AWS Incident Detection and Response の概念と手順

AWS Incident Detection and Response ユーザーガイド

Version May 26, 2026

AWS Incident Detection and Response ユーザーガイド: AWS Incident Detection and Response の概念と手順

Table of Contents

AWS Incident Detection and Response とは

AWS Incident Detection and Response は、対象となる AWS エンタープライズサポートのお客様に、障害の可能性を減らし、重要なワークロードの中断からの復旧を加速するための、プロアクティブなインシデント対応を提供します。Incident Detection and Response により、AWS とのコラボレーションが促進され、オンボーディングされた各ワークロードに合わせてカスタマイズされたランブックとレスポンスプランが策定できます。

インシデント検出と対応には、次の主要な機能があります。

- オブザーバビリティの向上: AWS の専門家は、ワークロードのアプリケーションレイヤーとインフラストラクチャレイヤー間のメトリクスとアラームの定義と関連付けを支援し、中断を早期に検出できるようにします。
- 5 分の応答時間: インシデント管理エンジニアは、ワークロードから、または送信した重大なケースに応じて、アラームから 5 分以内にプロアクティブにお客様をエンゲージします。
- より迅速な解決: IME は、ワークロード用に策定された事前定義済みのカスタムランブックを使用し、お客様に代わってサポートケースを作成し、ワークロードのインシデントを管理します。IME は、インシデントに対する一元化された所有権を提供し、インシデントが解決されるまで適切な AWS の専門家と連携し続けます。
- 障害の可能性の低減: 解決後、IME はインシデント後レビュー (リクエストに応じて) を提供します。また、AWS の専門家がお客様と協力して、インシデントレスポンスプランとランブックを改善するために学んだ教訓を適用します。また、ワークロードの回復性の継続的な追跡に AWS Resilience Hub を活用することもできます。

トピック

AWS アカウントへのサインアップ

AWS を使い始めるには、AWS アカウントが必要です。AWS アカウントの作成の詳細については、「AWS アカウント管理 リファレンスガイド」の「AWS アカウントの開始方法」を参照してください。

Incident Detection and Response の利用規約

次のリストは、AWS Incident Detection and Response を使用するための主要な要件と制限の概要を示しています。この情報は、サポートプランの要件、オンボーディングプロセス、最小サブスクリプション期間などの側面をカバーするため、サービスを使用する前に理解しておくことが重要です。

- AWS Incident Detection and Response は直販およびパートナーが再販したエンタープライズサポートアカウントで利用できます。
- AWS Incident Detection and Response は Partner-Led Support のアカウントでは利用できません。
- Incident Detection and Response サービスの期間中は、常に AWS エンタープライズサポートを維持する必要があります。詳細については、「AWS エンタープライズサポート」を参照してください。エンタープライズサポートを終了すると、AWS Incident Detection and Response サービスから同時に削除されます。
- AWS Incident Detection and Response のすべてのワークロードは、ワークロードのオンボーディングプロセスを経る必要があります。
- アカウントで AWS Incident Detection and Response をサブスクライブするための最小期間は 90 日です。すべてのキャンセルリクエストは、キャンセル予定日の 30 日前に提出する必要があります。
- AWS は、「AWS プライバシー通知」の説明に従ってお客様の情報を取り扱います。

> **Note**
>
> Incident Detection and Response の請求に関する質問については、AWS の請求に関連したヘルプについての記事を参照してください。

Incident Detection and Response のアーキテクチャ

次の図に示すように、AWS Incident Detection and Response は既存の環境と統合されます。このアーキテクチャには、以下のサービスが含まれます。

- Amazon EventBridge: Amazon EventBridge は、ワークロードと AWS Incident Detection and Response 間の唯一の統合ポイントとして機能します。アラームは、AWS によって管理される事前定義されたルールを使用して、Amazon EventBridge を介して Amazon CloudWatch などのモニタリングツールから取り込まれます。Incident Detection and Response が EventBridge ルールを構築および管理できるようにするには、サービスにリンクされたロールをインストールします。これらのサービスの詳細については、「Amazon EventBridge とは」、「Amazon EventBridge ルールとは」、「Amazon CloudWatch とは」、「AWS Health のサービスにリンクされたロールの使用」を参照してください。
- AWS Health: AWS Health は、リソースのパフォーマンスと、AWS のサービスのアカウントの可用性を継続的に可視化します。Incident Detection and Response では、AWS Health を使用して、ワークロードが使用する AWS のサービス のイベントを追跡し、ワークロードからアラートを受け取ったときに通知します。AWS Health の詳細については、「AWS Health とは」を参照してください。
- AWS Systems Manager: Systems Manager は、AWS リソース全体で自動化とタスク管理のための統合ユーザーインターフェイスを提供します。AWS Incident Detection and Response は、ワークロードアーキテクチャの詳細、アラームの詳細、対応するインシデント管理ランブックなどのワークロードに関する情報を AWS Systems Manager ドキュメントでホストします (詳細については、「AWS Systems Manager ドキュメント」を参照してください)。AWS Systems Manager の詳細については、「AWS Systems Manager とは」を参照してください。
- 特定のランブック: インシデント管理ランブックは、インシデント管理中に AWS Incident Detection and Response が実行するアクションを定義します。特定のランブックは、AWS Incident Detection and Response に、連絡先、連絡方法、共有する情報を伝えます。

Incident Detection and Response における役割と責任

AWS Incident Detection and Response RACI (Responsible = 実行責任者、Accountable = 説明責任者、Consulted = 相談先、Informed = 報告先) の表は、インシデントの検出と対応に関連するさまざまなアクティビティの役割と責任の概要を示します。この表は、データ収集、運用準備状況レ

ビュー、アカウント設定、インシデント管理、インシデント後レビューなどのタスクに対するお客様と AWS Incident Detection and Response チームの関与を定義するのに役立ちます。

アクティビティ	お客様	Incident Detection and Response
データ収集		
カスタマーとワークロードの導入	相談先	実行責任者
アーキテクチャ	実行責任者	説明責任者
オペレーション	実行責任者	説明責任者
設定する CloudWatch アラームを決定する	実行責任者	説明責任者
インシデントレスポンスプランを定義する	実行責任者	説明責任者
運用準備状況のレビュー		
ワークロードに関する Well Architected レビュー (WAR) を実施する	相談先	実行責任者
インシデント対応を検証する	相談先	実行責任者
アラームマトリックスを検証する	相談先	実行責任者
ワークロードで使用されている主要な AWS のサービスを特定する	説明責任者	実行責任者
アカウント設定		

アクティビティ	お客様	Incident Detection and Response
カスタマーアカウントに IAM ロールを作成する	実行責任者	報告先
作成したロールを使用してマネージド EventBridge ルールをインストールする	報告先	実行責任者
オンボーディングされたアラームをテストする (CloudWatch または APM)	説明責任者	報告先
カスタマーアラームがインシデントの検出と対応に関与していることを確認する	報告先	実行責任者
アラームを更新する	実行責任者	相談先
ランブックを更新する	相談先	実行責任者
インシデント管理		
Incident Detection and Response によって検出されたインシデントをプロアクティブに通知する	報告先	実行責任者
インシデント対応を提供する	報告先	実行責任者
インシデントの解決/インフラストラクチャの復元を提供する	実行責任者	相談先
インシデント後レビュー		
インシデント後レビューをリクエストする	実行責任者	報告先

アクティビティ	お客様	Incident Detection and Response
インシデント後レビューを提供する	報告先	実行責任者

Incident Detection and Response が利用可能なリージョン

AWS Incident Detection and Response は、次のいずれかの AWS リージョンでホストされている AWS エンタープライズサポートアカウントで英語、日本語、中国標準語、韓国語でご利用いただけます。

AWS リージョン	名前
米国東部 (バージニア州北部) リージョン	us-east-1
米国東部(オハイオ州)リージョン	us-east-2
米国西部 (北カリフォルニア) リージョン	us-west-1
米国西部 (オレゴン州) リージョン	us-west-2
カナダ (中部) リージョン	ca-central-1
カナダ西部 (カルガリー)	ca-west-1
南米 (サンパウロ) リージョン	sa-east-1
欧州 (フランクフルト) リージョン	eu-central-1
欧州 (アイルランド) リージョン	eu-west-1
欧州 (ロンドン) リージョン	eu-west-2
欧州 (パリ) リージョン	eu-west-3
欧州 (ストックホルム) リージョン	eu-north-1

AWS リージョン	名前
欧州 (チューリッヒ) リージョン	eu-central-2
欧州 (ミラノ) リージョン	eu-south-1
欧州 (スペイン) リージョン	eu-south-2
アジアパシフィック (ムンバイ)	ap-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
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (ハイデラバード)	ap-south-2
アジアパシフィック (ジャカルタ)	ap-southeast-3
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 (マレーシア)	ap-southeast-5
アフリカ (ケープタウン)	af-south-1
イスラエル (テルアビブ)	il-central-1
中東 (アラブ首長国連邦)	me-central-1
中東 (バーレーン)	me-south-1
AWS GovCloud (米国東部)	us-gov-east-1
AWS GovCloud (米国西部)	us-gov-west-1

Incident Detection and Response の開始方法

ワークロードとアラームは AWS Incident Detection and Response の中核です。AWS は、お客様と密接に連携して、ビジネスにとって重要な特定のワークロードを定義およびモニタリングします。AWS は、重大なパフォーマンスの問題やお客様への影響をチームに通知するアラームの設定を支援します。Incident Detection and Response 内のプロアクティブなモニタリングと迅速なインシデント対応には、適切に設定されたアラームが不可欠です。

Incident Detection and Response でのワークロードについて

AWS Incident Detection and Response を使用すると、特定のワークロードを選択して、モニタリングおよび重要なインシデント管理を行うことができます。ワークロードは、リソースとコードの集合であり、連携してビジネス価値を提供します。ワークロードとは、お客様の銀行支払いポータルまたは顧客関係管理 (CRM) システムを構成するすべてのリソースとコードです。ワークロードは、1 つの AWS アカウントまたは複数の AWS アカウントでホストできます。

例えば、モノリシックアプリケーションが 1 つのアカウントでホストされている場合があります (次の図の従業員パフォーマンスアプリケーションなど)。または、アプリケーション (図のストアフロントウェブアプリケーションなど) が、マイクロサービスに分割されて、複数の異なるアカウントにまたがっている場合があります。次の図に示すように、ワークロードが、データベースなどのリソースを他のアプリケーションやワークロードと共有している場合があります。

ワークロードのオンボーディングを開始する方法については、「Incident Detection and Response へのワークロードのオンボード」を参照してください。

Incident Detection and Response のアラームについて

アラームは、Incident Detection and Response の重要な部分です。アラームは、アプリケーションおよび基盤となる AWS インフラストラクチャのパフォーマンスを可視化します。AWS はお客様と連携して、モニタリング対象のワークロードに重大な影響がある場合にのみ適切なメトリクスとアラームをトリガーするしきい値を定義します。目標は、アラームにより、指定したリゾルバーをエンゲージしてインシデント管理チームと連携し、問題を迅速に軽減することです。アラームは、パフォーマンスやカスタマーエクスペリエンスの大幅な低下にすぐ対処する必要がある場合にのみ、[Alarm] 状態に入るように設定します。アラームの主なタイプには、ビジネスへの影響を示すアラーム、Amazon CloudWatch canary、依存関係をモニタリングする集計アラームなどがあります。

