect": "Allow",
        "Action": "kms:DescribeKey",
        "Resource": "arn:aws:kms:*:*:key/*"
    },
    {
        "Sid": "GuardDutyLogGroupPermission",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:CreateLogGroup",
            "logs:PutRetentionPolicy"
        ],
```

```
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
        },
        {
            "Sid": "GuardDutyLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
        },
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

AWSServiceRoleForAmazonGuardDutyMalwareProtection サービスにリンクされたロールにアタッチされている信頼ポリシーは次のとおりです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Malware Protection for EC2 のサービスにリンクされたロールの作成

AWSServiceRoleForAmazonGuardDutyMalwareProtection サービスにリンクされたロールは、EC2 の Malware Protection を初めて有効にするか、以前に有効にしていなかったサポートされているリージョンで EC2 の Malware Protection を有効にしたときに自動的に作成されます。IAM コンソール、IAM CLI、あるいは IAM API を使って、AWSServiceRoleForAmazonGuardDutyMalwareProtection サービスにリンクされたロールを手動で作成することもできます。

> **Note**
>
> デフォルトでは、Amazon を初めて使用する場合 GuardDuty、EC2 の Malware Protection は自動的に有効になります。

> **Important**
>
> 委任 GuardDuty 管理者アカウント用に作成されたサービスにリンクされたロールは、メンバー GuardDuty アカウントには適用されません。

サービスにリンクされたロールの作成、編集、削除をIAM プリンシパル (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。AWSServiceRoleForAmazonGuardDutyMalwareProtection サービスにリンクされたロールを正常に作成するには、 GuardDuty で使用する IAM ID に必要なアクセス許可が必要です。必要なアクセス許可を付与するには、次のポリシーをこの ユーザー、グループ、またはロールにアタッチします。

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

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

IAM ロールを手動で作成する方法の詳細は、「IAM ユーザーガイド」の「サービスにリンクされたロールを作成する」を参照してください。

Malware Protection for EC2 のサービスにリンクされたロールの編集

Malware Protection for EC2 では、AWSServiceRoleForAmazonGuardDutyMalwareProtection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すると、多くのエンティティによっ

てロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。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。

Malware Protection for EC2 のサービスにリンクされたロールの削除

サービスリンクロール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。これにより、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。

> **Important**
>
> を削除するにはAWSServiceRoleForAmazonGuardDutyMalwareProtection、まず、EC2 が有効になっているすべてのリージョンで Malware Protection for EC2 を無効にする必要があります。
> サービスにリンクされたロールを削除しようとしたときに Malware Protection for EC2 が無効になっていない場合、削除は失敗します。詳細については、「 GuardDuty実行型マルウェアスキャンを有効または無効にするには」を参照してください。

Disable を選択して Malware Protection for EC2 サービスを停止しても、AWSServiceRoleForAmazonGuardDutyMalwareProtection は自動的に削除されません。次に、Enable を選択して Malware Protection for EC2 サービスを再度開始すると、 GuardDuty は既存の の使用を開始しますAWSServiceRoleForAmazonGuardDutyMalwareProtection。

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、 AWS CLI、または IAM API を使用して、AWSServiceRoleForAmazonGuardDutyMalwareProtectionサービスにリンクされたロールを削除します。詳細については、IAM ユーザーガイドのサービスにリンクされたロールの削除を参照してください。

サポート対象 AWS リージョン

Amazon は、Malware Protection for EC2 AWS リージョン が利用可能なすべての で、AWSServiceRoleForAmazonGuardDutyMalwareProtectionサービスにリンクされたロールの使用 GuardDuty をサポートしています。

GuardDuty が現在利用可能なリージョンのリストについては、「」の「Amazon GuardDuty エンドポイントとクォータ」を参照してくださいAmazon Web Services 全般のリファレンス。

> **Note**
>
> EC2 の Malware Protection は現在、 AWS GovCloud （ 米国東部) および AWS GovCloud （ 米国西部) では利用できません。

AWS Amazon の マネージドポリシー GuardDuty

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

AWS サービスは、 AWS 管理ポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。サービスは、新機能をサポートするために、 AWS マネージドポリシーにアクセス許可を追加することがあります。この種の更新は、ポリシーがアタッチされているすべてのアイデンティティ (ユーザー、グループ、ロール) に影響を与えます。サービスは、新機能の起動時または新しいオペレーションが利用可能になったときに、 AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS 管理ポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が破損することはありません。

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

AWS マネージドポリシー: AmazonGuardDutyFullAccess

`AmazonGuardDutyFullAccess` ポリシーは IAM ID にアタッチできます。

このポリシーは、ユーザーにすべての GuardDuty アクションへのフルアクセスを許可する管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- GuardDuty – すべての GuardDutyアクションへのフルアクセスをユーザーに許可します。
- IAM:
  - GuardDuty サービスにリンクされたロールの作成をユーザーに許可します。
  - 管理者アカウントがメンバーアカウント GuardDuty に対して を有効にすることを許可します。
  - ユーザーが、このロール GuardDuty を使用して GuardDuty Malware Protection for S3 機能を有効にするロールを に渡すことを許可します。これは、 GuardDuty サービス内で、または個別に S3 の Malware Protection を有効にする方法とは関係ありません。
- Organizations – ユーザーが委任された管理者を指定し、 GuardDuty 組織のメンバーを管理できるようにします。

でiam:GetRoleアクションを実行するアクセス許可は、Malware Protection for EC2 のサービスにリンクされたロール (SLR) がアカウントに存在するかどうかAWSServiceRoleForAmazonGuardDutyMalwareProtectionを確立します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "AmazonGuardDutyFullAccessSid1",
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IamGetRoleSid1",
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        },
        {
            "Sid": "AllowPassRoleToMalwareProtectionPlan",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS マネージドポリシー: AmazonGuardDutyReadOnlyAccess

AmazonGuardDutyReadOnlyAccess ポリシーは IAM ID にアタッチできます。

このポリシーは、ユーザーが GuardDuty 組織 GuardDuty の結果と詳細を表示できるようにする読み取り専用アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- GuardDuty – ユーザーが GuardDuty 結果を表示し、Get、、Listまたは で始まる API オペレーションを実行できるようにしますDescribe。
- Organizations – 委任された管理者アカウントの詳細など、 GuardDuty 組織設定に関する情報の取得をユーザーに許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:Describe*",
                "guardduty:Get*",
                "guardduty:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS マネージドポリシー: AmazonGuardDutyServiceRolePolicy

IAM エンティティに AmazonGuardDutyServiceRolePolicy をアタッチすることはできません。この AWS 管理ポリシーは、 がユーザーに代わってアクションを実行できるようにするサービスに

リンクされたロール GuardDuty にアタッチされます。詳細については、「のサービスにリンクされたロールのアクセス許可 GuardDuty」を参照してください。

GuardDuty AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した GuardDuty 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、 GuardDuty ドキュメント履歴ページの 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
AmazonGuardDutyFullAccess - 既存ポリシーへの更新	Malware Protection for S3 を有効にするときに IAM ロールを GuardDuty に渡すことができるアクセス許可を追加しました。 { "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "guardduty.amazonaws.com" } }	2024 年 6 月 10 日

変更	説明	日付
	`}`	
AmazonGuardDutyServiceRolePolicy – 既存ポリシーへの更新。	Amazon EC2 の自動エージェントで Runtime Monitoring を有効にする場合は、 AWS Systems Manager アクションを使用して Amazon EC2 インスタンスの GuardDuty SSM 関連付けを管理します。GuardDuty 自動エージェント設定が無効になっている場合、包含タグ (`GuardDutyManaged : true`) を持つ EC2 インスタンスのみ GuardDuty を考慮します。	2024 年 3 月 26 日
AmazonGuardDutyServiceRolePolicy – 既存ポリシーへの更新。	GuardDuty は、共有 Amazon VPC アカウントの組織 ID を取得し、組織 ID で Amazon VPC エンドポイントポリシーを設定`organization:DescribeOrganization` するための新しいアクセス許可 を追加しました。	2024 年 2 月 9 日

変更	説明	日付
AmazonGuardDutyMalwareProtectionServiceRolePolicy – 既存ポリシーへの更新。	Malware Protection for EC2 に 2 つのアクセス許可が追加されました。 `GetSnapshotBlock` と `ListSnapshotBlocks` は、から EBS ボリュームのスナップショット (を使用して暗号化 AWS マネージドキー) を取得し、マルウェアスキャンを開始する前に GuardDuty サービスアカウントにコピーします AWS アカウント 。	2024 年 1 月 25 日
AmazonGuardDutyServiceRolePolicy – 既存ポリシーへの更新	が `guarddutyActivate` Amazon ECS アカウント設定を追加し、Amazon ECS クラスターでリストおよび記述オペレーションを実行 GuardDuty できるようにする新しいアクセス許可を追加しました。	2023 年 11 月 26 日
AmazonGuardDutyReadOnlyAccess – 既存ポリシーへの更新	GuardDuty は、 の新しいポリシー`organizations` をに追加しました`ListAccounts` 。	2023 年 11 月 16 日
AmazonGuardDutyFullAccess – 既存ポリシーへの更新	GuardDuty は、 の新しいポリシー`organizations` をに追加しました`ListAccounts` 。	2023 年 11 月 16 日

変更	説明	日付
AmazonGuardDutyServiceRolePolicy – 既存ポリシーへの更新	GuardDuty は、今後の GuardDuty EKS Runtime Monitoring 機能をサポートする新しいアクセス許可を追加しました。	2023 年 3 月 8 日
AmazonGuardDutyServiceRolePolicy – 既存ポリシーへの更新	GuardDuty は、 GuardDuty が Malware Protection for EC2 のサービスにリンクされたロールを作成できるようにする新しいアクセス許可を追加しました。これにより、GuardDutyEC2 の Malware Protection を有効にするプロセスを合理化できます。 GuardDuty では、次の IAM アクションを実行できるようになりました。 `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	2023 年 2 月 21 日

変更	説明	日付
AmazonGuardDutyFullAccess – 既存ポリシーへの更新	GuardDuty が の ARN を iam:GetRole に更新しました*AWSServiceRoleForAmazonGuardDutyMalwareProtection 。	2022 年 7 月 26 日
AmazonGuardDutyFullAccess – 既存ポリシーへの更新	GuardDuty は、EC2 サービスiam:CreateServiceLinkedRole 用 GuardDuty Malware Protection を使用してサービスにリンクされたロールを作成AWSServiceName できるようにする新しい を追加しました。 GuardDuty で iam:GetRole アクションを実行して、の情報を取得できるようになりましたAWSServiceRole 。	2022 年 7 月 26 日

変更	説明	日付
AmazonGuardDutyServiceRolePolicy – 既存ポリシーへの更新	GuardDuty は、Amazon EC2 ネットワークアクションを使用して検出結果を改善 GuardDuty できるようにする新しいアクセス許可を追加しました。 GuardDuty では、次の EC2 アクションを実行して、EC2 インスタンスの通信方法に関する情報を取得できるようになりました。この情報は、検出結果の精度を向上させるために使用されます。 • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	2021 年 8 月 3 日
GuardDuty が変更の追跡を開始しました	GuardDuty が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 8 月 3 日

Amazon GuardDuty 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、 および IAM の使用時に発生する可能性がある一般的な問題の診断 GuardDuty と修正に役立ちます。

トピック

でアクションを実行する権限がない GuardDuty

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なguardduty:*GetWidget* アクセス許可を持っていない場合に発生するものです。

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

この場合、guardduty:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

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

iam を実行する権限がありませんPassRole。

iam:PassRole アクションを実行する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 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 GuardDuty。

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

次の例のエラーは、 という IAM marymajor ユーザーがコンソールを使用して でアクションを実行しようする場合に発生します GuardDuty。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

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

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

自分の 以外のユーザーに自分の GuardDuty リソース AWS アカウント へのアクセスを許可したい。

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

詳細については、以下を参照してください:

- がこれらの機能 GuardDuty をサポートしているかどうかを確認するには、「」を参照してくださいAmazon と IAM GuardDuty の連携方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

Amazon のコンプライアンス検証 GuardDuty

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照

し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

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

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

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

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。

- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon GuardDuty の回復力

AWS のグローバルインフラストラクチャは AWS リージョンとアベイラビリティーゾーンを中心として構築されます。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。

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

Amazon GuardDuty でのインフラストラクチャセキュリティ

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

AWS が発行している API コールを使用して、ネットワーク経由で GuardDuty にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS) TLS 1.2 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

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

AWS と のサービス統合 GuardDuty

GuardDuty は、他の AWS セキュリティサービスと統合できます。これらのサービスは からデータを取り込むことができ GuardDuty 、検出結果を新しい方法で表示できます。以下の統合オプションを確認して、そのサービスが で動作するように設定される方法の詳細を確認してください GuardDuty。

GuardDuty との統合 AWS Security Hub

AWS Security Hub は、 AWS アカウント、サービス、およびサポートされているサードパーティーパートナー製品からセキュリティデータを収集し、業界標準とベストプラクティスに従って環境のセキュリティ状態を評価します。セキュリティ体制の評価に加えて、Security Hub は、統合されたすべての AWS サービスおよび AWS パートナー製品にわたる検出結果のための一元的な場所を作成します。で Security Hub を有効にすると GuardDuty 、Security Hub によって GuardDuty 結果データが自動的に取り込まれます。

で Security Hub を使用する方法の詳細については、 GuardDuty 「」を参照してくださいとの統合 AWS Security Hub。

Amazon Detective GuardDuty との統合

Amazon Detective は、 AWS アカウント全体のログデータを使用して、 環境とやり取りするリソースと IP アドレスのデータ視覚化を作成します。Detective のビジュアライゼーションは、セキュリティ問題をすばやく簡単に調査するのに役立ちます。両方のサービスを有効にすると、 GuardDuty 検出結果の詳細から Detective コンソールの情報にピボットできます。

で Detective を使用する方法の詳細については、 GuardDuty 「」を参照してくださいAmazon Detective を使用した調査。

との統合 AWS Security Hub

AWS Security Hub では、 AWS のセキュリティ状態を総合的に把握することができ、セキュリティ業界標準およびベストプラクティスに照らし合わせて環境をチェックすることができます。Security Hub は、 AWS アカウント、サービス、およびサポートされているサードパーティーパートナー製品からセキュリティデータを収集し、セキュリティの傾向を分析し、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。

Amazon と Security Hub GuardDuty の統合により、 から Security Hub GuardDuty に結果を送信できます。Security Hub では、このような検出結果をセキュリティ体制の分析に含めることができます。

目次

Amazon が検出結果を GuardDuty に送信する方法 AWS Security Hub

では AWS Security Hub、セキュリティの問題は検出結果として追跡されます。検出結果の中には、他の AWS のサービスやサードパーティーパートナーによって検出された問題に由来するものもあります。Security Hub には、セキュリティの問題を検出し、検出結果を生成するために使用する一連のルールもあります。

Security Hub には、これらすべてのソースからの結果を管理するためのツールが用意されています。検出結果の一覧を表示およびフィルタリングして、検出結果の詳細を表示できます。詳細については、AWS Security Hub ユーザーガイドの「検出結果の表示」を参照してください。検出結果の調査状況を追跡することもできます 詳細については、AWS Security Hub ユーザーガイドの「検出結果に対するアクションの実行」を参照してください。

Security Hub のすべての検出結果は、 AWS Security Finding Format (ASFF) と呼ばれる標準 JSON 形式を使用します。ASFF には、問題のソース、影響を受けるリソース、および検出結果の現在のステータスに関する詳細が含まれます。 AWS ユーザーガイド の「AWS Security Hub Security Finding 形式 (ASFF)」を参照してください 。

Amazon GuardDuty は、結果を Security Hub に送信する AWS サービスの 1 つです。

が Security Hub GuardDuty に送信する検出結果のタイプ

同じ 内の同じアカウントで GuardDuty と Security Hub を有効にすると AWS リージョン、GuardDuty は生成されたすべての検出結果を Security Hub に送信し始めます。これらの検出結果は、Security AWS Finding 形式 (ASFF) を使用して Security Hub に送信されます。ASFF では、Types フィールドが検出結果タイプを提供します。

新しい検出結果の送信のレイテンシー

が新しい検出結果 GuardDuty を作成すると、通常 5 分以内に Security Hub に送信されます。

Security Hub が使用できない場合の再試行

Security Hub が使用できない場合、 は検出結果を受信するまで送信を GuardDuty 再試行します。

Security Hub の既存の結果を更新する

Security Hub に結果を送信すると、 GuardDuty は結果アクティビティの追加観測を反映するように更新を Security Hub に送信します。これらの検出結果の新しい観察結果は、 ステップ 5 – 検出結果のエクスポート頻度の設定に基づいて Security Hub に送信されます AWS アカウント。

検出結果をアーカイブまたはアーカイブ解除する場合、その検出 GuardDuty 結果を Security Hub に送信しないでください。後で でアクティブになる手動でアーカイブ解除された検出 GuardDuty 結果は、Security Hub に送信されません。

で GuardDuty の結果の表示 AWS Security Hub

Security Hub で GuardDuty 検出結果を表示するには、概要ページから「Amazon GuardDuty の検出結果」を選択します。または、ナビゲーションパネルから検出結果を選択し、 値を持つ製品名 : フィールドを選択して GuardDuty 検出結果のみを表示するようにフィルタリングすることもできますGuardDuty。

で GuardDuty の検出結果名の解釈 AWS Security Hub

GuardDuty は、Security AWS Finding 形式 (ASFF) を使用して結果を Security Hub に送信します。ASFF では、Types フィールドが検出結果タイプを提供します。ASFF タイプは、タイプとは異なる命名スキーム GuardDutyを使用します。次の表は、Security Hub に表示される ASFF に対応するすべての GuardDuty 検出結果タイプの詳細を示しています。

> **Note**
>
> 一部の検出 GuardDuty 結果タイプでは、Security Hub は、検出結果の詳細のリソースロールが ACtor か TARGET かに応じて、異なる ASFF 検出結果名を割り当てます。詳細については、検出結果の詳細を参照してください。

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B

GuardDuty 検出結果タイプ	ASFF 結果タイプ
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion:IAMUser /AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
検出:IAMUser /AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
影響:IAMUser /AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:IAMUser /AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
永続性:IAMUser /AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser /AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleBindingCreated
PriviledgeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic

GuardDuty 検出結果タイプ	ASFF 結果タイプ
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin

GuardDuty 検出結果タイプ	ASFF 結果タイプ
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient

GuardDuty 検出結果タイプ	ASFF 結果タイプ
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

GuardDuty からの一般的な結果

GuardDuty は Security AWS Finding 形式 (ASFF) を使用して Security Hub に結果を送信します。

からの一般的な検出結果の例を次に示します GuardDuty。


```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
```

```
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
```

```
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


統合の有効化と構成

との統合を使用するには AWS Security Hub、Security Hub を有効にする必要があります。Security Hub を有効にする方法については、「AWS Security Hub ユーザーガイド」の「Setting up Security Hub」(Security Hub の設定) を参照してください。

GuardDuty と Security Hub の両方を有効にすると、統合は自動的に有効になります。 GuardDuty はすぐに Security Hub に結果を送信し始めます。

結果の Security Hub への公開の停止

Security Hub への結果の送信を停止するには、Security Hub コンソールまたは API を使用できます。

「 ユーザーガイド」の「統合からの検出結果のフローの無効化と有効化 (コンソール) 」または「統合からの検出結果のフローの無効化 (Security Hub API、 AWS CLI)」を参照してください。 AWS Security Hub

Amazon Detective を使用した調査

Amazon Detective は、経時的なリソースの動作方法や交信方法を示すデータを可視化することで、1 つ以上のアカウントの AWS セキュリティイベントを迅速に分析し、調査するのに役立ちます。Detective は、GuardDuty の検出結果の可視化を作成します。

Detective は、すべての検出結果タイプの検出結果の詳細を取り込み、検出結果に関連するさまざまなエンティティを調査する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。エンティティは AWS アカウント、アカウント内の AWS リソース、またはリソースと交信する IP アドレスである可能性があります。GuardDuty コンソールは、検出結果タイプに応じてエンティティ (AWS アカウント、IAM ロール、IAM ユーザー、IAM ロールセッション、ユーザーエージェント、フェデレーションユーザー、Amazon EC2 インスタンス、IP アドレス) から Amazon Detective へのピボットをサポートしています。

目次

統合の有効化

GuardDuty で Amazon Detective を使用するには、まず Amazon Detective を有効にする必要があります。Detective を有効にする方法については、「Amazon Detective の管理ガイド」の「Amazon Detective の設定」を参照してください。

GuardDuty と Detective の両方を有効にすると、統合は自動的に有効になります。有効にすると、Detective はすぐに GuardDuty の検出結果データを取り込みます。

> **Note**
>
> GuardDuty は、GuardDuty の検出結果エクスポート頻度に基づいて Detective に検出結果を送信します。デフォルトで、既存の検出結果の更新用のエクスポート頻度は 6 時間です。Detective が最新の更新検出結果を受信できるように、GuardDuty で Detective を使用する各リージョンで、エクスポート頻度を 15 分に変更することをお勧めします。詳細については、「ステップ 5 – 更新されたアクティブな検出結果をエクスポートする頻度を設定する」を参照してください。

GuardDuty の検出結果から Amazon Detective へのピボット

1. https://console.aws.amazon.com/guardduty/ コンソールにログインします。
2. 検出結果テーブルから 1 つの検出結果を選択します。
3. 検出結果詳細ペインで、[Investigate with Detective] (Detective で調査する) を選択します。
4. Amazon Detective で検出結果のアスペクトを選択します。これにより、その検出結果またはエンティティの Detective コンソールが開きます。

ピボットが正常に動作しない場合は、「Amazon Detective ユーザーガイド」の「ピボットのトラブルシューティング」を参照してください。

> **Note**
>
> Detective コンソールで GuardDuty の検出結果をアーカイブすると、その検出結果は GuardDuty コンソールでもアーカイブされます。

GuardDuty マルチアカウント環境との統合を使用します。

GuardDuty でマルチアカウント環境を管理している場合、アカウントの検出結果とエンティティの Detective データの可視化するために、メンバーアカウントを Amazon Detective に追加する必要があります。

Detective の管理者アカウントと同じ GuardDuty 管理者アカウントを使用することをお勧めします。Detective でのメンバーアカウントの追加についての詳細は、「メンバーアカウントの招待」を参照してください。

> **Note**
>
> Detective はリージョンレベルのサービスなので、Detective を有効にして、統合を使用したいリージョンごとにメンバーアカウントを追加する必要があります。

一時停止または無効化 GuardDuty

GuardDuty コンソールを使用して、 GuardDuty サービスを一時停止または無効にできます。サービスが停止 GuardDuty されている場合、 の使用に対して課金されることはありません。

- を一時停止または削除する前に、すべてのメンバーアカウントの関連付けを解除または削除する必要があります GuardDuty。
- を停止すると GuardDuty、 AWS 環境のセキュリティをモニタリングしたり、新しい検出結果を生成したりしなくなります。既存の検出結果はそのまま残り、 GuardDuty 停止の影響を受けません。 GuardDuty 後で再度有効にすることもできます。
- アカウント GuardDuty で を無効にすると、現在選択されている でのみ無効になります AWS リージョン。を完全に無効にするには GuardDuty、有効にされている各リージョンで無効にする必要があります。
- を無効にすると GuardDuty、既存の検出結果と GuardDuty 設定は失われ、復元できなくなります。既存の検出結果を保存する場合は、 を無効にすることを確認する前にエクスポートする必要があります GuardDuty。検出結果のエクスポート方法の詳細については、「検出結果のエクスポート」を参照してください。
- アカウント内の 1 つ以上の保護されたバケットに対して Malware Protection for S3 を有効にしている場合、S3 の Malware Protection で保護されたバケットのステータスには影響 GuardDuty しません。を一時停止または無効化した後でも GuardDuty、Malware Protection for S3 機能に関連する使用コストは引き続きアカウントに発生します。S3 の Malware Protection を無効にする方法については、「」を参照してください保護されたバケットの S3 の Malware Protection を無効にする。

を一時停止または無効化するには GuardDuty

1. https://console.aws.amazon.com/guardduty/ で GuardDuty 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. 停止 GuardDutyセクションで、 の停止 GuardDutyまたは無効化 GuardDutyを選択し、アクションを確認します。

一時停止 GuardDuty 後に再度有効にするには

1. https://console.aws.amazon.com/guardduty/ で GuardDuty 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. 再有効化を選択します GuardDuty。

Amazon SNS GuardDuty の発表をサブスクライブする

このセクションでは、新しくリリースされた検出結果タイプ、既存の検出結果タイプの更新、およびその他の機能の変更に関する通知を受け取るための GuardDuty 通知について、Amazon SNS (Simple Notification Service) にサブスクライブする方法について説明します。Amazon SNS がサポートするすべての形式で通知を使用できます。

GuardDuty SNS は、 全体の GuardDuty サービスの更新に関する通知を、サブスクライブしている AWS アカウントに送信します。アカウント内の検出結果に関する通知を受け取るには、「Amazon CloudWatch Events を使用した GuardDuty 結果へのカスタムレスポンスの作成」を参照してください。

> **Note**
>
> SNS をサブスクライブする場合、IAM ユーザーに `sns::subscribe` アクセス許可が必要です。

この通知トピックへの Amazon SQS キューをサブスクライブできますが、同じリージョンのトピックの ARN を使用する必要があります。詳細については、「Amazon Simple Queue Service デベロッパーガイド」の「チュートリアル: Amazon SNS トピックへの Amazon SQS キューのサブスクライブ」を参照してください。

また、 AWS Lambda 関数を使用して、通知を受信したときにイベントをトリガーすることもできます。詳細については、「Amazon Simple Queue Service デベロッパーガイド」の「Amazon SNS 通知を使用した Lambda 関数の呼び出し」を参照してください。

各リージョンの Amazon SNS トピックの ARN は次のとおりです。

AWS リージョン	Amazon SNS トピックの ARN
us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements
us-east-2	arn:aws:sns:us-east-2:118283430703:G

AWS リージョン	Amazon SNS トピックの ARN
	uardDutyAnnouncements
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

AWS リージョン	Amazon SNS トピックの ARN
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

AWS リージョン	Amazon SNS トピックの ARN
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

AWS リージョン	Amazon SNS トピックの ARN
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

AWS リージョン	Amazon SNS トピックの ARN
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

で GuardDuty 更新通知 E メールをサブスクライブするには AWS Management Console

1. https://console.aws.amazon.com/sns/v3/home で Amazon SNS コンソールを開きます。
2. リージョンのリストで、サブスクライブするトピックの ARN として同じリージョンを選択します。この例では、us-west-2 リージョンを使用します。
3. 左のナビゲーションペインで、[Subscriptions] (サブスクリプション)、[Create subscription] (サブスクリプションの作成) の順に選択します。
4. [Create Subscription] (サブスクリプションの作成) ダイアログボックスの [Topic ARN] (トピック ARN) で、トピック ARN `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements` を貼り付けます。
5. [Protocol] (プロトコル) で [Email] (E メール) を選択します。[Endpoint] (エンドポイント) で、通知を受信するために使用できる E メールアドレスを入力します。
6. [Create subscription] (サブスクリプションの作成) を選択します。
7. E メールアプリケーションで、 AWS 通知からのメッセージを開き、リンクを開いてサブスクリプションを確認します。

   ウェブブラウザに Amazon SNS の確認画面が表示されます。

を使用して GuardDuty 更新通知 E メールにサブスクライブするには AWS CLI

1. AWS CLIを使用して次のコマンドを実行します。

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. E メールアプリケーションで、 AWS 通知からのメッセージを開き、リンクを開いてサブスクリプションを確認します。

   ウェブブラウザに Amazon SNS の確認画面が表示されます。

Amazon SNS メッセージ形式

新しい検出結果に関する GuardDuty 更新通知メッセージの例を以下に示します。

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
```

```
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

解析された [Message] (メッセージ) の値 (エスケープした引用符は削除) は次のように表示されます。

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

GuardDuty 機能 GuardDuty の更新に関する更新通知メッセージの例を以下に示します。

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_cloudtrail\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
```

```
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

解析された [Message] (メッセージ) の値 (エスケープした引用符は削除) は次のように表示されます。

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_cloudtrail"
    }]
}
```