アラームの取り込みの使用を開始するには、「アラームの取り込み」を参照してください。

Incident Detection and Response へのワークロードのオンボード

AWS Incident Detection and Response を使用すると、選択したワークロードに対して、モニタリングおよび重大インシデント管理を行うことができます。ワークロードは、支払いポータルや顧客関係管理 (CRM) システムなど、ビジネス価値を提供するために連携するリソースのコレクションです。これらのワークロードは、アーキテクチャに応じて、単一の AWS アカウントでホストすることも、複数のアカウントに分散することもできます。

目次

IDR CLI により Incident Detection and Response にオンボードする

AWS Incident Detection and Response カスタマーコマンドラインインターフェイス (IDR CLI) は、AWS Incident Detection and Response へのオンボードを効率化するコマンドラインインターフェイスツールです。

IDR CLI は AWS CloudShell で実行され、次の機能を実行します。

- オンボーディング情報を収集する
- Resource Groups Tagging API を介して AWS リソースデータを収集する
- AWS サポート ケースを管理する
- 新しい Amazon CloudWatch アラームを作成するか、既存のアラームを取り込む
- AWS CloudFormation を介してインフラストラクチャをデプロイしてテストし、サードパーティーのツールが Incident Detection and Response にアラートを送信できるようにします。

IDR CLI をインタラクティブモードで実行してオンボーディング手順をガイドすることも、一括処理や DevOps ユースケースの場合はオフラインモードで実行することもできます。

インストール、前提条件、エンドツーエンドの例など、IDR CLI の使用方法の詳細については、「CLI for AWS Incident Detection and Response」を参照してください。

IDR CLI の言語サポート

AWS Incident Detection and Response は、英語、日本語、標準中国語、および韓国語で利用できます。日本語、標準中国語、および韓国語でサポートが必要な場合は、IDR CLI によって作成された AWS サポート ケースを介して AWS にお問い合わせになるか、テクニカルアカウントマネージャー (TAM) にお問い合わせください。

ワークロードをオンボードするための代替オプション

IDR CLI をオンボーディングに使用できない場合は、テクニカルアカウントマネージャー (TAM) に代替オプションを依頼してください。詳細については、Incident Detection and Response でのワークロードのオンボーディングとアラーム取り込みのアンケート (例外パス)を参照してください。

アラームの取り込み

AWS Incident Detection and Response カスタマーコマンドラインインターフェイス (CLI) は、新しい Amazon CloudWatch アラームを作成したり、既存のアラームを取り込んだりできます。また、AWS CloudFormation を介してインフラストラクチャをデプロイしてテストし、サードパーティーのツールが AWS Incident Detection and Response にアラートを送信できるようにします。

AWS Incident Detection and Response では、Amazon EventBridge を介して Amazon CloudWatch およびサードパーティーのアプリケーションパフォーマンスモニタリング (APM) ツールからアラームを取り込むことができます。

- CloudWatch アラームの取り込み
- サードパーティーのアプリケーションパフォーマンスモニタリングアラームの取り込み

アラームの取り込み手順

アラームの取り込みでは、次のステップを完了する必要があります。

- アラームの定義
- IDR CLI を使用したアラームの取り込み
- アラームの確認とフィードバック
- Incident Detection and Response にアラームを取り込むためのアクセスをプロビジョニングする
- アラームの本番稼働

アラームを取り込むための代替オプション

IDR CLI をアラームの取り込みに使用できない場合は、テクニカルアカウントマネージャー (TAM) に代替オプションを依頼してください。詳細については、Incident Detection and Response でのワークロードのオンボーディングとアラーム取り込みのアンケート (例外パス)を参照してください。

Incident Detection and Response にアラームを取り込むためのアクセスをプロビジョニングする

> **Note**
>
> IDR CLI オンボーディング中にサービスにリンクされたロール (SLR) を作成しなかった場合は、以下のステップに従ってアクセスを手動でプロビジョニングします。

AWS Incident Detection and Response がアカウントからアラームを取り込むことができるようにするには、`AWSServiceRoleForHealth_EventProcessor` SLR を作成します。AWS は、SLR を引き受けてアカウントでマネージド EventBridge ルールを作成します。マネージド EventBridge ルールは、アカウントから AWS Incident Detection and Response に通知を送信します。関連する AWS マネージドポリシーを含むこの SLR の詳細については、「ユーザーガイド」の「サービスにリンクされたロールの使用」を参照してください。

このサービスにリンクされたロールをアカウントに作成するには、「AWS Identity and Access Management ユーザーガイド」の「サービスにリンクされたロールの作成」の手順に従います。あるいは、次の AWS Command Line Interface (AWS CLI) コマンドを使用できます。

```
aws iam create-service-linked-role --aws-service-name event-
processor.health.amazonaws.com
```

重要なアウトプット

- サービスにリンクされたロールがアカウントに正常に作成されました。

> **Note**
>
> サービスにリンクされたロール AWSServiceRoleForHealth_EventProcessor は、AWS Incident Detection and Response にアラームを送信するために使用するアカウントごとに作成する必要があります。

関連情報

詳細については、以下の各トピックを参照してください。

- のサービスリンクロールの使用
- サービスにリンクされたロールの作成
- AWS マネージドポリシー: AWSHealth_EventProcessorServiceRolePolicy

アラームの定義

アラームを AWS Incident Detection and Response にオンボードするときは、アプリケーションのパフォーマンスを可視化するメトリクスとアラーム設定を定義する必要があります。このプロセスの一環として、これらのアラームへの対応を担当する組織内のチームも特定する必要があります。

アラームを準備する際に推奨されるベストプラクティスを以下に示します。

- アラームが「アラーム」状態になるのは、モニタリング対象のワークロードに継続的かつ重大な影響があり、チームと AWS からの早急な対応が必要なときのみです。トリガーされて自動的に復旧しないアラームが発生した場合は、チームがインシデントブリッジを AWS Incident Detection and Response に結合する必要があります。
- 指定した連絡先情報により、AWS Incident Detection and Response が組織内の適切なチームを 24 時間 365 日インシデントブリッジに確実にエンゲージすることができます。

重要なアウトプット

- IDR CLI を使用して AWS Incident Detection and Response に提供するアラームと連絡先の詳細のリスト。

Amazon CloudWatch アラームの定義と取り込みの詳細については、「CloudWatch アラームの取り込み」を参照してください。

サードパーティーのアプリケーションパフォーマンスモニタリングアラームの取り込みの詳細については、「サードパーティーのアプリケーションパフォーマンスモニタリングアラームの取り込み」を参照してください。

CloudWatch アラームの取り込み

AWS Incident Detection and Response は、Amazon CloudWatch アラームを取り込み、重大なワークロードをプロアクティブにモニタリングできます。AWS Incident Detection and Response は、Amazon CloudWatch アラームを取り込むことで、以下のことができます。

- アラームがいつ「アラーム」状態になったかを自動的に検出します。
- チームをエンゲージし、協力しながらインシデントに対応して解決します。

オンボードしたアラームを確実に有効にするために、AWS Incident Detection and Response では以下のベストプラクティスを推奨しています。

- 誤検出アラームのエンゲージメントを回避するために、定期的なメンテナンスまたはバッチジョブの実行中にアラームを抑制するメトリクス数式を使用してアラームを設定します。
- 予想されるデータポイントの配信頻度に基づいて、アラームに欠落データ処理を設定します。例えば、データポイントの継続的なストリームを生成するアラームモニタリングメトリクスでは、欠落しているデータを「違反」(不良) として扱う必要があります。欠落しているデータポイントは、モニタリング対象の基盤となるリソースに問題があることを示している可能性があるためです。逆に、障害やエラーが発生したときにのみデータポイントを記録するアラームモニタリングメトリクスなど、データポイントを頻繁に報告しないメトリクスをモニタリングするアラームでは、欠落しているデータを「違反でない」(良好) として扱う必要があります。
- ワークロードに重大で継続的な影響がある場合に「アラーム」状態になるアラームを定義します。例えば、異常なリソースを最初に検出したときではなく、異常なリソースを自動的に置き換えるのに必要だと予想される時間が経過した後にトリガーするようにアラームを設定します。
- ワークロードのカスタマーエクスペリエンスを直接表すカスタムメトリクスのアラームを特定して作成します。

一般的な AWS のサービスに推奨される Amazon CloudWatch アラームのリストについては、AWS re:Post の Incident Detection and Response のアラームに関するベストプラクティスについてのページを参照してください。

サードパーティーのアプリケーションパフォーマンスモニタリングアラームの取り込み

AWS Incident Detection and Response は、Amazon EventBridge を介したサードパーティーのアプリケーションパフォーマンスモニタリング (APM) ツールからのアラームの取り込みをサポートしています。この統合により、APM アラートを取り込むことで柔軟性が得られ、さまざまな AWS のサービスを介してアカウントの Amazon EventBridge イベントバスに APM イベントをルーティングできます。

統合パスの例:

- ソース (APM) → AWS のサービス (例: Amazon API Gateway や Amazon SNS) → Transform Lambda 関数 → カスタム Amazon EventBridge イベントバス → AWS Incident Detection and Response
- ソース (APM) → パートナーの Amazon EventBridge イベントバス → Transform Lambda 関数 → カスタム Amazon EventBridge イベントバス → AWS Incident Detection and Response

AWS Incident Detection and Response は、カスタムイベントバスにマネージドルールをインストールして、Transform Lambda 関数によって送信されたアラートを取り込みます。SaaS Amazon EventBridge 統合の場合、パートナーイベントバスはマネージドルールがインストールされているイベントバスではないことに注意してください。Amazon EventBridge とのパートナー統合を行っている APM の詳細なリストについては、「Amazon EventBridge の統合」を参照してください。

パートナーイベントバスまたは他の AWS イベントバスソースを使用した統合の例

次の図は、パートナーイベントバスまたは他の AWS イベントバスソースを使用した統合の例を示しています。

Amazon EventBridge とのパートナー統合を行っている APM の詳細なリストについては、「Amazon EventBridge の統合」を参照してください。

Amazon API Gateway を使用した統合の例

次の図は、API Gateway を使用した統合の例を示しています。

Amazon Simple Notification Service を使用した統合の例

次の図は、Amazon SNS を使用した統合の例を示しています。

統合プロセスを簡素化するために、AWS Incident Detection and Response は最も一般的に使用される統合タイプ用の CloudFormation テンプレートを提供します。これらのテンプレートは、AWS リソースと必要な IAM ロールのセットアップを自動化します。

CloudFormationさまざまな統合タイプを手動で作成するための テンプレートと手順については、以下の対応する統合のドキュメントを参照してください。

- EventBridge と直接統合されている APM からアラームを取り込む
- EventBridge と直接統合していない APM からアラームを取り込む
- Amazon SNS を直接統合した APM からアラームを取り込む

> **Note**
>
> CloudFormation テンプレートには変更が必要です。これらの変更については、前のトピックで説明しています。AWS Incident Detection and Response に APM アラートを送信するために必要なペイロード形式の詳細については、「EventBridge で APM アラートを取り込むためのペイロード要件」を参照してください。

EventBridge で APM アラートを取り込むためのペイロード要件

Incident Detection and Response は APM アラートをどこから取り込みますか?