更新された結果に関する GuardDuty 更新通知メッセージの例を以下に示します。

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
```

```
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

解析された [Message] (メッセージ) の値 (エスケープした引用符は削除) は次のように表示されます。

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

Amazon GuardDuty クォータ

には、 ごとに、以前 AWS アカウント は制限と呼ばれていたデフォルトのクォータがあります AWS のサービス。特に明記されていない限り、クォータは地域固有です。一部のクォータの増加を要求できますが、他のクォータは増加できません。

のクォータを表示するには GuardDuty、Service Quotas コンソール を開きます。ナビゲーションペインで、Amazon GuardDutyAWS のサービスを選択して選択します。

クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。

AWS アカウント には、リージョン GuardDuty ごとに Amazon の次のクォータがあります。

> **Note**
>
> - Malware Protection for EC2 に固有のクォータについては、 GuardDuty 「」を参照してくださいEC2 クォータの Malware Protection。
> - Malware Protection for S3 に固有のクォータについては、「」を参照してくださいMalware Protection for S3 のクォータ。

GuardDuty リージョンあたりのクォータ

リソース	デフォルト	コメント
ディテクター	1	各リージョンの AWS アカウントごとに作成できるディテクターリソースの最大数。 クォータの引き上げをリクエストすることはできません。
フィルター	100	リージョンごとの AWS アカウントあた

リソース	デフォルト	コメント
		りの保存済みフィルターの最大数。 クォータの引き上げをリクエストすることはできません。
検出結果の保持期間	90 日間	検出結果を保持する最大日数。 クォータの引き上げをリクエストすることはできません。
信頼できる IP リストあたりの IP アドレスと CIDR 範囲	2,000	1 つの信頼できる IP リストに含めることができる IP アドレスと CIDR 範囲の最大数。 クォータの引き上げをリクエストすることはできません。
脅威リストあたりの IP アドレスと CIDR 範囲	250,000	脅威リストに含めることができる IP アドレスと CIDR 範囲の最大数。 クォータの引き上げをリクエストすることはできません。

リソース	デフォルト	コメント
最大ファイルサイズ	35 MB	信頼できる IP リストまたは脅威リストに含める IP アドレスまたは CIDR 範囲のリストをアップロードするために使用されるファイルの最大ファイルサイズ。 クォータの引き上げをリクエストすることはできません。
メンバーアカウント数 (招待による)	5000	管理者アカウントに関連付けられたメンバーアカウントの最大数。 クォータの引き上げをリクエストすることはできません。

リソース	デフォルト	コメント
メンバーアカウント	50,000	を通じて管理者アカウントに関連付けられているメンバーアカウントの最大数 AWS Organizations。これには、招待によって組織に追加されたメンバーアカウントが含まれます。 このデフォルト値は、 のメンバーアカウントの現在のクォータによって異なります AWS Organizations。を通じて GuardDuty 追加された のメンバーアカウントの数は AWS Organizations 、組織内のメンバーアカウントの数を超えることはできません。組織 AWS アカウント 内の の数については、「 ユーザーガイド」の「最大値と最小値AWS Organizations 」を参照してください。

リソース	デフォルト	コメント
脅威インテリジェンスセット	6	各リージョンの AWS アカウントごとに追加できる脅威インテリジェンスセットの最大数。 クォータの引き上げをリクエストすることはできません。
信頼できる IP セット	1	リージョンごとに AWS アカウントごとにアップロードおよびアクティブ化できる信頼された IP セットの最大数。 クォータの引き上げをリクエストすることはできません。

Amazon のトラブルシューティング GuardDuty

に固有のアクションを実行することに関連する問題が発生した場合は GuardDuty、このセクションのトピックを参照してください。

トピック

の一般的な問題 GuardDuty

GuardDuty 検出結果のエクスポート中にアクセスエラーが発生します。これを解決するにはどうすればよいですか？

検出結果をエクスポートするように設定した後、 GuardDuty が検出結果をエクスポートできない場合、 GuardDuty コンソールの設定ページにエラーメッセージが表示されます。これは、Amazon S3 バケットが削除された場合やバケットへのアクセス許可が変更された場合など、 がターゲットリソースにアクセス GuardDuty できなくなった場合に発生する可能性があります。これは、 が Amazon GuardDuty S3 バケット内のデータの暗号化に使用された AWS KMS キーにアクセスできなくなった場合にも発生する可能性があります。 Amazon S3 GuardDuty が エクスポートできない場合、 アカウントに関連付けられた E メールに通知を送信し、この問題に関する情報を提供します。

この問題を解決するには、対応するリソースが存在し、必要なリソースにアクセスするためのアクセス許可 GuardDuty があることを確認してください。で 90 日間の検出結果の保持期間が完了する前に問題を解決しない場合 GuardDuty、検出結果はエクスポートされません。 は、特定のリージョンでこのアカウントの検出結果のエクスポート設定を GuardDuty 無効にします。この保持日以降でも、設定を更新して、特定のリージョンで検出結果のエクスポートを再開できます。

詳細については、「検出結果のエクスポート」を参照してください。

EC2 の問題に対する Malware Protection

オンデマンドのマルウェアスキャンを開始しようとしていますが、必要な許可がないというエラーが表示されます。

Amazon EC2 インスタンスでオンデマンドマルウェアスキャンを開始するのに必要な許可がないことを示すエラーが表示された場合は、AWS マネージドポリシー: AmazonGuardDutyFullAccess ポリシーを IAM ロールにアタッチしていることを確認してください。

AWS 組織のメンバーでも同じエラーが表示される場合は、管理アカウントに接続します。詳細については、「AWS Organizations SCP – アクセス拒否」を参照してください。

Malware Protection for EC2 の使用中に**`iam:GetRole`**エラーが発生します。

このエラー が表示される場合は`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`、 GuardDuty実行型マルウェアスキャンを有効にするか、オンデマンドマルウェアスキャンを使用するためのアクセス許可がないことを意味します。AWS マネージドポリシー: AmazonGuardDutyFullAccess ポリシーが IAM ロールにアタッチされていることを確認します。

GuardDuty実行型マルウェアスキャンを有効にする必要がある GuardDuty 管理者アカウントですが、 AWS 管理ポリシー AmazonGuardDutyFullAccess を使用して を管理していません GuardDuty。

- で使用する IAM ロールを設定 GuardDuty して、 GuardDuty実行型マルウェアスキャンを有効にするために必要なアクセス許可を付与します。必要なアクセス許可の詳細については、「Malware Protection for EC2 のサービスにリンクされたロールの作成」を参照してください。
- AWS マネージドポリシー: AmazonGuardDutyFullAccess を IAM ロールにアタッチします。これにより、メンバーアカウントの GuardDuty実行型マルウェアスキャンを有効にすることができます。

Runtime Monitoring の問題

AWS Step Functions ワークフローが予期せず失敗している

GuardDuty コンテナがワークフローの失敗の原因であった場合は、「」を参照してくださいカバレッジ問題のトラブルシューティング。問題が解決しない場合は、 GuardDuty コンテナが原因でワークフローが失敗しないように、次のいずれかのステップを実行します。