AWS Incident Detection and Response は、変換された最終的なペイロードの送信先となるイベントバスにマネージドルールをインストールします。この目的のためにカスタムイベントバスを作成するのがベストプラクティスです。

ペイロードはどのような形式にする必要がありますか?

AWS Incident Detection and Response によって取り込まれるイベントバスのイベントには、最低でも次の JSON キーと値のペアが必要です。

```
{
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent"
    "detail": {
        "incident-detection-response-identifier": "Your alarm name from your APM",
    }
```

```
}
```

次の例は、変換前と変換後のパートナーイベントバスからのイベントを示しています。

変換前:

```
{
    "version": "0",
    "id": "a6150a80-601d-be41-1a1f-2c5527a99199",
    "detail-type": "Datadog Alert Notification",
    "source": "aws.partner/datadog.com/Datadog-aaa111bbbc",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "alert_type": "error",
        "event_type": "query_alert_monitor",
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
                "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 <= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
```

```
                }
            },
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
            "aws_account:123456789012",
            "monitor"
        ]
    }
}
```

イベントが変換される前に、detail-type と source はアラートが発生した APM の詳細を示すことに注意してください。これらは取り込み前に変更する必要があります。incident-detection-response-identifier キーはまだ存在していないため、取り込み前に追加する必要があります。

Lambda 関数は上記のイベントを変換し、ターゲットのカスタムイベントバスまたはデフォルトのイベントバスに配置します。変換されたペイロードには、必要なキーと値のペアが含まれる必要があります。

変換後:

```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "incident-detection-response-identifier": "UnHealthyHostCount",
        "alert_type": "error",
```

```
        "event_type": "query_alert_monitor",
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
                "query":
"max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
<= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
                }
            },
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
            "aws_account:123456789012",
            "monitor"
```

```
        ]
    }
}
```

detail-type は ams.monitoring/generic-apm、ソースは GenericAPMEvent になり、詳細には新しいキーと値のペアである incident-detection-response-identifier が存在するようになりました。

incident-detection-response-identifier 値は、APM が送信するペイロードに基づいてアラート名から取得されます。APM アラート名のパスは、APM ごとに異なります。Lambda 関数は、Lambda が受け取った APM JSON ペイロードの正しいパスからアラーム名を取得し、incident-detection-response-identifier 値に使用するように設定する必要があります。

incident-detection-response-identifier 値は、AWS Incident Detection and Response に送信されるアラームタイプごとに一意である必要があります。incident-detection-response-identifier で設定される一意の名前はそれぞれ、オンボーディング中に AWS Incident Detection and Response チームに提供される必要があります。incident-detection-response-identifier キーの値が不明または欠落しているイベントは処理されません。

EventBridge と直接統合されている APM からアラームを取り込む

次のトピックは、Amazon EventBridge と直接統合されているアプリケーションパフォーマンスモニタリング (APM) ツールから AWS Incident Detection and Response にアラームを送信するプロセスを示しています。Amazon EventBridge と直接統合されている APM の詳細なリストについては、「Amazon EventBridge の統合」を参照してください。

提供された CloudFormation テンプレートをデプロイすることも、この統合を手動でセットアップすることもできます。統合を設定する前に、AWS のサービスにリンクされたロール (SLR) AWSServiceRoleForHealth_EventProcessor がアカウントに作成されていることを確認します。

オプション 1: を使用するCloudFormation

CloudFormation テンプレートを使用すると、Amazon EventBridge 統合を使用して APM から AWS Incident Detection and Response にアラームを取り込むために必要な統合インフラストラクチャを作成するプロセスを簡素化できます。

> **Note**
>
> - この CloudFormation テンプレートを介してデプロイされたリソース (Lambda や EventBridge など) には、追加コストが発生します。これらのサービスの料金の詳細については、「AWS の料金」を参照してください。
> - この CloudFormation テンプレートは、AWS Incident Detection and Response がアラームを取り込む必要があるすべての AWS アカウントとリージョンにデプロイします。インシデントとサポートケースは、APM アラートの受信元となった AWS アカウントで開かれます。
> - このドキュメントでは例として New Relic を使用していますが、CloudFormation テンプレートは Amazon EventBridge と SaaS 統合されている任意の APM に使用できます。
> - 統合をテストしたら、logger.info() ステートメントを `TransformLambdaFunction` から削除して、ペイロードが Amazon CloudWatch Logs に表示されないようにします。

この CloudFormation テンプレートをデプロイするための前提条件:

- パートナーイベントソースを Amazon EventBridge で設定する必要があります。APM をイベントソースとして設定する手順については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge での SaaS パートナーからのインベントの受信」を参照してください。
- テンプレートの `TransformLambdaFunction` (Lambda 関数) を変更して、APM ペイロードのアラート名の JSON パスに基づいて `["detail"]["incident-detection-response-identifier"]` を目的の値に設定する必要があります。

前提となる手順:

1. EventBridge コンソールを開きます。[統合] メニューで、[パートナーイベントソース] を選択します。
   - [Amazon EventBridge パートナー] ボックスで APM を検索します。
   - [セットアップ] を選択し、手順に従います。
     - 注意: 最後のステップでは、パートナーイベントソースのコンソールで [イベントバスと関連付ける] を選択します。このオプションを選択すると、パートナーイベントソースと同じ名前のパートナーイベントバスが自動的に作成されます (名前は一致する必要があります)。

- パートナーイベントバスまたはソースの名前をコピーします。イベントバスまたはソースは、CloudFormation テンプレートをデプロイするときに、`PartnerEventBusNameParameter` という名前のパラメータとして使用されます。
  - New Relic の例: `aws.partner/newrelic.com/1234567/source_name`
- CloudFormation テンプレートをデプロイするときに、`PartnerEventBusPrefixParameter` に入力するパートナーイベントバスまたはソースの最初の部分をコピーします。
  - New Relic の例は `aws.partner/newrelic.com` です

2. CloudFormation テンプレートをダウンロードして編集します。
   - テンプレートで `TransformLambdaFunction` を見つける
   - `def lambda_handler(event, context)` で、`event["detail"]["incident-detection-response-identifier"]` をアラーム名が APM アラームの JSON ペイロードに表示される JSON パスに設定します。APM ごとにパスが異なります。以下に例をいくつか示しますが、特定のペイロードは異なる場合があります。
     - New Relic の例: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["workflowName"]`。
     - Datadog の例: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["meta"]["monitor"]["name"]`
     - Splunk の例: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["ruleName"]`
   - CloudFormation テンプレートを保存します。

CloudFormation テンプレートのデプロイ:

1. ターゲットアカウントおよびリージョンで CloudFormation コンソールを開きます。
2. [スタックの作成] の [新しいリソースを使用 (標準)] を選択します。
   - [既存のテンプレートを選択]、[テンプレートファイルのアップロード]、[ファイルを選択] の順に選択し、ローカルに保存した CloudFormation テンプレートをアップロードします。
3. スタックの詳細を指定する:
   - スタック名を入力します (例: `NewRelicIntegrationForIDR`)。
   - 前提条件の完了時に取得した [パラメータ値] を指定します。
     - APMNameParameter (例: `NewRelic`)
     - PartnerEventBusNameParameter (例: `aws.partner/newrelic.com/1234567/source_name`)

    - PartnerEventBusPrefixParameter (例: `aws.partner/newrelic.com`)
  - [次へ] を選択します。
4. スタックオプションを設定する:
  - ページの下部までスクロールし、CloudFormation がカスタム名で IAM リソースを作成できるようにするチェックボックスをオンにします。
5. 確認と作成:
  - パラメータ値が正しく設定されていることを検証し、[送信] を選択します。
6. CloudFormation スタックは、APM イベントを AWS Incident Detection and Response に統合するために必要なリソースをデプロイします。スタックステータスが `CREATE_COMPLETE` と表示されるまで待ちます。
7. CloudFormation スタックは、サンプル値が New Relic のパラメータに入力され、US-EAST-1 リージョンで実行されたと仮定して、次のリソースを作成します。
  - CustomEventBus: NewRelic-AWSIncidentDetectionResponse-EventBus
  - EventBridgeRule: aws.partner/newrelic.com/1234567/source_name|NewRelic-AWSIncidentDetectionResponse-EventBridgeRule
  - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
  - TransformLambdaFunction: NewRelic-AWSIncidentDetectionResponse-Lambda-Transform
  - TransformLambdaPermission: NewRelicIntegrationForIDR-TransformLambdaPermission-[random_string]

インテグレーションテスト

スタックをデプロイしたら、APM からテストペイロードを送信して統合をテストします。

1. Lambda コンソールに移動して、`APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` 関数を選択します。[Monitor] (モニタリング) タブを選択します。
2. メトリクスグラフで正常な呼び出しを探します。
3. [Amazon CloudWatch Logs を表示する] を選択して、テストペイロードまたはエラーのログストリームを確認します。

AWS Incident Detection and Response へのイベントバス ARN の共有

1. Amazon EventBridge コンソールを開きます。[イベントバス] を選択します。

2. CloudFormation スタックの一部として作成された [カスタムイベントバス] の ARN をコピーします (例: *arn:aws:events:us-east-1:123456789123:event-bus/NewRelic-AWSIncidentDetectionResponse-EventBus*)。
   - この ARN を アラーム取り込みのアンケート – 概要 の「サードパーティー APM アラーム」セクションの「EventBridge イベントバス ARN」フィールドに追加します。
3. オンボーディングプロセス中、AWS Incident Detection and Response は、このカスタムイベントバスでマネージド EventBridge ルールを作成して APM アラームを取り込みます。

オプション 2: 手動の統合

AWS Incident Detection and Response がアラームを取り込む必要がある AWS アカウントと AWS リージョンごとに、次の手順を実行します。AWS Incident Detection and Response では、影響を受けているリソースをより迅速に特定して調査できるように、アプリケーションリソースと同じ AWS アカウントとリージョンでアラームを設定することが推奨されます。インシデントとサポートケースは、APM アラートの受信元となった AWS アカウントで開かれます。

1. APM を Amazon EventBridge パートナーイベントソース (`aws.partner/apm_name/integrationName` など) として設定して、EventBridge パートナーイベントバスを作成します。APM をイベントソースとして設定するガイドラインについては、「Receiving events from a SaaS partner with Amazon EventBridge」を参照してください。
2. 次のいずれかを実行します。
   - (推奨) `$YourApmName-AWSIncidentDetectionResponse-EventBus` という名前の EventBridge カスタムイベントバスを作成します。
   - (代替方法) カスタムイベントバスの代わりにデフォルトの EventBridge イベントバスを使用します。

   AWS Incident Detection and Response は、`AWSServiceRoleForHealth_EventProcessor` SLR を介してカスタムイベントバスまたはデフォルトのイベントバスにマネージドルール (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) をインストールします。ルールソースはカスタムイベントバスまたはデフォルトのイベントバスとなり、ルールの送信先は AWS Incident Detection and Response となります。また、ルールはサードパーティーの APM イベントを取り込むパターンと一致します。
3. パートナーイベントバスイベントを変換する、`$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` という名前の Lambda 関数を作成しま

す。変換されたイベントは、マネージドルール `AWSHealthEventProcessorEventSource-DO-NOT-DELETE` と一致します。

- 変換されたイベントには一意の AWS Incident Detection and Response の識別子が含まれ、イベントのソースタイプと詳細タイプを必要な値に設定します。これにより、変換された JSON ペイロード構造がマネージドルールパターンと一致するようになります。
- Lambda 関数のターゲットを、ステップ 2 で作成したカスタムイベントバス (推奨) またはデフォルトのイベントバスに設定します。

4. EventBridge ルールを作成し、AWS Incident Detection and Response にプッシュするイベントのリストと一致するイベントパターンを定義します。ルールのソースは、ステップ 1 (`aws.partner/apm_name/integrationName`) で作成したパートナーイベントバスです。ルールのターゲットは、ステップ 3 (`[apm_name]-AWSIncidentDetectionResponse-LambdaFunction`) で作成した Lambda 関数です。EventBridge ルールの定義に関するガイドラインについては、「Amazon EventBridge ルール」を参照してください。

パートナーイベントバスと AWS Incident Detection and Response の統合を手動で設定する方法のステップバイステップの例については、「Datadog と Splunk からの通知の統合」を参照してください。

EventBridge と直接統合していない APM からアラームを取り込む

AWS Incident Detection and Response では、Amazon EventBridge と直接統合していないサードパーティーの APM からアラームを取り込む場合のウェブフックの使用をサポートしています。

CloudFormation テンプレートをデプロイすることも、この統合を手動で設定することもできます。統合を設定する前に、AWS のサービスにリンクされたロール (SLR) `AWSServiceRoleForHealth_EventProcessor` がアカウントに作成されていることを確認します。

オプション 1: CloudFormation テンプレートの使用

CloudFormation テンプレートを使用すると、Amazon EventBridge と直接統合されていない APM から AWS Incident Detection and Response にアラームを取り込むために必要な統合インフラストラクチャを作成するプロセスを簡素化できます。

この CloudFormation テンプレートをデプロイする前に考慮すべき点

- このソリューションでは、API Gateway Lambda オーソライザーを使用して、APM からペイロードに渡されたシークレットトークンを AWS Secrets Manager のトークンと比較します。トークン

が一致しない場合、明示的な拒否を含むポリシーが返されます。詳細については、「Lambda オーソライザー」を参照してください。

- AWS の責任共有モデルでは、組織のセキュリティ要件を満たす認証アプローチを使用するのはお客様の責任となります。API キーや認可トークンなどの機密情報をハードコードされた変数として保存する代わりに、AWS Secrets Manager または同様のサービスを使用することをお勧めします。詳細については、「AWS Secrets Manager を使用したシークレットの作成および管理」を参照してください。
- Hash-based Message Authentication Code (HMAC) を実装するその他の例については、aws-samples Github ページの「receive-webhooks」を参照してください。トークン認可の実装の詳細については、API Gateway ドキュメントの「TOKEN オーソライザー Lambda 関数の例」を参照してください。
- このソリューションは、API Gateway の RateLimit、BurstLimit、および Quota を使用してリクエストボリュームを制御します。これらのツールは、設定された時間内に処理できるリクエストの数を制限します。これにより、システムの過負荷を防ぎ、サービスを安定させることができます。スロットリングの詳細については、「API Gateway デベロッパーガイド」を参照してください。
- AWS ウェブアプリケーションファイアウォール (WAF) を使用して、API Gateway を既知の不正な IP アドレスから保護することを検討してください。これにより、攻撃者が実際のログイベントをブロックする可能性のあるフェイクリクエストで API をフラッディングするリスクが軽減されます。
- AWS Secrets Manager トークン値は、HTTP ヘッダーとしてアプリケーションパフォーマンスモニタリング (APM) ツールに保存する必要があります。セキュリティのベストプラクティスとして、トークンを定期的にローテーションしてください。
- この CloudFormation テンプレートを介してデプロイされたリソース (Lambda や EventBridge など) には、追加コストが発生します。これらのサービスの料金の詳細については、「AWS の料金」を参照してください。
- 統合をテストしたら、logger.info() ステートメントを `TransformLambdaFunction` (Lambda 関数) から削除して、ペイロードが Amazon CloudWatch Logs に表示されないようにします。
- この CloudFormation テンプレートは、AWS Incident Detection and Response がアラームを取り込む必要があるすべての AWS アカウントとリージョンにデプロイします。

CloudFormation テンプレートの準備:

注意: 統合ステップでは例として Dynatrace を使用しますが、このテンプレートは API Gateway にペイロードを送信できる任意の APM に使用できます。

1. CloudFormation テンプレートをダウンロードして開きます。
2. テンプレートで APIGWUsagePlan を見つけます。デフォルトでは 20、50、2000 に設定されている RateLimit、BurstLimit、Quota Limit に設定された値を確認します。要件を満たすように値を調整します。
3. テンプレートで AuthorizerLambdaFunction を見つけます。この Lambda 関数は、認証メカニズムの例となります。APM から渡される authorizationToken というヘッダーからトークン値を抽出します。このコードは、組織のセキュリティポリシーと APM 要件に合わせて変更できます。
4. テンプレートで TransformLambdaFunction を見つけます。ディクショナリパス raw_json["detail"]["ProblemTitle"] を、APM から JSON ペイロードで送信されるアラーム名へのパスに置き換えます。Dynatrace の場合は、このパスをそのままにします。

CloudFormation テンプレートのデプロイ:

1. ターゲットアカウントおよび AWS リージョン で CloudFormation コンソールを開きます。
2. [スタックの作成] の [新しいリソースを使用 (標準)] を選択します。
   - [既存のテンプレートを選択]、[テンプレートファイルのアップロード]、[ファイルを選択] の順に選択し、ローカルに保存した CloudFormation テンプレートをアップロードします。
3. スタックの詳細を指定する:
   - スタック名 (例えば、*DynatraceIntegrationForIDR*) を入力します。
   - APMNameParameter (例えば、*Dynatrace*) を入力します。
   - [次へ] を選択します。
4. スタックオプションを設定する:
   - ページの下部までスクロールし、CloudFormation がカスタム名で IAM リソースを作成できるようにするチェックボックスをオンにします。
5. 確認と作成:
   - パラメータ値が正しく設定されていることを検証し、[送信] を選択します。
6. CloudFormation スタックは、APM イベントを AWS Incident Detection and Response に統合するために必要なリソースをデプロイします。CloudFormation スタックのステータスが CREATE_COMPLETE になるまで待ちます。
7. CloudFormation スタックは、サンプル値 Dynatrace がパラメータに入力され、US–EAST–1 リージョンで実行されたと仮定して、次のリソースを作成します。

- シークレット名: DynatraceMySecretTokenName (シークレットキー APMSecureToken に対してランダムなシークレット値が作成されます)
- API Gateway リソース:
  - API 名: Dynatrace-AWSIncidentDetectionResponse-APIGW
  - ステージ名: Dynatrace-Stage-Prod
  - オーソライザー: Dynatrace-APIGW-Authorizer
  - 使用量プラン: APIGW_Throttling_Plan
- Lambda 関数:
  - 認可の関数: Dynatrace-AWSIncidentDetectionResponse-Lambda-Authorizer
  - 変換の関数: Dynatrace-AWSIncidentDetectionResponse-Lambda-Transform
- カスタム EventBus 名: Dynatrace-AWSIncidentDetectionResponse-EventBus
- IAM ロール:
  - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
  - AuthorizerLambdaExecutionRole: IDR-AuthorizerLambdaExecutionRole-us-east-1

8. ウェブフックの URL とトークン値を記録します。
   - API Gateway コンソールを開き、CloudFormation スタックの一部として作成された API 名を選択します。
   - 左側のナビゲーションからステージを選択し、+ 記号を使用してステージ名を展開してから、POST を選択します。呼び出し URL を記録します。APM で、アラームイベントのウェブフックの送信先としてこの URL を設定します。
   - AWS Secrets Manager コンソールを開き、CloudFormation スタックの一部として作成されたシークレット名を選択します (例: DynatraceMySecretTokenName)。
     - [シークレット値] タブで、[シークレットの値を取得する] を選択します。シークレットキーは APMSecureToken と表示されます。シークレット値を記録します。このシークレット値を誰とも共有しないでください。

インテグレーションテスト

スタックをデプロイしたら、APM からテストペイロードを送信して統合をテストします。

1. Lambda コンソールに移動して、`APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` 関数を選択します。[Monitor] (モニタリング) タブを選択します。
2. メトリクスグラフで正常な呼び出しを探します。

3. [Amazon CloudWatch Logs を表示する] を選択して、テストペイロードまたはエラーのログストリームを確認します。

AWS Incident Detection and Response へのイベントバス ARN の共有

1. Amazon EventBridge コンソールを開きます。イベントバスを選択します。
2. CloudFormation スタックの一部として作成された [カスタムイベントバス] の ARN をコピーします (例: *arn:aws:events:us-east-1:123456789123:event-bus/Dynatrace-AWSIncidentDetectionResponse-EventBus*)。
   - この ARN を アラーム取り込みのアンケート – 概要 の「サードパーティー APM アラーム」セクションの「EventBridge イベントバス ARN」フィールドに追加します。
3. オンボーディングプロセス中、AWS Incident Detection and Response は、このカスタムイベントバスにマネージド EventBridge ルールを作成して APM アラームを取り込みます。

オプション 2: 手動の統合

次の手順を使用して、AWS Incident Detection and Response との統合を設定します。

1. APM からのペイロードを受け入れる Amazon API Gateway を作成します。
2. 認証トークンを使用して認可用の Lambda 関数を定義します。
3. 次のいずれかを実行します。
   - (推奨) `$YourApmName-AWSIncidentDetectionResponse-EventBus` という名前の EventBridge カスタムイベントバスを作成します。
   - (代替方法) カスタムイベントバスの代わりにデフォルトの EventBridge イベントバスを使用します。
4. Transform Lambda 関数を定義して、AWS Incident Detection and Response 識別子をペイロードに追加します。この関数を使用すると、AWS Incident Detection and Response に送信するイベントをフィルタリングすることもできます。
   - API Gateway は、API Gateway によって渡されるペイロードを変換する Transform Lambda 関数を呼び出す必要があります。
   - Transform Lambda 関数は、上記のポイント 3 で定義されたイベントバスに、変換されたイベントを書き込む必要があります。
5. API Gateway で生成された URL に通知を送信するよう APM を設定します。

Amazon SNS を直接統合した APM からアラームを取り込む

APM が Amazon SNS トピックへのアラームの送信をサポートしている場合は、このガイドに従って AWS Incident Detection and Response に APM アラームを取り込むことができます。