- 関連付けられた Amazon ECS クラスターに `GuardDutyManaged：false` タグを追加します。
- アカウントレベルで AWS Fargate (ECS のみ) の自動エージェント設定を無効にします。GuardDuty 自動エージェントでモニタリングを継続する関連付けられた Amazon ECS クラスターに包含タグ `GuardDutyManaged：true` を追加します。

Runtime Monitoring でのメモリ不足エラーのトラブルシューティング (Amazon EC2 サポートのみ)

このセクションでは、 に基づいてメモリ不足エラーが発生しCPU とメモリの制限、 GuardDuty セキュリティエージェントを手動でデプロイした場合のトラブルシューティング手順について説明します。

`out-of-memory` が問題のために GuardDuty エージェント`systemd`を終了し、 GuardDuty エージェントにより多くのメモリを提供することが合理的であると判断した場合は、制限を更新できます。

1. root 権限で、`/lib/systemd/system/amazon-guardduty-agent.service` を開きます。
2. `MemoryLimit` と `MemoryMax`を検索し、両方の値を更新します。

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. 値を更新したら、次のコマンドを使用して GuardDuty エージェントを再起動します。

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. 以下のコマンドを実行して、ステータスを表示します。

```
sudo systemctl status amazon-guardduty-agent
```

予想される出力には、新しいメモリ制限が表示されます。

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

複数のアカウントの問題の管理

複数のアカウントを管理したいが、必要な AWS Organizations 管理アクセス許可がない。

このエラー が表示される場合はThe request failed because you do not have required AWS Organization master permission.、組織内の複数のアカウントに対して GuardDuty実行型マルウェアスキャンを有効にするアクセス許可がないことを意味します。管理アカウントへのアクセス許可の付与の詳細については、「」を参照してください GuardDutyが開始するマルウェアスキャンを有効にするための信頼されたアクセスを確立する。

その他の問題のトラブルシューティング

問題に適したシナリオが見つからない場合は、次のトラブルシューティングもご参照ください。

- https://console.aws.amazon.com/guardduty/ へのアクセス時の IAM に関する一般的な問題については、「Amazon GuardDuty 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。
- にアクセスする際の認証と承認の問題については AWS AWS Console Home、「IAM のトラブルシューティング」を参照してください。

リージョンとエンドポイント

Amazon GuardDuty が利用可能な を表示するには、 AWS リージョン 「」の「Amazon GuardDuty エンドポイント」を参照してくださいAmazon Web Services 全般のリファレンス。

サポートされているすべての GuardDuty で を有効にすることをお勧めします AWS リージョン。これにより、アクティブ GuardDuty に使用されていないリージョンでも、不正または異常なアクティビティに関する検出結果を生成できます。これにより、 GuardDuty はサポートされている の AWS CloudTrail イベントをモニタリングでき AWS リージョン、グローバルサービスを含むアクティビティを検出する機能が低下します。

リージョン固有機能の可用性

GuardDuty 機能の可用性を指定するためのリージョン別相違点のリスト。

ListFindings および GetFindingsStatistics APIs

GetFindingsStatistics および ListFindings APIs には一時`consoleOnly`フラグがあります。これらの APIs、 `consoleOnly`フラグは、API が最大 1000 件まで結果を取得できることを意味します。

GuardDuty リージョン格差のある の機能

GuardDuty EC2 のマルウェア保護

GuardDuty は、AWS Dedicated Local Zones で EC2 の Malware Protection 機能をサポートしています。

一般的な API サポート

Amazon APIs リファレンスの次の GuardDuty API は、以前に指定した の一部のデータソースまたは機能が使用できないため、リージョンによって異なる場合があります AWS リージョン。

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors

- DescribeOrganizationConfiguration

Amazon EC2 検出結果 - DefenseEvasion:EC2/UnusualDoHActivity および DefenseEvasion:EC2/UnusualDoTActivity

次の表は、 GuardDuty が利用可能な AWS リージョン が、これら 2 つの Amazon EC2 検出結果タイプがまだサポートされていない を示しています。

AWS リージョン	リージョンコード
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (ジャカルタ)	ap-southeast-3

AWS GovCloud (US) リージョン

最新情報については、「 ユーザーガイド」の「Amazon GuardDutyAWS GovCloud (US) 」を参照してください。

中国リージョン

最新情報については、「機能の可用性と実装の違い」を参照してください。

GuardDuty レガシーアクションとパラメータ

Amazon GuardDuty は API アクションとパラメータの一部を廃止しましたが、引き続きサポートしています。従来のオプションに置き換わる新しい API アクションとパラメータを使用するのがベストプラクティスです。次の表では、従来のアクションとパラメータを、新しいアクションとパラメータと比較しています。

従来のアクション/パラメータ	新しいアクション/パラメータ	比較
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	両方のアクションで同じ実装では、 は Administrator の用語 GuardDuty を使用しますDisassociateFromAdministratorAccount 。
autoEnable DescribeOrganizationConfigurationおよびの パラメータ UpdateOrganizationConfiguration	autoEnableOrganizationMembers	を使用するとautoEnableOrganizationMembers 、GuardDuty 管理者アカウントはすべてのメンバーアカウント GuardDuty を監査し、いずれかの値に適用できます。API を使用すると、すべてのメンバーアカウントの設定を更新するのに最大 24 時間かかる場合があります。autoEnableOrganizationMembers フィールドの可能な値の詳細については、autoEnableOrganization「メンバー」を参照してください。
GuardDuty 2023 年 3 月の API の変更点 にリストされている API の dataSourc	features	2023 年 3 月以降、 を使用して Amazon での EC2 のマルウェア保護 GuardDutyと新しい GuardDuty 保護プランを設定できますfeatures。Malware Protection for EC2 を含む 2023 年 3 月より前に開始された保護プランは、引き続き

従来のアクション/パラメータ	新しいアクション/パラメータ	比較
es パラメータ。		を使用した設定をサポートしていますdataSources 。API を使用して保護プランを設定する場合、各 API リクエストには dataSources または features のいずれかを含めることができます。両方を含めることはできません。

Amazon のドキュメント履歴 GuardDuty

次の表は、Amazon GuardDuty ユーザーガイド の前回のリリース以降のドキュメントの重要な変更点を示しています。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。

変更	説明	日付
検出結果の GuardDuty テスタースクリプトを更新しました	GuardDuty は、専用アカウントで異なる AWS リソースを持つ 100 を超える検出結果をサポートするようになりました。 `amazon-guardduty-tester` リポジトリを使用し、手順に従って検出結果をテストし、確認して検出結果の詳細を理解します。詳細については、「専用アカウントで GuardDuty の検出結果のテスト」を参照してください。	2024 年 6 月 28 日
Runtime Monitoring の機能を更新しました	Runtime Monitoring は、Amazon EC2 リソース用の新しいセキュリティエージェントバージョン 1.2.0 をリリースしました。リリースノートの詳細については、GuardDuty Amazon EC2 インスタンスのセキュリティエージェント」を参照してください。セキュリティエージェントをこのリリースバージョンに手動で更新する方法については、Amazon EC2 インスタンスのセキュリティ	2024 年 6 月 13 日

	エージェントの手動管理」を参照してください。	
新機能 - Malware Protection for S3 Region Availability	GuardDuty Malware Protection for S3 が、 GuardDuty が利用可能なすべての商用リージョンで利用可能になりました。この機能は、新しく Amazon S3 バケットにアップロードされたオブジェクトをスキャンして潜在的なマルウェアや疑わしいアップロードがないか確認し、ダウンストリームプロセスに取り込まれる前にそれらを分離するアクションを実行するのに役立ちます。S3 の Malware Protection を有効にする方法については、「GuardDuty Malware Protection for S3」を参照してください。	2024 年 6 月 12 日

新機能 - Malware Protection for S3	GuardDuty は、Amazon S3 バケットにAmazon S3 の一般提供を発表しました。この機能は によって完全に管理されます AWS。 は S3 オブジェクトのスキャン結果を EventBridge デフォルトのイベントバスに GuardDuty 発行します。がスキャンした S3 オブジェクト GuardDuty にタグを追加することを許可できます。隔離バケットへの分離などのダウンストリームワークフローを構築したり、ユーザーやアプリケーションが特定のオブジェクトにアクセスできないようにタグを使用してバケットポリシーを定義したりできます。詳細については、「GuardDuty Malware Protection for S3」を参照してください。現在、次のリージョンで利用できます。 • 米国東部 (バージニア北部) • 米国東部 (オハイオ) • 米国西部 (オレゴン) • 欧州 (アイルランド) • 欧州 (フランクフルト) • 欧州 (ストックホルム) • アジアパシフィック (シドニー) • アジアパシフィック (東京) • アジアパシフィック (シンガポール)	2024 年 6 月 11 日

更新されたAmazonGuardDutyFullAccessポリシー	Malware Protection for S3 を有効にするときに IAM ロールを GuardDuty に渡すことができるアクセス許可を追加しました。このポリシーの更新の詳細については、「GuardDuty AWS 管理ポリシーの更新」を参照してください。	2024 年 6 月 10 日
GuardDuty RDS Protection の機能を更新しました	RDS Protection は、RDS for PostgreSQL データベースのログインアクティビティをモニタリングするためのサポートを拡張します。この拡張の一環として、 GuardDuty は RDS for PostgreSQL データベースから GuardDuty RDS Protection を既に有効にしているアカウントのログインデータのモニタリングを自動的に開始します。詳細については、「RDS Protection」を参照してください。	2024 年 6 月 6 日
GuardDuty Runtime Monitoring - Fargate の機能を更新 (Amazon ECS のみ)	Runtime Monitoring は、 AWS Fargate (Amazon ECS のみ) リソース用の新しいエージェントバージョン 1.2.0 をリリースしました。リリースノートの詳細については、GuardDuty 「Fargate-ECS のセキュリティエージェント」を参照してください。	2024 年 5 月 31 日

Malware Protection for EC2 GuardDuty の機能を更新しました	Amazon EC2 インスタンスとコンテナワークロードにアタッチされている各 Amazon EBS ボリュームについて、GuardDuty Malware Protection for EC2 はスキャンする EBS ボリュームのサイズを最大 2048 GB に増やしました。インスタンスにアタッチされた Amazon EBS ボリュームのスキャンについては、GuardDuty EC2 の Malware Protection」を参照してください。	2024 年 5 月 29 日
Runtime Monitoring の機能を更新しました	Amazon ECS-Fargate リソースのランタイムモニタリングで、 AWS Batch および によって起動されたタスクに対する潜在的な脅威の検出がサポートされるようになりました AWS CodePipeline。詳細については、「Runtime Monitoring が Fargate と連携する方法 (Amazon ECS のみ)」を参照してください。	2024 年 5 月 28 日
Runtime Monitoring の機能を更新しました	Runtime Monitoring は、Amazon EKS リソース用の新しいエージェントバージョン 1.6.1 をリリースしました。リリースノートの詳細については、「EKS アドオンエージェントのリリース履歴」を参照してください。	2024 年 5 月 14 日

Runtime Monitoring のリージョンサポートの拡張	GuardDuty は、Runtime Monitoring のサポートをカナダ西部 (カルガリー) リージョンに拡張しました。Runtime Monitoring の開始方法については、「Runtime Monitoring の有効化」を参照してください。	2024 年 5 月 7 日
RDS Protection のリージョンサポートの拡張	GuardDuty は、RDS Protection のサポートを次の に拡張します AWS リージョン。 • カナダ西部 (カルガリー) • アジアパシフィック (ハイデラバード) • 欧州 (スペイン) • 欧州 (チューリッヒ) • 中東 (アラブ首長国連邦) • イスラエル (テルアビブ) • アジアパシフィック (メルボルン) この機能を有効にする方法については、「RDS Protection」を参照してください。	2024 年 5 月 3 日

Runtime Monitoring の機能を更新しました	Runtime Monitoring は、 AWS Fargate (Amazon ECS のみ) リソース用の新しいエージェントバージョン 1.1.0 をリリースしました。リリースノートの詳細については、GuardDuty 「Fargate-ECS のセキュリティエージェント」を参照してください。	2024 年 5 月 1 日
Runtime Monitoring の機能を更新しました	Runtime Monitoring は、Amazon EKS リソース用の新しいエージェントバージョン 1.6.0 をリリースしました。リリースノートの詳細については、「EKS アドオンエージェントのリリース履歴」を参照してください。	2024 年 4 月 29 日
IPAddressv6 のサポート	GuardDuty は、ローカル IP の詳細とリモート IP の詳細の両方に対する IPAddressv6 サポートを追加しました。関連付けられたフィルター属性を使用して、結果をフィルタリング GuardDutyしたり、抑制ルール を作成したりできます。	2024 年 4 月 18 日
コンソールエクスペリエンスを更新して、結果のエクスポートを設定	GuardDuty はコンソールエクスペリエンスを更新して AWS アカウント、 で生成された結果を Amazon S3 バケットにエクスポートしました。詳細については、 GuardDuty 「検出結果のエクスポート」を参照してください。	2024 年 4 月 1 日

Runtime Monitoring の機能を更新しました	Runtime Monitoring は、Amazon EC2 リソース用の新しいセキュリティエージェントバージョン 1.1.0 をリリースしました。このバージョンでは、Amazon EC2 インスタンスのランタイムモニタリングで GuardDuty 自動エージェント設定がサポートされています。リリースノートの詳細については、GuardDuty Amazon EC2 インスタンスのセキュリティエージェント」を参照してください。	2024 年 3 月 28 日

Amazon EC2 インスタンスの Runtime Monitoring の一般提供	GuardDuty は、Amazon EC2 インスタンスの Runtime Monitoring の一般提供 (GA) を発表しました。これで、自動エージェント設定を有効にして GuardDuty 、 がユーザーに代わって Amazon EC2 インスタンスのセキュリティエージェントをインストールおよび管理できるようにできるようになりました。GuardDuty 自動エージェントでは、包含タグまたは除外タグを使用して、選択した Amazon EC2 インスタンスにのみセキュリティエージェントをインストールおよび管理 GuardDuty するように に通知することもできます。詳細については、「How Runtime Monitoring works with Amazon EC2 instances」を参照してください。 この GA と共にリリースされた新しい検出結果タイプのリスト • 実行：ランタイム/SuspiciousTool • 実行：ランタイム/SuspiciousCommand • DefenseEvasion：ランタイム/SuspiciousCommand • DefenseEvasion：ランタイム/PtraceAntiDebugging	2024 年 3 月 28 日

- 実行：ランタイム/Malicious FileExecuted

Amazon GuardDuty がサービスにリンクされたロール (SLR) を更新しました	Amazon EC2 の自動エージェントで Runtime Monitoring を有効にする場合は、 AWS Systems Manager アクションを使用して Amazon EC2 インスタンスの GuardDuty SSM 関連付けを管理します。GuardDuty 自動エージェント設定が無効になっている場合、包含タグ (`GuardDuty Managed ：true`) を持つ EC2 インスタンスのみ GuardDuty を考慮します。 • 次のリストは、新しいアクセス許可を示しています。 `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	2024 年 3 月 26 日

Runtime Monitoring の機能を更新しました	Amazon EKS 用の最新の GuardDuty セキュリティエージェント (アドオン) v1.5.0 リリースでは、Runtime Monitoring で、CPU とメモリの設定、`PriorityClass` 設定、DNS ポリシー設定など、GuardDuty セキュリティエージェントの特定のパラメータの設定がサポートされるようになりました。詳細については、「セキュリティエージェント (EKS アドオン) パラメータの設定 GuardDuty」を参照してください。	2024 年 3 月 7 日
Runtime Monitoring の機能を更新しました	Runtime Monitoring は、Amazon EKS リソース用の新しいエージェントバージョン 1.5.0 をリリースしました。リリースノートの詳細については、「EKS アドオンエージェントのリリース履歴」を参照してください。	2024 年 3 月 7 日
カナダ西部 (カルガリー) のサポート	Amazon GuardDuty がカナダ西部 (カルガリー) リージョンで利用可能になりました。内の一部の保護プラン GuardDuty は、このリージョンでは利用できない場合があります。最新情報については、「リージョンとエンドポイント」を参照してください。	2024 年 3 月 6 日

Runtime Monitoring の機能を更新しました	Amazon EKS クラスター GuardDuty のセキュリティエージェントバージョン 1.0.0 および 1.1.0 は、2024 年 5 月 14 日以降サポートされなくなります。標準サポートが終了する前に実行できる手順については、GuardDuty「Amazon EKS クラスターのセキュリティエージェント」を参照してください。	2024 年 2 月 16 日
Runtime Monitoring の機能を更新しました	Runtime Monitoring は、既存のセキュリティエージェントバージョン 1.4.1 で最新の Kubernetes バージョン 1.29 をサポートしています。このサポートは、この Kubernetes バージョンのリリース以降、利用可能です。サポートされている Kubernetes バージョンの詳細については、GuardDuty「セキュリティエージェント でサポートされている Kubernetes バージョン」を参照してください。	2024 年 2 月 16 日

Runtime Monitoring の更新された機能 - リージョンの可用性	GuardDuty Runtime Monitoring は、同じ 内の共有 Amazon VPC をサポートするようになりました AWS Organizations。GuardDuty サービスにリンクされたロール (SLR) には新しいアクセス許可があります。`organizations:DescribeOrganization` これにより、共有 Amazon VPC アカウントの組織 ID を取得してエンドポイントポリシーを設定できます。Runtime Monitoring で共有 Amazon VPC エンドポイントを使用するための前提条件については、「共有 Amazon VPC のサポート」を参照してください。この機能は、 が Runtime Monitoring GuardDuty をサポートしているすべてのリージョンで使用できます。	2024 年 2 月 12 日

Runtime Monitoring の更新された機能 - リージョンの可用性	GuardDuty Runtime Monitoring は、同じ 内の共有 Amazon VPC をサポートするようになりました AWS Organizations。GuardDuty サービスにリンクされたロール (SLR) には新しいアクセス許可があります。`organizations:DescribeOrganization` これにより、共有 Amazon VPC アカウントの組織 ID を取得してエンドポイントポリシーを設定できます。Runtime Monitoring で共有 Amazon VPC エンドポイントを使用するための前提条件については、「共有 Amazon VPC のサポート」を参照してください。現在、この機能はの一部で利用できます AWS リージョン。詳細については、「 リージョンとエンドポイント」を参照してください。	2024 年 2 月 9 日
新しい のサポートで機能を更新 – EC2 AWS リージョン の Malware Protection	Malware Protection for EC2 は、米国西部 (オレゴン) リージョン AWS マネージドキーで で暗号化された EBS ボリュームのスキャンをサポートするようになりました。	2024 年 2 月 6 日

新しい のサポートで機能を更新 – EC2 AWS リージョン の Malware Protection	Malware Protection for EC2 は、次の AWS マネージドキー で で暗号化された EBS ボリュームのスキャンをサポートするようになりましたAWS リージョン。 • アジアパシフィック (シンガポール) (ap-southeast-1) • 欧州 (フランクフルト) (eu-central-1) • アジアパシフィック (大阪) (ap-northeast-3) • 米国東部 (オハイオ) (us-east-2) • 欧州 (ミラノ) (eu-south-1) • アジアパシフィック (東京) (ap-northeast-1) • アジアパシフィック (ソウル) (ap-northeast-2) • カナダ (中部) (ca-central-1) • 欧州 (アイルランド) (eu-west-1) • 米国東部 (バージニア北部) (us-east-1)	2024 年 2 月 5 日

Runtime Monitoring の機能を更新しました	GuardDuty Runtime Monitoring は、Amazon EC2 インスタンス用の新しい GuardDuty セキュリティエージェントバージョン (v1.0.2) をリリースしました。このエージェントバージョンには、最新の Amazon ECS AMIsのサポートが含まれています。エージェントリリース履歴の詳細については、GuardDuty Amazon EC2 インスタンスのセキュリティエージェント」を参照してください。	2024 年 2 月 21 日

新しい のサポートで機能を更新 – EC2 AWS リージョン の Malware Protection	Malware Protection for EC2 は、次の で で暗号化された Amazon EBS ボリューム AWS マネージドキー のスキャンをサポートするようになりました AWS リージョン。 • 欧州 (ロンドン) (eu-west-2) • 欧州 (ストックホルム) (eu-north-1) • アジアパシフィック (香港) (ap-east-1) • アフリカ (ケープタウン) (af-south-1) • 中東 (バーレーン) (me-south-1) • アジアパシフィック (ハイデラバード) (ap-south-2) • 欧州 (スペイン) (eu-south-2) • アジアパシフィック (メルボルン) (ap-southeast-4) • アジアパシフィック (シドニー) (ap-southeast-2) • イスラエル (テルアビブ) (il-central-1)	2024 年 1 月 31 日

でアカウントの管理を更新 AWS Organizations	「でアカウントを管理する」のコンテンツを再編成し AWS Organizations、委任された GuardDuty 管理者アカウントを変更する手順を追加し、GuardDuty 「管理者アカウントとメンバーアカウントとの関係について」を更新しました。	2024 年 1 月 30 日
新しい をサポートするように機能を更新しました AWS リージョン	Malware Protection for EC2 は、次の AWS マネージドキー で で暗号化された EBS ボリュームのスキャンをサポートするようになりました AWS リージョン。 • アジアパシフィック (ジャカルタ) (ap-southeast-3) • 米国西部 (北カリフォルニア) (us-west-1) • 中東 (アラブ首長国連邦) (me-central-1) • 欧州 (チューリッヒ) (eu-central-2) • アジアパシフィック (ムンバイ) (ap-south-1) • 南米 (サンパウロ) (sa-east-1)	2024 年 1 月 29 日

Malware Protection for EC2 の機能を更新しました	Malware Protection for EC2 で、 を使用して暗号化された EBS ボリュームのスキャンがサポートされるようになりました AWS マネージドキー。Malware Protection for EC2 サービスにリンクされたロール (SLR) には、`GetSnapshotBlock` との 2 つの新しいアクセス許可がありますListSnapshotBlocks 。これらのアクセス許可は、 から EBS ボリュームのスナップショット (を使用して暗号化 AWS マネージドキー) GuardDuty を取得し AWS アカウント 、マルウェアスキャンを開始する前にGuardDuty サービスアカウントにコピーするのに役立ちます。現在、この機能は欧州 (パリ) (`eu-west-3`) でのみ利用できます。詳細については、「マルウェアスキャンでサポートされているボリューム」を参照してください。	2024 年 1 月 25 日

Runtime Monitoring の機能を更新しました	GuardDuty Runtime Monitoring は、一般的なパフォーマンスのチューニングと機能強化機能を備えた新しい GuardDuty セキュリティエージェントバージョン (v1.0.1) をリリースしました。エージェントリリース履歴の詳細については、GuardDuty Amazon EC2 インスタンスのセキュリティエージェント」を参照してください。	2024 年 1 月 23 日
Runtime Monitoring の機能を更新しました	Runtime Monitoring は、Amazon EKS リソース用の新しいエージェントバージョン 1.4.1 をリリースしました。詳細については、「EKS アドオンエージェントのリリース履歴」を参照してください。	2024 年 1 月 16 日
Runtime Monitoring が Amazon EKS リソース用の新しいエージェント v1.4.0 をリリース	Runtime Monitoring は、Amazon EKS リソース用の新しいエージェントバージョン 1.4.0 をリリースしました。詳細については、「EKS アドオンエージェントのリリース履歴」を参照してください。	2023 年 12 月 21 日

欧州 (チューリッヒ) 、欧州 (スペイン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (メルボルン) 、イスラエル (テルアビブ) に S3 および AWS CloudTrail 機械学習 (ML) ベースの検出結果タイプを追加しました。	GuardDutyの異常検出機械学習 (ML) モデルを使用して異常な動作を特定する次の S3 および CloudTrail 検出結果は、欧州 (チューリッヒ) 、欧州 (スペイン) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (メルボルン) 、イスラエル (テルアビブ) の各リージョンで利用可能になりました。 • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	2023 年 12 月 21 日