提供された CloudFormation テンプレートをデプロイすることも、この統合を手動でセットアップすることもできます。統合を設定する前に、AWS のサービスにリンクされたロール (SLR) `AWSServiceRoleForHealth_EventProcessor` がアカウントに作成されていることを確認します。

オプション 1: を使用するCloudFormation

CloudFormation テンプレートを使用すると、Amazon SNS 統合を使用して APM から AWS Incident Detection and Response にアラームを取り込むために必要な統合インフラストラクチャを作成するプロセスを簡素化できます。

> **Note**
>
> - この CloudFormation テンプレートを介してデプロイされたリソース (Lambda や EventBridge など) には、追加コストが発生します。これらのサービスの料金の詳細については、「AWS の料金」を参照してください。
> - この CloudFormation テンプレートは、AWS Incident Detection and Response によってアラームを取り込む必要がある各 AWS アカウントとリージョンにデプロイする必要があります。
> - このドキュメントで提供される例は Grafana 用ですが、このテンプレートは Amazon Simple Notification Service と直接統合されているすべての APM に使用できます。
> - セキュリティ上の理由から、AWS では、ペイロードが Amazon CloudWatch Logs に記録されないようにするため、`TransformLambdaFunction` から `logger.info()` ステートメントを削除することが推奨されます。

この CloudFormation テンプレートをデプロイするための前提条件:

- APM からアラームイベントを受け取るには、Amazon Simple Notification Service の標準トピックを作成する必要があります。Amazon Simple Notification Service コンソールで SNS トピックを作成します。

- テンプレートの TransformLambdaFunction を変更して、使用中の APM に基づいて目的の値に ["detail"]["incident-detection-response-identifier"] を設定する必要があります。

前提条件の完了:

1. Amazon SNS コンソールを開き、[トピック] を選択します。APM からアラームイベントを受け取るために作成された Amazon SNS の標準トピックの ARN をコピーします。
   - 例:arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns
2. CloudFormation テンプレートをダウンロードして開きます。
   - テンプレートで TransformLambdaFunction を見つける
     - def lambda_handler(event, context) で、event["detail"]["incident-detection-response-identifier"] をアラーム名が SNS レコードの JSON ペイロードに表示される JSON パスに設定します。
       - SNS 経由で TransformLambdaFunction に送信されるイベントには、親ペイロード構造として event["Records"][n]["Sns"]["Message"] があります。ソース (APM) からの実際のペイロードオリジンは、親構造内にラップされます。
       - Grafana の例: event["Records"][n]["Sns"]["Message"]["alerts"][n]["labels"]["alertname"]

CloudFormation テンプレートのデプロイ:

1. 統合を設定する必要があるアカウントとリージョンで CloudFormation コンソールに移動します。
2. CloudFormation に移動します。
   - [スタックの作成] の [新しいリソースを使用 (標準)] を選択します。
     - [既存のテンプレートを選択]、[テンプレートファイルのアップロード]、[ファイルを選択] の順に選択し、ローカルに保存した CloudFormation テンプレートをアップロードします。
3. スタックの詳細を指定する:
   - スタック名 (例: <your-apm-name>IntegrationForIDR) を入力します。
   - 前提条件の完了時に取得したパラメータ値を指定します。
     - APMNameParameter 例: Grafana
     - TriggerSNSParameter 例: arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns

- [次へ] を選択します。

4. スタックオプションを設定する:
   - ページの下部までスクロールし、CloudFormation がカスタム名で IAM リソースを作成できるようにするチェックボックスをオンにします。
5. 確認と作成:
   - パラメータ値が正しく設定されていることを検証し、[送信] を選択します。
6. CloudFormation スタックは、APM イベントを AWS Incident Detection and Response に統合するために必要なリソースをデプロイします。CloudFormation スタックのステータスが CREATE_COMPLETE になるまで待ちます。
7. CloudFormation スタックは、サンプル値が Grafana のパラメータに入力され、EU–WEST–1 リージョンで実行されたと仮定して、以下のリソースを作成します。
   - CustomEventBus: Grafana-AWSIncidentDetectionResponse-EventBus
   - SNSSubscription: arn:aws:sns:eu-west-1:012345678912:grafana-sns:[random_string]
   - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-eu-west-1
   - TransformLambdaFunction: Grafana-AWSIncidentDetectionResponse-Lambda-Transform
   - TransformLambdaPermission: GrafanaIntegrationForIDR-TransformLambdaPermission-[random_string]

インテグレーションテスト

CloudFormation スタックが正常にデプロイされたら、APM からテストペイロードを送信して統合を検証できます。APM からテストペイロードが送信されると、次のようになります。

1. Lambda コンソールに移動して、`APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` 関数を選択します。[モニタリング] タブを選択します。
2. 成功した呼び出しは、メトリクスグラフで確認する必要があります。
3. [Amazon CloudWatch Logs を表示する] を選択します。ログストリームのログイベントから検証して、APM から送信されたテストペイロードが存在するか、またはエラーが発生したかどうかを確認できます。

AWS Incident Detection and Response へのイベントバス ARN の共有

1. Amazon EventBridge コンソールにサインインします。イベントバスを選択します。

2. CloudFormation スタックの一部としてデプロイされた [カスタムイベントバス] の ARN を記録します (例: `arn:aws:events:eu-west-1:012345678912:event-bus/Grafana-AWSIncidentDetectionResponse-EventBus`)。
   - アラーム取り込みのアンケート – 概要 の「サードパーティー APM アラーム」セクションの「EventBridge イベントバス ARN」フィールドで、このカスタムイベントバスの ARN を AWS Incident Detection and Response に提供します。
3. オンボーディングプロセス中、AWS Incident Detection and Response は、このカスタムイベントバスにマネージド EventBridge ルールを作成して APM アラームを取り込みます。

オプション 2: 手動の統合

1. Amazon SNS コンソールを開き、`[apm_name]-sns` という名前の Amazon SNS の標準トピックを作成して、APM からアラームイベントを受け取ります。トピックタイプとして、(FIFO ではなく) 必ず [標準] を選択してください。作成された Amazon SNS トピックの ARN を書き留めます。
2. 次のいずれかを実行します。
   - (推奨) `[apm_name]-AWSIncidentDetectionResponse-EventBus` という名前の EventBridge カスタムイベントバスを作成します。
   - (代替方法) カスタムイベントバスの代わりにデフォルトの EventBridge イベントバスを使用します。

   AWS Incident Detection and Response は、`AWSServiceRoleForHealth_EventProcessor` SLR を介してカスタムイベントバスまたはデフォルトのイベントバスにマネージドルール (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) をインストールします。ルールソースはカスタムイベントバスまたはデフォルトのイベントバスとなり、ルールの送信先は AWS Incident Detection and Response となります。また、ルールはサードパーティーの APM イベントを取り込むパターンと一致します。
3. `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` という名前の Lambda 関数を作成して、SNS ペイロードを変換します。
   - 変換されたイベントは、「EventBridge で APM アラートを取り込むためのペイロード要件」で説明されているペイロード要件を満たしている必要があります。
   - Lambda 関数のターゲットを、ステップ 2 で作成したカスタムイベントバス (推奨) またはデフォルトのイベントバスに設定します。

4. SNS トピックを Lambda 関数 `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` のトリガーとして設定します。
   - [トリガーを追加] ページで「SNS」を検索します。
   - ステップ 1 で作成した専用 SNS トピックの ARN を追加します。
   - [追加] を選択します。
5. APM ドキュメントに従って、AWS Incident Detection and Response が取り込む必要がある APM ペイロードの SNS 送信先を設定します。

AWS Incident Detection and Response は、`AWSServiceRoleForHealth_EventProcessor` SLR を介してカスタムイベントバスまたはデフォルトのイベントバスにマネージドルール (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) をインストールします。ルールソースはカスタムイベントバスまたはデフォルトのイベントバスとなり、ルールの送信先は AWS Incident Detection and Response となります。また、ルールはサードパーティーの APM イベントを取り込むパターンと一致します。

アラームの最適化とモニタリングの調整

インシデント検出の最適な精度を確保するために、AWS のインシデント管理エンジニアが、重大なワークロードに対するアラームのパフォーマンスを継続的に評価します。推奨されるアラーム設定の変更が提供されるので、お客様はこれらの設定を行い、テクニカルアカウントマネージャー (TAM) とプロアクティブに協力して改善する必要があります。

顧客に対して対応する影響がないのにアラートがトリガーされる場合や、アラーム状態が頻繁に変動する場合など、アラームがビジネスクリティカルなオペレーションと整合していない可能性があることをモニタリングデータが示している場合は、重大でないアラームをオフボーディングし、ワークロードへの重大な影響をより適切に反映するアラームをオンボーディングすることをお勧めします。これにより、インシデント対応カバレッジの全体的な有効性を維持できます。

アラームの確認とフィードバック

AWS Incident Detection and Response は、モニタリングのためにアラームをオンボーディングする前に、アラームの包括的な確認を行います。アラームは、設定パラメータ、データ品質、アラートの有効性などの技術的な受け入れ基準に照らして評価されます。

この確認に基づいて、次の 2 種類のフィードバックが提供されます。

- 必須の設定要件 – アラームを受け入れるには、これらの変更を実装する必要があります。

- オプションの改善推奨事項 – これらの変更はアラームの有効性を向上させますが、アラームの受け入れに必須ではありません。

このフィードバックを受け取ったら、受け入れ済みのアラームとオプションの改善が必要なアラームのみをオンボーディングし、必須の設定要件があるアラームの設定変更を並行して進める決定ができます。

あるいは、本番稼働前にすべての変更を実装することもできます。このアプローチは、調整が必要なアラームの数に基づいて、オンボーディングのタイムラインを延長します。

アラームの本番稼働

アラームの取り込みが完了すると、AWS Incident Detection and Response はワークロードのモニタリングを有効にします。この時点以降、オンボーディングされたアラームはアクティブにモニタリングされ、オンボーディングされたアラームが [ALARM] 状態になると、AWS Incident Detection and Response はワークロードのランブックに応じてお客様をエンゲージします。

重要なアウトプット

- ワークロードはライブとして確認され、AWS Incident Detection and Response によってモニタリングされます。

次のステップ:

- オンボーディングされたアラームが想定どおりに AWS Incident Detection and Response をエンゲージすることを検証する方法については、「Incident Detection and Response でオンボードしたワークロードをテストする」を参照してください。
- オンボーディングされたアラーム、ランブック、またはワークロード情報を変更する方法については、「Incident Detection and Response でオンボードしたワークロードへの変更をリクエストする」を参照してください。

Incident Detection and Response でのワークロードのオンボーディングとアラーム取り込みのアンケート (例外パス)

> **Note**
>
> IDR CLI を使用してワークロードをオンボーディングできない場合は、ワークロードとアラームのオンボーディングに関する次のアンケートを使用します。