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty は、 を通じて 50,000 のメンバーアカウントをサポートします。 AWS Organizations	委任 GuardDuty 管理者は、 を通じて最大 50,000 のメンバーアカウントを管理できるようになりました AWS Organizations。これには、招待によって GuardDuty 管理者アカウントに関連付けられた最大 5000 のメンバーアカウントも含まれます。	2023 年 12 月 20 日
GuardDuty Runtime Monitoring のサポートが 19 に拡張されました AWS リージョン	Runtime Monitoring が利用可能な地域は次の通りです: アジアパシフィック (ジャカルタ)、欧州 (パリ)、アジアパシフィック (大阪)、アジアパシフィック (ソウル)、中東 (バーレーン)、欧州 (スペイン)、アジアパシフィック (ハイデラバード)、アジアパシフィック (メルボルン)、イスラエル (テルアビブ)、米国西部 (北カリフォルニア)、欧州 (ロンドン)、アジアパシフィック (香港)、欧州 (ミラノ)、中東 (UAE)、南米 (サンパウロ)、アジアパシフィック (ムンバイ)、カナダ (中部)、アフリカ (ケープタウン)、欧州 (チューリッヒ)。	2023 年 12 月 6 日

GuardDuty が Runtime Monitoring 機能を拡張	Amazon EKS クラスターへの脅威を検出するだけでなく、 は、Amazon ECS ワークロードへの脅威を検出する Runtime Monitoring の一般提供と、Amazon EC2 インスタンスへの脅威を検出するプレビューリリース GuardDuty を発表しました。現在 Runtime Monitoring がサポートされている AWS リージョン の詳細については、「リージョンとエンドポイント」をご確認ください。	2023 年 11 月 26 日

Amazon GuardDuty がサービスにリンクされたロール (SLR) を更新しました	GuardDuty は、Amazon ECS アクションを使用して Amazon ECS クラスターに関する情報を管理および取得し、 で Amazon ECS アカウント設定を管理するための新しいアクセス許可を追加しましたguardduty Activate 。Amazon ECS に関連するアクションは、 に関連付けられたタグに関する情報も取得します GuardDuty。 • Runtime Monitoring 機能の GuardDuty 拡張の一環として、次のアクセス許可が追加されました。 `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	2023 年 11 月 26 日
AWS 管理ポリシーを更新しました	GuardDuty は、 AmazonGuardDutyFullAccessPolicyと organizations:ListAccounts に新しいアクセス許可を追加しましたAmazonGuardDutyReadOnlyAccess。	2023 年 11 月 16 日

GuardDuty は、EKS 監査ログのモニタリングを使用する新しい検出結果タイプをリリースしました。	EKS 監査ログモニタリングでは、アジアパシフィック (メルボルン) (`ap-southeast-4`) で以下の検出結果タイプがサポートされるようになりました。 • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	2023 年 11 月 11 日

GuardDuty は、EKS 監査ログのモニタリングを使用する新しい検出結果タイプをリリースしました。	EKS 監査ログモニタリングでは、アジアパシフィック (ハイデラバード) (ap-south-2)、欧州 (チューリッヒ) (eu-central-2)、欧州 (スペイン) (eu-south-2)で以下の検出結果タイプがサポートされるようになりました。 • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	2023 年 11 月 10 日

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty は、EKS 監査ログのモニタリングを使用する新しい検出結果タイプをリリースしました。	EKS 監査ログモニタリングでは、以下の検出結果タイプがサポートされるようになりました。次の検出結果タイプは、アジアパシフィック (ハイデラバード) (`ap-south-2`)、欧州 (チューリッヒ) (`eu-central-2`)、欧州 (スペイン) (`eu-south-2`)、アジアパシフィック (メルボルン)(`ap-southeast-4`)では現在ご利用いただけません。 • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	2023 年 11 月 8 日

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKS Runtime Monitoring が新しいエージェント v1.3.1 をリリース	EKS Runtime Monitoring が重要なセキュリティパッチと更新を含む新しいエージェントバージョン 1.3.1 をリリースしました。	2023 年 10 月 23 日
検出結果の新しいフィルター属性	GuardDuty は、生成された結果をフィルタリングするための新しい基準を追加しました。DNS リクエストドメインのサフィックスは、検出結果の生成 GuardDuty を促したアクティビティに関係する 2 番目と最上位のドメインを提供します。	2023 年 10 月 17 日
EKS Runtime Monitoring が Kubernetes バージョン 1.28 をサポートする新しいエージェント v1.3.0 をリリース	EKS Runtime Monitoring が、Kubernetes バージョン 1.28 をサポートする新しいエージェントバージョン 1.3.0 をリリースしました。Ubuntu のサポートを追加しました。詳細については、「EKS アドオンエージェントのリリース履歴」を参照してください。	2023 年 10 月 5 日

アジアパシフィック (ジャカルタ) および中東 (アラブ首長国連邦) リージョンに S3 および AWS CloudTrail 機械学習 (ML) ベースの検出結果タイプを追加	の異常検出機械学習 (ML) モデルを使用して異常な動作を特定する次の S3 と CloudTrail 検出 GuardDuty結果は、アジアパシフィック (ジャカルタ) および中東 (アラブ首長国連邦) リージョンで利用可能になりました。 • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior	2023 年 9 月 20 日

	• Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKS Runtime Monitoring でクラスターレベルで GuardDuty のセキュリティエージェントの管理を導入	EKS Runtime Monitoring は、個々の EKS クラスター GuardDuty のセキュリティエージェントを管理し、これらの選択的なクラスターのみからのランタイムイベントをモニタリングするサポートを追加します。EKS Runtime Monitoring は、タグのサポートによりこの機能を拡張します。	2023 年 9 月 13 日
GuardDuty Malware Protection for EC2 のサポートを延長 AWS リージョン	Malware Protection for EC2 が、アジアパシフィック (ハイデラバード)、アジアパシフィック (メルボルン)、欧州 (チューリッヒ)、欧州 (スペイン) で利用可能になりました。	2023 年 9 月 11 日

GuardDuty がイスラエル (テルアビブ) リージョンで利用可能に	イスラエル (テルアビブ) リージョンを、 AWS リージョン GuardDuty が利用可能になった のリストに追加しました。イスラエル (テルアビブ) リージョンでは、次の保護プランも利用できます。 • GuardDuty EKS 保護 には、EKS 監査ログのモニタリングと EKS ランタイムモニタリングの両方が含まれます。 • GuardDuty Lambda 保護. • GuardDuty EC2 のマルウェア保護. • GuardDuty S3 保護. イスラエル (テルアビブ) リージョンで利用可能な保護プランの詳細については、「リージョンとエンドポイント」を参照してください。	2023 年 8 月 24 日
GuardDuty が保護プランレベルで組織の自動有効化設定を追加しました	リージョンの保護プランの組織設定を更新します。可能な設定オプションは、すべてのアカウントのために有効にする、新しいアカウントのために自動的に有効にする、組織内のいずれのアカウントのためにも自動的に有効にしない、のいずれかです。	2023 年 8 月 16 日

の異常検出機械学習 (ML) モデルを使用して異常な動作を識別する S3 GuardDuty検出結果タイプが、アジアパシフィック (大阪) で利用可能になりました	次の検出結果タイプがアジアパシフィック (大阪) リージョンで利用できるようになりました。 • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	2023 年 8 月 10 日
EKS ランタイムモニタリングがアジアパシフィック (メルボルン) で利用可能に	EKS Protection 内の GuardDuty EKS Runtime Monitoring は、 AWS 環境内の Amazon EKS クラスターのランタイム脅威検出を提供します。現在、アジアパシフィック (メルボルン) リージョンでサポートされています。	2023 年 8 月 8 日
GuardDuty実行型マルウェアスキャンを呼び出す GuardDuty 検出結果のリストを更新しました。	一部の EKS Runtime Monitoring の検出結果タイプでは、 で GuardDuty実行型マルウェアスキャンを呼び出すことができるようになりました AWS アカウント。	2023 年 7 月 19 日

GuardDuty は、 を通じて 10,000 のメンバーアカウントをサポートします。 AWS Organizations	GuardDuty 管理者アカウントは、 を通じて最大 10,000 個のメンバーアカウントを管理できるようになりました AWS Organizations。これには、招待によって管理者アカウントに関連付けられた最大 5000 GuardDutyのメンバーアカウントも含まれます。	2023 年 6 月 29 日
EKS Runtime Monitoring が 3 つの新しい検出結果タイプを発表	EKS Runtime Monitoring は、プロセスインジェクション技術に基づく 3 つの新しい検出結果タイプをサポートしています。新しい検出結果タイプは DefenseEvasion:Runtime/ですProcessInjection。Proc、DefenseEvasion:Runtime/ProcessInjection。Ptrace、および DefenseEvasion:Runtime/ProcessInjectionVirtualMemoryWrite.	2023 年 6 月 22 日
EKS Runtime Monitoring が Kubernetes バージョン 1.27 をサポートする新しいエージェント v1.2.0 をリリース	EKS Runtime Monitoring が、ARM64 ベースのインスタンスもサポートする新しいエージェントバージョン 1.2.0 をリリースしました。Bottlerocket のサポートが追加されました。詳細については、「EKS アドオンエージェントのリリース履歴」を参照してください。	2023 年 6 月 16 日

GuardDuty コンソールには、検出結果の概要が表示されます。	GuardDuty コンソールのサマリーダッシュボードには、検出結果の集計ビューが表示されます GuardDuty。現在、ダッシュボードには、現在のリージョンのアカウント (または GuardDuty 管理者アカウントの場合はメンバーアカウント) に対して生成された過去 10,000 件の検出結果のデータがさまざまなウィジェットに表示されます。	2023 年 6 月 12 日
EKS Audit Log Monitoring は現在、アジアパシフィック (ハイデラバード)、アジアパシフィック (メルボルン)、欧州 (チューリッヒ) および欧州 (スペイン)リージョンでご利用可能	アカウントの EKS 監査ログのモニタリング (EKS Protection 内) を有効にして、Amazon EKS クラスターからの EKS 監査ログをモニタリングし、潜在的に悪意のあるアクティビティや疑わしいアクティビティがないか分析します。	2023 年 6 月 1 日
EKS 監査ログのモニタリングが中東 (UAE) で利用可能になりました	EKS 監査ログのモニタリングが中東 (UAE) で利用可能になりました。アカウントの EKS 監査ログのモニタリングを有効にして、Amazon EKS クラスターからの EKS 監査ログをモニタリングし、潜在的に悪意のあるアクティビティや疑わしいアクティビティがないか分析します。	2023 年 5 月 3 日

GuardDuty Malware Protection for EC2 がオンデマンドのマルウェアスキャンを発表	Malware Protection for EC2 は、Amazon EC2 インスタンスとコンテナワークロードにアタッチされた Amazon EBS ボリュームにマルウェアが存在する可能性を検出するのに役立ちます。 GuardDuty 開始スキャンとオンデマンドスキャンの 2 種類のスキャンが提供されるようになりました。 GuardDuty開始マルウェアスキャンは、 が開始マルウェアスキャン を呼び出す検出結果の 1 つ GuardDuty を生成する場合にのみ、Amazon EBS ボリュームでエージェントレススキャンを自動的に開始します。 GuardDuty Amazon EC2 インスタンスに関連付けられた Amazon リソースネーム (ARN) を指定することで、アカウントの Amazon EC2 インスタンスのオンデマンドマルウェアスキャンを開始できます。両方のスキャンタイプの違いの詳細については、EC2 の Malware Protection」を参照してください。 • GuardDutyが開始するマルウェアスキャン • オンデマンドのマルウェアスキャン	2023 年 4 月 27 日