このトピックでは、ワークロードを AWS Incident Detection and Response にオンボーディングする場合と、サービスに取り込むアラームを設定する場合に、回答する必要があるアンケートについて説明します。ワークロードのオンボーディングに関するアンケートでは、ワークロード、アーキテクチャの詳細、インシデント対応の問い合わせに関する一般的な情報をカバーします。アラームの取り込みに関するアンケートでは、Incident Detection and Response でワークロードのインシデント作成をトリガーする重要なアラームと、誰に連絡すべきか、どのようなアクションを実行すべきかに関するランブック情報を指定します。アンケートへの適切な入力は、AWS ワークロードのモニタリングおよびインシデント対応プロセスを設定する重要なステップです。

ワークロードオンボーディングのアンケートをダウンロードします。

- 英語版
- 日本語版

アラーム取り込みのアンケートをダウンロードします。

- 英語版
- 日本語版

ワークロードオンボーディングのアンケート - 一般的な質問

一般的な質問

質問	レスポンスの例
エンタープライズ名	Amazon Inc.
このワークロードの名前 (略語を含む)	Amazon Retail Operations (ARO)

質問	レスポンスの例
プライマリエンドユーザーとこのワークロードの機能。	このワークロードは、エンドユーザーがさまざまなアイテムを購入できるようにする e コマースアプリケーションです。このワークロードは、弊社のビジネスの主要な収益源です。

ワークロードオンボーディングのアンケート - アーキテクチャに関する質問

アーキテクチャに関する質問

質問	レスポンスの例
このワークロードの一部であるリソースを定義するために使用される AWS リソースタグのリスト。AWS は、これらのタグを使用してこのワークロードのリソースを識別し、インシデント中のサポートを迅速化します。 **Note** タグでは、大文字と小文字が区別されます。複数のタグを指定する場合、このワークロードで使用されるすべてのリソースに同じタグが必要です。	appName: Optimax environment: Production
このワークロードで利用する AWS のサービス、およびそれらのサービスを利用する AWS アカウントと AWS リージョンのリスト。	AWS のサービス: Route 53、ALB、ECS、... アカウント: 123456789101、123456789102、... リージョン: US-EAST-1、US-WEST-2、...

アラーム取り込みのアンケート – 概要

アラーム取り込みのアンケートでは、AWS Incident Detection and Response をエンゲージするワークロードの重大なアラームと、それらのアラームがトリガーされたときにインシデント管理エンジニアがエンゲージする連絡先を指定します。

アラーム取り込みのアンケートは、以下のセクションに分かれています。

- 連絡先セクション: 最初に、アラームがトリガーされたときに AWS Incident Detection and Response で作成される サポート ケースに含める主な連絡先と、インシデントブリッジ用の任意の会議アプリケーションを指定します。ブリッジ設定が指定されていない場合、AWS Incident Detection and Response はインシデント中にインシデントブリッジを作成します。次に、主要な連絡先と連絡がつかない場合にエンゲージする、エスカレーション連絡先と時間間隔を指定します。最後に、インシデントの期間中、サポートケースを介してインシデントステータスの定期的な更新情報を受け取る連絡先を一覧表示します。
- アラームマトリクス: トリガーされたときに AWS Incident Detection and Response をエンゲージするアラームのセットを一覧表示します。オンボーディング用のアラームを選択するときは、AWS Incident Detection and Response で定義されている「重大なアラーム基準」を参照してください。詳細については、「アラームの定義」を参照してください。
  - Amazon CloudWatch アラーム (Amazon CloudWatch アラームがない場合はこのセクションを空白のままにします)
  - サードパーティーの APM アラーム (サードパーティーの APM アラームがない場合は、このセクションを空白のままにします)
    - EventBridge EventBus ARN: これは、EventBridge と直接統合されている APM からアラームを取り込む または EventBridge と直接統合していない APM からアラームを取り込む で作成したカスタム EventBus ARN の ARN です。
    - アラーム識別子: APM アラームのアカウント番号、リージョン、および名前を共有します。

アラーム取り込みのアンケート – ランブックの質問

ランブックに関する質問

質問	レスポンスの例
AWS は、サポート ケースを介してワークロードの連絡先をエンゲージします。このワーク	アプリケーションチーム app@example.com

質問	レスポンスの例
ロードでアラームがトリガーされた場合、主な連絡先は誰ですか。 優先する会議アプリケーションを指定すると、AWS はインシデント中にこれらの詳細をリクエストします。 Note 優先する会議アプリケーションが指定されていない場合、インシデント中に AWS が連絡を取り、参加できる Chime ブリッジを提供します。	+61 2 3456 7890
インシデント中に主な連絡先が利用できない場合は、希望する通信順序でエスカレーション連絡先とタイムラインを指定してください。	1. 10 分経過しても、主要連絡先から応答がない場合は、次の連絡先と連絡を取ります。 John Smith - アプリケーションスーパーバイザー john.smith@example.com +61 2 3456 7890 2. 10 分経過しても、John Smith から応答がない場合は、次の連絡先と連絡を取ります。 Jane Smith - オペレーションマネージャー jane.smith@example.com +61 2 3456 7890

アラームのマトリックス

ワークロードに代わってインシデントを作成するために AWS Incident Detection and Response をエンゲージする一連のアラームを特定するために、次の情報を提供します。AWS Incident Detection

and Response のエンジニアがアラームを確認すると、追加のオンボーディング手順が提供されます。

AWS Incident Detection and Response の重大なアラーム基準:

- AWS Incident Detection and Response のアラームは、オペレーターの即時対応を必要とするモニタリング対象のワークロードに、重大なビジネスへの影響 (収益の損失/カスタマーエクスペリエンスの低下) がある場合にのみ、「Alarm」状態に入る必要があります。
- AWS Incident Detection and Response のアラームは、ワークロードのリゾルバーを同時に、またはエンゲージメントの前に、エンゲージさせる必要もあります。AWSIncident Managers は、緩和プロセスでリゾルバーと連携しますが、エスカレーションする第一線の応答者としては機能しません。
- AWS Incident Detection and Response のアラームのしきい値は、アラームが発せられたときに調査が行われるように、適切なしきい値と期間に設定する必要があります。アラームが「Alarm」状態と「OK」状態の間で移動している場合、オペレータの応答と注意を必要とする十分な影響が発生しています。

基準違反の AWS Incident Detection and Response ポリシー:

これらの基準は、イベントが発生したときにケースバイケースでのみ評価できます。インシデント管理チームは、テクニカルアカウントマネージャー (TAM) と連携して、顧客のアラームがこの基準に準拠しておらず、一定の間隔で不必要にインシデント管理チームにエンゲージしていると疑われる場合、アラームを調整し、まれにモニタリングを無効にします。

> **Important**
>
> 連絡先アドレスを提供する際にグループ配布用の E メールアドレスを指定すると、ランブックを更新せずに受信者の追加と削除を制御できます。
> 最初のエンゲージメント E メールを送信した後に AWS Incident Detection and Response チームから電話をもらいたい場合は、サイト信頼性エンジニアリング (SRE) チームの連絡先電話番号を指定します。

CloudWatch アラームのアラームマトリックステーブル

CloudWatch アラーム ARN	このアラームの主要連絡先。	このアラームに最も関連性の高い AWS のサービスを指定して、適切なエンジニアをエ

	(ワークロードの主要連絡先と異なる場合)	ンゲージします。必要に応じて「N/A」と入力します。
例: arn:aws:cloudwatch:us-east-1:123456789012:alarm:ALB_5xx_Target_Response	例: Sam Smith – Application Manager sam.smith@example.com +61 2 3456 7890	例: ECS

サードパーティー APM アラームのアラームマトリックステーブル

EventBridge イベントバス ARN (これは、アラートを AWS Incident Detection and Response にルーティングするためのサードパーティー APM の統合の一部として作成されます)		例: (アカウント/リージョンの組み合わせごとにイベントバスがあります) arn:aws:events:us-east-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus arn:aws:events:us-west-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus	
アラーム識別子	このメトリクスが表す内容 このアラームが重要である理由	このアラームの主要連絡先。 (ワークロードの主要連絡先と異なる場合)	このアラームに最も関連性の高い AWS のサービス を指定して、適切なエンジニアをエンゲージします。必要に応じて「N/A」と入力します。
例:	例:	例:	例: ECS

ALB_5xx_Target_Response アカウント ID: 123456789012 リージョン: us-east-1	このメトリクスは、ALB の背後にあるターゲットからのトランザクション対応を表します。5XX エラーがしきい値を超えた場合、ビジネストランザクションの処理に対する重大な障害を表します。	Sam Smith – Application Manager sam.smith@example.com +61 2 3456 7890	

Incident Detection and Response でワークロードを管理する

効果的なインシデント管理で重要な部分は、モニタリング対象のワークロードのオンボーディング、テスト、維持に適したプロセスと手順を設定することです。このセクションでは、インシデント中にチームをガイドするための包括的なランブックと対応計画の作成、新しいワークロードの徹底したテストと検証、ワークロードのモニタリングを更新する変更のリクエスト、必要に応じたワークロードの適切なオフボーディングなど、重要なステップについて説明します。

トピック

Incident Detection and Response でインシデントに対応するためのランブックと対応計画を作成する

AWS Incident Detection and Response では、IDR CLI オンボーディングから取得した情報を使用して、ワークロードに影響するインシデントを管理するためのランブックを作成します。ランブックは、Incident Manager がインシデントに対応するときに実行するステップを文書化したものです。対応計画は、少なくとも 1 つのワークロードにマッピングされます。インシデント管理チームは、ワークロードのオンボーディングで提供された情報から、これらのテンプレートを作成します。

重要なアウトプット:

- AWS Incident Detection and Response に関するワークロードの定義を入力します。
- AWS Incident Detection and Response に関するアラームとランブックが完了します。

AWS Incident Detection and Response ランブックの例、aws-idr-runbook-example.zip をダウンロードすることもできます。

ランブックの例

Exampleランブックの例

説明

このドキュメントは、[CustomerName] – [WorkloadName] を対象としています。

ステップ: 優先

優先度アクション

1. 次のように、サポート ケースに関する最初の連絡をお客様に送信します。

```
Hello,

This is <<Engineer's name>> from AWS Incident Detection and Response. An alarm has
 triggered for your workload <<Application_Name>>. I am currently investigating and
 will update you in a few minutes once I have finished initial investigation.

Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
```

ステップ: 情報

エンゲージメント計画

このセクションでは、このランブックに適用されるエンゲージメントプランについて説明し、連絡先の詳細のみを示します。エンゲージメントプランは、ステップバイステップのコミュニケーション計画で参照されます。

- 初期エンゲージメント

  AWS Incident Detection and Response チームは、以下のカスタマーステークホルダーのアドレスを サポート ケースに追加します。AWS ステークホルダーは、問題の認識が必要になる可能性のある追加のステークホルダーを対象としています。

  - カスタマーステークホルダー: customeremail1、customeremail2、mobile1
  - AWS ステークホルダー: aws-idr-oncall@amazon.com、tam-team-email など
  - 1 回限りの連絡先: [これらは、最初のコミュニケーションにのみ含まれる E メールの連絡先です。最初のコミュニケーションが終了したら、これらの連絡先を削除します。これらの連絡先

は、すべての通信でページングしてはならない、pager-duty などのカスタマーページング用の E メールアドレスなどです。[優先] セクションの [コミュニケーション計画] に、[1 回限りの連絡先] が利用可能な場合にのみこれらを使用する方法に関する指示を明示的に追加します。]