GuardDuty Lambda Protection を発表	Lambda Protection は、 AWS Lambda 関数の潜在的なセキュリティ脅威を特定するのに役立ちます。 • Lambda Protection の検出結果タイプ • 侵害された可能性のある Lambda 関数の修復	2023 年 4 月 20 日
GuardDuty がアジアパシフィック (メルボルン) リージョンで利用可能に	GuardDuty が利用可能な のリストにアジアパシフィック (メルボルン) を追加 AWS リージョン しました。このリージョンで利用可能な機能については、「リージョンとエンドポイント」を参照してください。	2023 年 4 月 19 日
GuardDuty に 3 つの新しい EC2 検出結果タイプを追加	GuardDuty では、外部 DNS リゾルバーと暗号化された DNS テクノロジーの使用を検出するための新しい検出結果タイプが導入されました。これらの検出結果タイプがサポートされている AWS リージョン 場所については、「リージョンとエンドポイント」を参照してください。 • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	2023 年 4 月 5 日

GuardDuty が EKS Protection での EKS Runtime Monitoring を発表	EKS Protection 内の EKS Runtime Monitoring は、 AWS 環境内の Amazon EKS クラスターのランタイム脅威検出を提供します。Amazon EKS アドオンエージェント (`aws-guardduty-agent`) を使用して、EKS ワークロードからランタイムイベントを収集します。 GuardDuty は、これらのランタイムイベントを受信した後、それらをモニタリングおよび分析して、疑わしい潜在的なセキュリティ脅威を特定します。詳細については、「検出結果の詳細」と「EKS Runtime Monitoring の検出結果タイプ」を参照してください。	2023 年 3 月 30 日

GuardDuty が新機能を追加 – autoEnableOrganizationMembers	Amazon は、 GuardDuty 管理者アカウントが組織のメンバーに対して有効 GuardDuty になっている (必要な場合) ALL を監査および強制するのに役立つ新しい組織設定オプション GuardDuty を追加します。現在のベストプラクティスは、autoEnable の代わりに autoEnableOrganizationMembers を使用することです。autoEnable は非推奨ですが、まだサポートされています。次の API はこの新機能の影響を受けます。 • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	2023 年 3 月 23 日

Amazon の RDS Protection GuardDuty 機能が一般利用可能になりました	GuardDuty RDS Protection は、RDS ログインアクティビティをモニタリングおよびプロファイリングして、Amazon Aurora データベースインスタンスでの疑わしいログイン動作を特定します。RDS Protection をサポートする AWS リージョン については、「リージョンとエンドポイント」を参照してください。	2023 年 3 月 16 日
GuardDuty が機能のアクティベーションを発表	これまで、 GuardDuty API では機能とデータソースの両方の設定が許可されていましたが、現在では、すべての新しい GuardDuty 保護タイプがデータソースとしてではなく機能として設定されます。 GuardDuty は API 経由でデータソースをサポートしますが、新しい API は追加されません。機能のアクティベーションは、 GuardDuty または 内の保護タイプを有効にするために使用される APIs の動作に影響します GuardDuty。API、SDK、または CFN テンプレートを使用して GuardDuty アカウントを管理する場合は、GuardDuty 2023 年 3 月の API の変更を参照してください。	2023 年 3 月 16 日

GuardDuty Malware Protection for EC2 が中東 (UAE) リージョンで利用可能に	の Malware Protection for EC2 機能は GuardDuty 、中東 (UAE) リージョンでサポートされています。詳細については、「リージョンとエンドポイント」を参照してください。	2023 年 3 月 13 日
Amazon GuardDuty がサービスにリンクされたロール (SLR) を更新しました	GuardDuty は、今後の GuardDuty EKS Runtime Monitoring 機能をサポートするために、次の新しいアクセス許可を追加しました。 • Amazon EKS アクションを使用して、EKS クラスターに関する情報を管理および取得し、EKS クラスター上の EKS アドオンを管理します。EKS アクションは、 に関連付けられたタグに関する情報も取得します GuardDuty。 `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	2023 年 3 月 8 日

Amazon GuardDuty がサービスにリンクされたロール (SLR) を更新しました	GuardDuty SLR が更新され、EC2 の Malware Protection が有効になった後にEC2 SLR の Malware Protection を作成できるようになりました。	2023 年 2 月 21 日
GuardDuty には TLS v1.2 以降が必要です	AWS リソースと通信するために、 は TLS v1.2 以降 GuardDuty を必要とし、サポートしています。詳細については、「データの保護」および「インフラストラクチャのセキュリティ」を参照してください。	2023 年 2 月 14 日
GuardDuty がアジアパシフィック (ハイデラバード) リージョンで利用可能に	GuardDuty が利用可能な のリストにアジアパシフィック (ハイデラバード) リージョンを追加 AWS リージョン しました。詳細については、「リージョンとエンドポイント」を参照してください。	2023 年 2 月 14 日
Amazon GuardDuty ユーザーガイドは IAM のベストプラクティスに沿ったものです	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM 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。	2023 年 2 月 10 日
GuardDuty が欧州 (スペイン) リージョンで利用可能に	が利用可能な のリストに欧州 (スペイン) GuardDuty を追加 AWS リージョン しました。詳細については、「リージョンとエンドポイント」を参照してください。	2023 年 2 月 8 日

GuardDuty が欧州 (チューリッヒ) リージョンで利用可能に	が利用可能な のリストに欧州 (チューリッヒ) GuardDuty を追加 AWS リージョン しました。詳細については、「リージョンとエンドポイント」を参照してください。	2022 年 12 月 12 日
新機能のプレビューリリース – GuardDuty RDS Protection	GuardDuty RDS Protection は、RDS ログインアクティビティをモニタリングおよびプロファイリングして、Amazon Aurora データベースインスタンスでの疑わしいログイン動作を特定します。現在、5 つの AWS リージョンでプレビューリリースを利用できます。詳細については、「リージョンとエンドポイント」を参照してください。	2022 年 11 月 30 日
GuardDuty が中東 (アラブ首長国連邦) リージョンで利用可能になりました	が利用可能な のリストに中東 (UAE) GuardDuty を追加 AWS リージョン しました。詳細については、「リージョンとエンドポイント」を参照してください。	2022 年 10 月 6 日

新機能のコンテンツを追加 – EC2 の GuardDuty マルウェア保護	GuardDuty EC2 の Malware Protection は、Amazon に対するオプションの強化です GuardDuty。はリスクのあるリソース GuardDuty を識別しますが、Malware Protection for EC2 は、侵害の原因である可能性のあるマルウェアを検出します。Malware Protection for EC2 を有効にすると、が Amazon EC2 インスタンスまたはマルウェアを示すコンテナワークロードで疑わしい動作 GuardDuty を検出するたびに、 GuardDuty Malware Protection for EC2 は、影響を受けた EC2 インスタンスまたはコンテナワークロードにアタッチされた EBS ボリュームでエージェントレススキャンを開始してマルウェアの存在を検出します。Malware Protection for EC2 の仕組みとこの機能の設定については、GuardDuty 「Malware Protection for EC2」を参照してください。 • EC2 検出結果の Malware Protection の詳細については、「検出結果の詳細」を参照してください。 • 侵害された EC2 インスタンスとスタンドアロンコンテナの修復については、「 によって検出されたセキュリ	2022 年 7 月 26 日

	ティ問題の修復 GuardDuty」を参照してください。 • マルウェアスキャンの CloudWatch ログの監査と、マルウェアスキャン中にリソースをスキップする理由については、CloudWatch「ログの理解とスキップの理由」を参照してください。 • 誤検出の脅威検出の詳細については、EC2 の GuardDuty Malware Protection での誤検出の報告」を参照してください。	
廃止された検出結果のタイプの 1 つ	Exfiltration:S3/ObjectRead.Unusual は廃止されました。	2022 年 7 月 5 日

の異常検出機械学習 (ML) モデルを使用して異常な動作を識別する新しい GuardDutyS3 検出結果タイプを追加しました。	次の新しい S3 の検出結果タイプを追加しました。これらの検出結果タイプでは、API リクエストが IAM エンティティを異常な方法で呼び出したかどうかを識別します。機械学習モデルは、アカウント内のすべての API リクエストを評価し、攻撃者が使用するテクニックに関連する異常なイベントを特定します。これらの新しい検出結果の詳細については、「S3 の検出結果タイプ」を参照してください。 • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	2022 年 7 月 5 日

の GuardDuty EKS Protection コンテンツを追加 GuardDuty	GuardDuty は、EKS 監査ログのモニタリングを通じて Amazon EKS リソースの検出結果を生成できるようになりました。この機能を設定する方法については、「Amazon での EKS Protection GuardDuty」を参照してください。Amazon EKS リソースに対して生成 GuardDuty できる検出結果のリストについては、「Kubernetes の検出結果」を参照してください。「Kubernetes の検出結果の修復ガイド」でこれらの検出結果の修復をサポートするために、新しい修復ガイダンスが追加されました。	2022 年 1 月 25 日
1 つの新しい検出結果が追加されました	新しい検出結果 UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS が追加されました。この検出結果は、インスタンス認証情報が AWS 環境外の AWS アカウントによってアクセスされたときに通知します。	2022 年 1 月 20 日

log4j に関連する問題の特定に役立つ検出結果タイプを更新しました	Amazon GuardDuty では、CVE-2021-44228 および CVE-2021-45046: Backdoor:EC2/C&CActivity.B; Backdoor:EC2/C&CActivity.B!DNS; Behavior:EC2/ に関連する問題を特定し、優先順位を付けるのに役立つように、次の検出結果タイプを更新しました NetworkPortUnusual。	2021 年 12 月 22 日
検出結果の変更	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration は UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS に変更されました。この検出結果の改善バージョンでは、オンプレミスネットワークでの送信済みトラフィックの検出結果を減らすため、認証情報を使用する典型的な場所を学習します。UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	2021 年 9 月 7 日
GuardDuty SLR の更新	GuardDuty SLR が新しいアクションで更新され、検出結果の精度が向上しました。	2021 年 8 月 3 日
各検出結果タイプのデータソース情報が追加されました。	検出結果の説明に、 がその検出結果を生成するために GuardDuty 使用するデータソースに関する情報が含まれるようになりました。	2021 年 5 月 10 日

廃止された 13 の検出結果タイプ	13 件の検出結果が廃止され、新しい Anomalous Behavoir 検出結果に置き換えられました。Persistence:IAMUser/NetworkPermissions、Persistence:IAMUser/ResourcePermissionsPersistence:IAMUser/UserPermissionsPrivilegeEscalation:IAMUser/AdministrativePermissions、、、Recon:IAMUser/NetworkPermissions、Recon:IAMUser/ResourcePermissions、Recon:IAMUser/UserPermissions、ResourceConsumption:IAMUser/ComputeResourcesStealth:IAMUser/LoggingConfigurationModified、、Discovery:S3/BucketEnumeration.UnusualImpact:S3/ObjectDelete.Unusual、Impact:S3/PermissionsModification.Unusual。	2021 年 3 月 12 日

異常動作の 8 つの新しい検出結果タイプが追加されました。	IAM プリンシパルの異常動作に基づいて 8 つの新しい IAMUser 検出結果タイプが追加されました (CredentialAccess:IAMUser/AnomalousBehavior、DefenseEvasion:IAMUser/AnomalousBehavior、Discovery:IAMUser/AnomalousBehavior、Exfiltration:IAMUser/AnomalousBehavior、Impact:IAMUser/AnomalousBehavior、InitialAccess:IAMUser/AnomalousBehavior、Persistence:IAMUser/AnomalousBehavior、PrivilegeEscalation:IAMUser/AnomalousBehavior)。	2021 年 3 月 12 日
ドメインの評判に基づく EC2 の検出結果が追加されました。	ドメインの評判に基づく、新しい 4 つのインパクト検出結果タイプが追加されました。Impact:EC2/AbusedDomainRequest.Reputation 、Impact:EC2/BitcoinDomainRequest.Reputation、Impact:EC2/MaliciousDomainRequest.Reputation。また、新しい C&CAtivity の EC2 検出結果を追加しました。Impact:EC2/SuspiciousDomainRequest.Reputation	2021 年 1 月 27 日