- インシデントコールの設定

  お客様がブリッジを作成するために AWS Incident Detection and Response を必要とするかどうか、お客様が静的ブリッジを使用するかどうか、またはインシデントが開かれたときにお客様がブリッジを提供するかどうかを示します。

  (お客様の好みに基づいて 1 つのオプションを選択します)

  - AWS Incident Detection and Response で Amazon Chime/Zoom ブリッジを作成する
  - お客様が提供した静的ブリッジ
    - 会議番号: < 会議番号を挿入 >
  - お客様は、AWS Incident Detection and Response チームから送信されたコミュニケーションに応答して、すべてのインシデントのブリッジ詳細を提供します。
  - その他 – 詳細を指定します。
- エンゲージメントのエスカレーション

  初期エンゲージメントプランの連絡先がインシデントに応答しない場合、AWS Incident Detection and Response は次の連絡先に連絡します。

  エスカレーションする連絡先ごとに、サポート ケースに追加する、電話をかける、またはその両方を行う必要があるかどうかを指定します。

  - エスカレーションする前に、該当する場合、初期エンゲージメントの連絡先に連絡したことを確認してください。
  - 最初のエスカレーション連絡先: [escalationEmailAddress#1] / [PhoneNumber] – この連絡先にエスカレーションする前に XX 分待ちます。
    - この連絡先を [ケースに追加します/電話をかけます]。
  - 2 番目のエスカレーション連絡先: [escalationEmailAddress#2] / [PhoneNumber] – この連絡先にエスカレーションする前に XX 分待ちます。
    - この連絡先を [ケースに追加します/電話をかけます]。
  - その他

コミュニケーション計画

このセクションでは、インシデント管理エンジニアがインシデントコールおよびコミュニケーションチャネル外の指定されたステークホルダーとコミュニケーションを取る方法について説明します。

- 影響がある場合のコミュニケーション計画

  この計画は、AWS Incident Detection and Response が、アラートがお客様への潜在的な影響を示しているとトリアージステップから判断した場合に開始されます。

  AWS Incident Detection and Response は、「エンゲージメントプラン – インシデントコールの設定」に示されているように、事前に決められたブリッジへの参加をお客様にリクエストします

  ([1 回限りの連絡先] が利用可能かどうかに応じて 1 つ選択します)。

  1. [エンゲージメントプラン – 初期エンゲージメント] の [カスタマーステークホルダー] がケースの CC に追加されていることを確認します。

  OR

  1. [エンゲージメントプラン – 初期エンゲージメント] の [カスタマーステークホルダー] および [1 回限りの連絡先] がケースの CC に追加されていることを確認します。
  2. 次のテンプレートに基づいて、エンゲージメント通知をお客様に送信します。

     (1 つを選択します)

     影響がある場合のテンプレート – Amazon Chime ブリッジ

     ```
     The following alarm has engaged AWS Incident Detection and Response to an Incident
      bridge:
         Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
         Alarm State Change Reason - <insert_state_change_reason>
         Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
     Please join the Amazon Chime Bridge below so we can start the steps outlined in
      your Runbook:
         Amazon Chime Meeting ID: <insert_Meeting_ID_here>
         Link to Amazon Chime Bridge: <insert_Link_here>
         International dial-in numbers: https://chime.aws/dialinnumbers/
     ```

     影響がある場合のテンプレート – お客様が提供したブリッジ

     ```
     The following alarm has engaged AWS Incident Detection and Response:
         Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
         Alarm State Change Reason - <insert_state_change_reason>
     ```

```
    Alarm Start Time - <Example: 1 January 2025 3:30 PM UTC>
Please respond with your internal bridge details so we can join and start the steps
 outlined in your Runbook.
```

影響がある場合のテンプレート – お客様の静的なブリッジ

```
The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
    Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
Please join the Bridge below so we can start the steps outlined in your Runbook:
    Conference Number: <insert_conference_number>
    Conference URL: <insert_bridge_URL>
```

3. ケースを、保留中のカスタマーアクションに設定します。
4. 上記の、影響がある場合のコミュニケーションを送信した後、ケースから [1 回限りの連絡先]を削除します ([1 回限りの連絡先] が利用可能な場合)。
5. 上記の [エンゲージメントのエスカレーション] 計画に従います。
6. お客様が 30 分以内に応答しない場合は、アラームが回復するまで連絡を中止し、モニタリングを続行します。

- 影響がない場合のコミュニケーション計画

  この計画は、Incident Detection and Response が最初の [トリアージ] を完了する前にアラームが回復したときに開始されます。

  1. 影響がない場合の通知を送信する前に、[エンゲージメントプラン – 初期エンゲージメント] エンゲージメントプランに記載されている連絡先に基づいて、サポート ケースの CC からお客様の連絡先を検証し、削除または追加します。

     ["[1 回限りの連絡先] を追加しないでください。"] ([1 回限りの連絡先] が利用可能な場合に適用されます)
  2. 次のテンプレートに基づいて、エンゲージメントがない通知をお客様に送信します。

     影響がない場合のテンプレート

     ```
     AWS Incident Detection and Response received an alarm that has recovered for your
      workload.
         Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
         Alarm State Change Reason - <insert state change reason>
     ```

```
    Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
    Alarm End Time - <Example: 1 January 2025, 3:35 PM UTC>
This may indicate a brief customer impact that is currently not ongoing.
If there is an ongoing impact to your workload, please let us know and we will
 engage to assist.
```

3. ケースを、[保留中のカスタマーアクション] に設定します。
4. お客様が 30 分以内に応答しない場合は、ケースを解決します。

アプリケーションのアーキテクチャ概要

このセクションでは、インシデント管理エンジニアとオペレーションエンジニアが認識するアプリケーション/ワークロードアーキテクチャの概要を説明します。

- 主要なサービスがある AWS アカウントとリージョン – このアプリケーションをサポートするリージョンがある AWS アカウントのリスト。アプリケーションをサポートする、基盤となるインフラストラクチャの評価をエンジニアに支援します。
  - 123456789012
    - US–EAST–1 – 必要に応じて簡単な説明
      - Amazon EC2 – 必要に応じて簡単な説明
      - DynamoDB – 必要に応じて簡単な説明
      - その他
    - US–WEST–1 – 必要に応じて簡単な説明
      - その他
  - 別のアカウント
    - その他

Incident Detection and Response でオンボードしたワークロードをテストする

アラームの取り込みが完了すると、AWS Incident Detection and Response はワークロードのモニタリングを有効にし、稼働の確認を送信します。ワークロードはこの時点からアクティブにモニタリングされます。

アラームテストでは、オンボーディングされたアラームが想定どおりに AWS Incident Detection and Response をエンゲージし、適切なランブックをトリガーし、アラームの取り込み中に選択した場合のケース自動作成など、その他の必要なアクションが実行されることを検証します。

テストはオプションですが、強くお勧めします。お客様は実際のインシデントが発生する前に、対応策を検証する責任があります。

テストオプション

AWS Incident Detection and Response には 2 つのテストオプションがあります。

オプション 1: スケジュールされたゲームデー (推奨)

スケジュールされたゲームデーは、実際にインシデントが発生した場合に起きる可能性があることをライブかつエンドツーエンドでシミュレートします。AWS Incident Detection and Response は、実際のインシデントがどのように展開されるかに関するインサイトを提供するために、規定のランブックのステップに従います。ゲームデーは、エンゲージメントを向上させるために質問したり、指示を改良したりする機会です。

ゲームデーをスケジュールするには、次の手順を実行します。

1. 優先日とタイムゾーンを含む 1 時間の時間枠を使用して、AWS Incident Detection and Response に通知します。少なくとも 48 時間のリードタイムを設けます。
2. SRE/Ops チームやエスカレーション連絡先など、ゲームデーのリソースを計画します。

ゲームデーのスケジュール:

1. お客様と AWS Incident Detection and Response が通話に参加します。
2. 必要に応じて、アラームアクションを無効にします。
3. 「アラームをテストする方法」の手順を使用して、アラームを [ALARM] 状態に手動で設定します。
4. AWS Incident Detection and Response がアラーム通知の受け取りを確認します。
5. AWS Incident Detection and Response がアラームに応答し、ランブックに規定されたブリッジに参加します。
6. お客様と AWS Incident Detection and Response がゲームデーの結果を確認します。

オプション 2: オフラインアラームテスト

アラームは、コールをスケジュールしなくても、いつでも個別にテストできます。アラームをトリガーすると、実際のインシデント時と同様に、ランブックに従って AWS Incident Detection and Response がエンゲージされます。

オフラインアラームテストを実行するには、次の手順を実行します。

1. 意図しないアクションを防ぐには、Amazon CloudWatch アラームアクションを無効にします。
2. 「アラームをテストする方法」の手順を使用してアラームをトリガーします。
3. 5 分以内に、お客様に代わってサポートケースが作成され、AWS Incident Detection and Response がランブックで指定されているとおりにお客様をエンゲージします。
4. オフラインアラームテストを実行していることを Incident Manager に通知します。
5. Incident Manager は、受け取ったアラーム状態の変更を確認し、対応策を検証します。

サポートケースが 5 分以内に作成されない場合は、インシデントリクエストを送信して、トラブルシューティングのために AWS Incident Detection and Response を手動でエンゲージします。

アラームをテストする方法

Amazon CloudWatch アラーム

> **Note**
>
> アラームテストに使用する AWS Identity and Access Management ユーザーまたはロールには `cloudwatch:SetAlarmState` の権限が必要です。

AWS Command Line Interface または AWS CloudShell を使用して、アラームを [ALARM] 状態に手動で設定します。これらのコマンドは、ワークロードに影響を与えずにアラームの状態を変更します。

Amazon EC2 インスタンスの再起動などの意図しないアクションを防ぐには、アラーム状態を変更する前に CloudWatch のアラームアクションを無効にします。テストが完了したら、CloudWatch アラームアクションを再度有効にできます。アラームアクションの無効化または有効化の詳細については、「Amazon CloudWatch API リファレンス」の「DisableAlarmActions」および「EnableAlarmActions」を参照してください。

アラームアクションの無効化。

```
aws cloudwatch disable-alarm-actions --alarm-names "ExampleAlarm" --region us-east-1
```

アラーム状態を ALARM に設定します。

```
aws cloudwatch set-alarm-state --alarm-name "ExampleAlarm" --state-value ALARM --state-
reason "Testing AWS Incident Detection and Response" --region us-east-1
```

テスト後にアラームアクションを再度有効にします。

```
aws cloudwatch enable-alarm-actions --alarm-names "ExampleAlarm" --region us-east-1
```

アラーム状態は数秒以内に自動的に [OK] に戻ります。

複合アラーム

`set-alarm-state` コマンドは、複合アラームが [OK] 状態に戻ることを保証するものではありません。ベストプラクティスとして、テスト後に複合アラームの状態を検証します。複合アラームを手動でリセットするには、次のコマンドを使用します。

```
aws cloudwatch set-alarm-state --alarm-name "ExampleCompositeAlarm" --state-value OK --
state-reason "Testing AWS Incident Detection and Response" --region us-east-1
```

CloudWatch アラームの状態を手動で変更する方法の詳細については、「Amazon CloudWatch API リファレンス」の「SetAlarmState」を参照してください。

CloudWatch API オペレーションに必要なアクセス許可の詳細については、「Amazon CloudWatch の許可リファレンス」を参照してください。

サードパーティーの APM アラーム

Datadog、Splunk、New Relic、Dynatrace などのサードパーティーのアプリケーションパフォーマンスモニタリング (APM) ツールを使用するワークロードでは、アラームをシミュレートするためのさまざまな手順が必要です。

1. APM でアラームアクションを無効にして、意図しないアクションを防止してください。
2. アラームのしきい値または比較演算子を変更して、アラームを [ALARM] ステータスに強制します。これにより、AWS Incident Detection and Response へのペイロードがトリガーされます。

3. テストが完了したら、しきい値または比較演算子の変更をロールバックして、アラームを [OK] ステータスに復元します。

主な結果

テストが成功した後:

- アラームの取り込みが確認され、アラームも正しく設定されています。
- アラームは AWS Incident Detection and Response によって受け取られます。
- サポートケースが作成され、所定の連絡先に通知されます。
- AWS Incident Detection and Response は、所定の会議手段でお客様をエンゲージします。
- テスト中に生成されたすべてのアラームとサポートケースが解決されます。

よくある質問

アラームテストは必須ですか?