4 つの新しい検出結果タイプが追加されました。	新しく 3 つの S3 Malicious IPCaller の検出結果が追加されました。Discovery:S3/MaliciousIPCaller、Exfiltration:S3/MaliciousIPCaller、Impact:S3/MaliciousIPCaller。また、新しい C&CAtivity の EC2 検出結果を追加しました。Backdoor:EC2/C&CActivity.B	2020 年 12 月 21 日
UnauthorizedAccess:EC2/TorIPCaller 検出結果タイプは廃止されました。	UnauthorizedAccess:EC2/TorIPCaller 検出結果タイプは から廃止されました GuardDuty。詳細はこちら。	2020 年 10 月 1 日
Impact:EC2/WinRmBruteForce 検出結果タイプが追加されました。	新しい Impact 検出結果 Impact:EC2/WinRmBruteForce が追加されました。詳細はこちら。	2020 年 9 月 17 日
Impact:EC2/PortSweep 検出結果タイプが追加されました。	新しい Impact 検出結果 Impact:EC2/PortSweep が追加されました。詳細はこちら。	2020 年 9 月 17 日
GuardDuty がアフリカ (ケープタウン) および欧州 (ミラノ) リージョンで利用可能になりました。	が利用可能な AWS リージョンのリストにアフリカ (ケープタウン) と欧州 (ミラノ) GuardDuty を追加しました。詳細はこちら	2020 年 7 月 31 日

GuardDuty コストをモニタリングするための新しい使用状況の詳細を追加しました。	新しいメトリクスを使用して、管理しているアカウントとアカウント GuardDuty の使用コストデータをクエリできるようになりました。使用コストの新しい概要は、https://console.aws.amazon.com/guardduty/ のコンソールで入手できます。詳細な情報には API からアクセスできます。	2020 年 7 月 31 日
の S3 データイベントモニタリングによる S3 保護に関するコンテンツを追加しました GuardDuty。	GuardDuty S3 Protection は、新しいデータソースとして S3 データプレーンイベントをモニタリングすることで利用できるようになりました。新しいアカウントでは、この機能が自動的に有効になります。既に GuardDuty を使用している場合は、自分またはメンバーアカウントで新しいデータソースを有効にできます。	2020 年 7 月 31 日
14 の新しい S3 検出結果が追加されました。	S3 コントロールプレーンとデータプレーンのソースに、14 の新しい S3 検出結果タイプが追加されました。	2020 年 7 月 31 日

S3 検出結果のサポートを追加し、2 つの既存の検出結果タイプ名を変更しました。	GuardDuty 検出結果には、S3 バケットに関連する検出結果の詳細が含まれるようになりました。S3 アクティビティに関連する既存の検出結果タイプの名前が変更されました。Policy:IAMUser/S3BlockPublicAccessDisabled は Policy:S3/BucketBlockPublicAccessDisabled に変更されました。Stealth:IAMUser/S3ServerAccessLoggingDisabled は Stealth:S3/ServerAccessLoggingDisabled に変更されました。	2020 年 5 月 28 日
AWS Organizations 統合のコンテンツを追加しました。	GuardDuty が AWS Organizations 委任された管理者と統合され、組織内の GuardDuty アカウントを管理できるようになりました。委任された管理者を GuardDuty 管理者アカウントとして設定すると、組織メンバー GuardDuty を委任された管理者アカウントで管理できるように を自動的に有効にできます。新しい AWS Organizations メンバーアカウント GuardDuty で を自動的に有効にすることもできます。詳細はこちら。	2020 年 4 月 20 日
エクスポート検出結果機能のコンテンツが追加されました。	の検出結果のエクスポート機能を説明するコンテンツを追加しました GuardDuty。	2019 年 11 月 14 日

UnauthorizedAccess:EC2/MetadataDNSRebind 検出結果タイプが追加されました。	新しい Unauthorized 検出結果 UnauthorizedAccess:EC2/MetadataDNSRebind が追加されました。詳細はこちら。	2019 年 10 月 10 日
Stealth:IAMUser/S3ServerAccessLoggingDisabled 検出結果タイプが追加されました。	新しい Stealth 検出結果 Stealth:IAMUser/S3ServerAccessLoggingDisabled が追加されました。詳細はこちら。	2019 年 10 月 10 日
Policy:IAMUser/S3BlockPublicAccessDisabled 検出結果タイプが追加されました。	新しい Policy 検出結果 Policy:IAMUser/S3BlockPublicAccessDisabled が追加されました。詳細はこちら。	2019 年 10 月 10 日
Backdoor:EC2/XORDDOS 検出結果タイプは廃止されました。	Backdoor:EC2/XORDDOS 検出結果タイプは から廃止されました GuardDuty。詳細はこちら	2019 年 6 月 12 日
PrivilegeEscalation 検出結果タイプが追加されました。	PrivilegeEscalation 検出結果タイプでは、ユーザーが自分のアカウントの権限を昇格して過剰な特権を割り当てようした場合に検出されます。詳細はこちら	2019 年 5 月 14 日
GuardDuty が欧州 (ストックホルム) リージョンで利用可能になりました。	が利用可能な AWS リージョンのリストに欧州 (ストックホルム) GuardDuty を追加しました。詳細はこちら	2019 年 5 月 9 日

新しい検出結果タイプ Recon:EC2/PortProbeEMRUnprotectedPort が追加されました。	この検出結果は、EC2 インスタンス上にある EMR 関連のセンシティブなポートがブロックされておらず、悪意のあるホストが探していることを知らせるものです。詳細はこちら	2019 年 5 月 8 日
EC2 インスタンスがサービス拒否 (DoS) 攻撃に使われる可能性がある場合に検出される 5 つの新しい検出結果タイプが追加されました。	これらの検出結果から、環境内の EC2 インスタンスがサービス拒否 (DoS) 攻撃の実行に利用されている可能性があることがわかります。詳細はこちら	2019 年 3 月 8 日
新しい検出結果タイプ Policy:IAMUser/RootCredentialUsage が追加されました。	Policy:IAMUser/RootCredentialUsage 検出結果タイプは、のルートユーザーのサインイン認証情報 AWS アカウントが、 AWS サービスへのプログラムによるリクエストに使用されていることを知らせるものです。詳細はこちら	2019 年 1 月 24 日
UnauthorizedAccess:IAMUser/UnusualASNCaller 検出結果タイプは廃止されました	UnauthorizedAccess:IAMUser/UnusualASNCaller 検出結果タイプは廃止されました。これで、他のアクティブな GuardDuty 検出結果タイプを介して異常なネットワークから呼び出されたアクティビティが通知されます。生成される検出結果タイプは、異常なネットワークから呼び出された API のカテゴリに基づきます。詳細はこちら	2018 年 12 月 21 日

2 つの新しい検出結果タイプ PenTest:IAMUser/ParrotLinux および PenTest:IAMUser/PentooLinux が追加されました。	PenTest:IAMUser/ParrotLinux の検出結果タイプは、Parrot Security Linux を実行しているコンピュータで、自身の AWS アカウントの認証情報を使用して API コールが行われていることを通知します。PenTest:IAMUser/PentooLinux 検出結果タイプは、Pentoo Linux を実行しているマシンで、自身の AWS アカウントの認証情報を使用して API コールが行われていることを通知します。詳細はこちら	2018 年 12 月 21 日
Amazon の GuardDuty お知らせ SNS トピックのサポートを追加	GuardDuty お知らせ SNS トピックをサブスクライブして、新しくリリースされた検出結果タイプ、既存の検出結果タイプの更新、およびその他の機能の変更に関する通知を受信できるようになりました。Amazon SNS がサポートするすべての形式で通知を使用できます。詳細はこちら	2018 年 11 月 21 日

2 つの新しい検出結果タイプ UnauthorizedAccess:EC2/TorClient および UnauthorizedAccess:EC2/TorRelay が追加されました。	UnauthorizedAccess:EC2/TorClient 検出結果タイプは、 AWS 環境の EC2 インスタンスが Tor Guard または Authority ノードに接続していることを知らせるものです。UnauthorizedAccess:EC2/TorRelay検出結果タイプは、AWS 環境の EC2 インスタンスが Tor リレーとして動作していることを示す方法で Tor ネットワークに接続していることを知らせるものです。詳細はこちら	2018 年 11 月 16 日
新しい検出結果タイプ CryptoCurrency:EC2/BitcoinTool.B が追加されました。	この検出結果は、 AWS 環境内の EC2 インスタンスが Bitcoin に関連付けられたドメイン名、またはその他の暗号通貨関連のアクティビティをクエリしていることを知らせるものです。詳細はこちら	2018 年 11 月 9 日
Events に送信される通知の頻度を更新するためのサポートを追加 CloudWatch	既存の検出結果のその後の出現について、 CloudWatch イベントに送信される通知の頻度を更新できるようになりました。有効な値は、15 分、1 時間、またはデフォルトの 6 時間です。詳細はこちら	2018 年 10 月 9 日
リージョンサポートが追加されました	AWS GovCloud （ 米国西部) のリージョンサポートを追加 詳細はこちら	2018 年 7 月 25 日

AWS CloudFormation StackSets で のサポートを追加 GuardDuty	Amazon テンプレートを有効にするを使用して GuardDuty 、複数のアカウントで GuardDuty 同時に を有効にできます。詳細はこちら	2018 年 6 月 25 日
GuardDuty 自動アーカイブルールのサポートを追加	お客様は、検出結果の数を抑えられるよう、詳細な自動アーカイブルールを構築できるようになりました。自動アーカイブルールに一致する検出結果の場合、 は自動的にアーカイブ済みとして GuardDuty マークします。これにより、お客様はさらに を調整し GuardDuty て、現在の検出結果テーブルに関連する検出結果のみを保持できます。詳細はこちら	2018 年 5 月 4 日
GuardDuty が欧州 (パリ) リージョンで利用可能に	GuardDuty が欧州 (パリ) で利用可能になりました。これにより、このリージョンで継続的なセキュリティモニタリングと脅威検出を拡張できます。詳細はこちら	2018 年 3 月 29 日
による GuardDuty 管理者アカウントとメンバーアカウントの作成がサポートされる AWS CloudFormation ようになりました。	詳細については、「`AWS::GuardDuty::master`」および「`AWS::GuardDuty::member`」を参照してください。	2018 年 3 月 6 日

9 つの新しい CloudTrailベースの異常検出を追加しました。	これらの新しい検出結果タイプは、サポートされているすべてのリージョン GuardDuty で で自動的に有効になります。 詳細はこちら	2018 年 2 月 28 日
つの新しい脅威インテリジェンス検出 (検出結果タイプ) が追加されました。	これらの新しい検出結果タイプは、サポートされているすべてのリージョン GuardDuty で で自動的に有効になります。詳細はこちら	2018 年 2 月 5 日
GuardDuty メンバーアカウントの引き上げを制限します。	このリリースでは、アカウント (GuardDuty 管理者アカウント) ごとに AWS 最大 1,000 個の GuardDuty メンバーアカウントを追加できます。詳細はこちら	2018 年 1 月 25 日
GuardDuty 管理者アカウントとメンバーアカウントの信頼された IP リストと脅威リストのアップロードとさらなる管理の変更。	このリリースでは、管理者アカウント GuardDuty アカウントのユーザーは、信頼できる IP リストと脅威リストをアップロードおよび管理できます。メンバー GuardDuty アカウントのユーザーは、リストをアップロードおよび管理できません。管理者アカウントによってアップロードされる信頼された IP リストと脅威リストは、メンバーアカウントの GuardDuty 機能に適用されます。詳細はこちら	2018 年 1 月 25 日

以前の更新

変更	説明	日付
初版発行	Amazon GuardDuty ユーザーガイドの初回発行。	2017 年 11 月 28 日

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