いいえ。テストはオプションですが、実際のインシデントが発生する前にエンドツーエンドの対応策を検証することを強くお勧めします。

ワークロードは影響を受けますか?

いいえ。ただし、テスト中にアラームに設定されているアラームアクションは、無効にしない限りトリガーされます。テスト前にアラームアクションを無効にして、意図しない影響を防止してください。

テスト中に通知されるのは誰ですか?

スケジュールされたゲームデー中は、検証のため、ランブック内のすべての連絡先とエスカレーションパスに対して連絡が行われます。オフラインアラームテスト中は、アラームのオンボーディング中に指定された最初の連絡先のみに通知されます。

ケースの更新に対して E メールで返信できますか?

いいえ。サポート ケース通信の E メールのコピーは、no-reply アドレスから送信されます。ケースを更新するには、AWS Support Center Console を使用してください。

本番稼働後にゲームデーをリクエストするにはどうすればよいですか?

既存のオンボーディングサポートケースが存在する場合は、そのケースに返信するか、Incident Detection and Response でオンボードしたワークロードへの変更をリクエストするを作成します。

Incident Detection and Response でオンボードしたワークロードへの変更をリクエストする

オンボーディングされたワークロードの変更をリクエストするには、次の手順を実行して、AWS Incident Detection and Response でサポートケースを作成します。

1. 次の例に示すように、AWS サポート センターに移動し、[ケースの作成] を選択します。

2. [技術] を選択します。
3. [サービス] で、[Incident Detection and Response] を選択します。
4. [カテゴリ] で、[ワークロードの変更リクエスト] を選択します。
5. [重要度] で、[一般的なガイダンス] を選択します。
6. この変更の [件名] を入力します。例えば、次のようになります。

   AWS Incident Detection and Response - *workload_name*
7. この変更の [説明] を入力します。例えば、「このリクエストは、AWS Incident Detection and Response にオンボーディングされた既存のワークロードを変更するためのものです」と入力します。リクエストには、次の情報が含まれていることを確認してください。

   - ワークロード名: ワークロードの名前。
   - アカウント ID: ID1、ID2、ID3 など。
   - 変更の詳細: リクエストした変更の詳細を入力します。
8. [追加の連絡先 - オプション] セクションに、この変更に関する連絡を受け取る E メール ID を入力します。

   次に示すのは、[追加の連絡先 - オプション] セクションの例です。

> **Important**
>
> [追加の連絡先 - オプション] セクションに E メール ID を追加しなかった場合、変更プロセスが遅れる可能性があります。

9. [Submit] を選択してください。

   変更リクエストを送信したら、組織から E メールを追加することができます。E メールを追加するには、次の例に示すように、[ケースの詳細] で [返信] を選択します。

   次に、[追加の連絡先 - オプション] セクションで、E メール ID を追加します。

   以下は、追加の E メールを入力できる場所を示す [返信] ページの例です。

Incident Detection and Response との連動によるアラームの抑制

オンボードされたワークロードアラームのうち、AWS Incident Detection and Response モニタリングと連動するものを指定し、一時的またはスケジュールに従って抑制します。例えば、計画的なメンテナンス中にワークロードアラームを一時的に抑制して、アラームが Incident Detection and Response と連動しないようにすることができます。または、毎日再起動アクティビティがある場合は、スケジュールに従ってアラームを抑制することもできます。Amazon CloudWatch などのアラームソースでアラームを抑制したり、ワークロード変更リクエストを送信したりできます。

トピック

- アラームソースでアラームを抑制
- ワークロード変更リクエストを送信してアラームを抑制
- チュートリアル: Metric Math 関数を使用してアラームを抑制
- チュートリアル: Metric Math 関数を削除してアラーム抑制を解除

アラームソースでアラームを抑制

アラームソースでアラームを抑制することで、Incident Detection and Response に連動するアラームと、連動するタイミングを指定します。

トピック

Metric Math 関数を使用して CloudWatch アラームを抑制

Amazon CloudWatch アラームの Incident Detection and Response モニタリングを抑制するには、Metric Math 関数を使用して、指定されたウィンドウ中に CloudWatch アラームが ALARM 状態に入らないようにします。

> **Note**
>
> CloudWatch のアラームで [アラームアクション] を無効にしても、Incident Detection and Response によるアラームのモニタリングは抑制されません。アラーム状態の変更は、CloudWatch のアラームアクションではなく Amazon EventBridge を介して取り込まれます。

Metric Math 関数を使用して CloudWatch アラームを抑制するには、次の手順を実行します。

1. AWS マネジメントコンソール にサインインして、CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. [アラーム] を選択し、Metric Math 関数を追加するアラームを見つけます。
3. [アクション] を選択してから、[編集] を選択して、アラームを変更します。
4. [メトリクスを編集] を選択して、アラームのメトリクスを変更します。
5. [数式の追加]、[空の式から開始] の順に選択します。
6. 数式を入力し、[適用] を選択します。
7. アラームがモニタリングした既存のメトリクスの選択を解除します。
8. 先ほど作成した式を選択し、その後 [メトリクスの選択] を選択します。
9. [プレビューと作成にスキップ] を選択します。
10. 変更内容を確認して、Metric Math 関数が期待どおりに適用されていることを確認し、[アラームの更新] を選択します。

Metric Math 関数を使用して CloudWatch アラームを抑制するステップバイステップの例については、「チュートリアル: Metric Math 関数を使用してアラームを抑制」を参照してください。

構文と利用可能な関数の詳細については、「Amazon CloudWatch ユーザーガイド」の「Metric Math 構文と関数」を参照してください。

Metric Math 関数を削除して CloudWatch アラーム抑制を解除

Metric Math 関数を削除して CloudWatch アラームの抑制を解除します。アラームから Metric Math 関数を削除するには、次の手順を実行します。

1. AWS マネジメントコンソール にサインインして、CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. [アラーム] を選択し、メトリクス数式を削除するアラームを見つけます。
3. Metric Math セクションで、[編集] を選択します。
4. アラームからメトリクスを削除するには、メトリクスの [編集] を選択し、メトリクス数式の横にある [x] ボタンを選択します。
5. 元のメトリクスを選択し、[メトリクスの選択] を選択します。
6. [プレビューと作成にスキップ] を選択します。
7. 変更内容を確認して、Metric Math 関数が期待どおりに適用されていることを確認し、[アラームの更新] を選択します。

Metric Math 関数と関連するユースケースの例

次の表は、Metric Math 関数の例と、関連するユースケース、各メトリクスコンポーネントの説明を示しています。

Metric Math 関数	ユースケース	説明
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	毎週火曜日の午前 1 時から午前 3 時 (UTC) までの期間中、実際のデータポイントを 0 に置き換えることでアラームを抑制します。	• DAY(m1) == 2: 火曜日 (月曜日 = 1、日曜日 = 7) であることを確認します。 • HOUR(m1) >= 1 && HOUR(m1) > 3: 午前 1 時から午前 3 時 (UTC) の時間範囲を指定します。

Metric Math 関数	ユースケース	説明
		• IF(condition, value_if_true, value_if_false): 条件が true の場合は、メトリクス値を 0 に置き換えます。それ以外の場合は、元の値 (m1) を返します。
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	毎日午後 11 時から午前 4 時 (UTC) までの期間中、実際のデータポイントを 0 に置き換えることでアラームを抑制します。	• HOUR(m1) >= 23: 23:00 (UTC) から始まる時間をキャプチャします。 • HOUR(m1) < 4: 04:00 (UTC) までの時間をキャプチャします (ただし、04:00 (UTC) は含まない)。 • ||: 論理 OR により、条件が深夜と早朝の 2 つの範囲で適用されるようにします。 • IF(condition, value_if_true, value_if_false): 指定された時間範囲内に 0 を返します。範囲外では元のメトリクス値 m1 を保持します。
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	毎日午前 11 時から午後 1 時 (UTC) までの期間中、実際のデータポイントを 0 に置き換えることでアラームを抑制します。	• HOUR(m1) >= 11 && HOUR(m1) < 13: 11:00 ~ 13:00 (UTC) の時間範囲をキャプチャします。 • IF(condition, value_if_true, value_if_false): 条件が true の場合 (例えば、時刻が 11:00 から 13:00 (UTC) の間)、0 を返します。条件が false の場合、元のメトリクス値 (m1) を保持します。

Metric Math 関数	ユースケース	説明
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	毎週火曜日の午前 1 時から午前 3 時 (UTC) までの期間中、実際のデータポイントを 99 に置き換えることでアラームを抑制します。	• DAY(m1) == 2: 火曜日 (月曜日 = 1、日曜日 = 7) であることを確認します。 • HOUR(m1) >= 1 && HOUR(m1) < 3: 午前 1 時から午前 3 時 (UTC) の時間範囲を指定します。 • IF(condition, value_if_true, value_if_false): 条件が true の場合は、メトリクス値を 99 に置き換えます。それ以外の場合は、元の値 (m1) を返します。
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	毎日午後 11 時から午前 4 時 (UTC) までの期間中、実際のデータポイントを 100 に置き換えることでアラームを抑制します。	• HOUR(m1) >= 23: 23:00 (UTC) から始まる時間をキャプチャします。 • HOUR(m1) < 4: 04:00 (UTC) までの時間をキャプチャします (ただし、04:00 (UTC) は含まない)。 • ||: 論理 OR により、条件が深夜と早朝の 2 つの範囲で適用されるようにします。 • IF(condition, value_if_true, value_if_false): 指定された時間範囲内に 100 を返します。範囲外では元のメトリクス値 m1 を保持します。

Metric Math 関数	ユースケース	説明
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	毎日午前 11 時から午後 1 時 (UTC) までの期間中、実際のデータポイントを 99 に置き換えることでアラームを抑制します。	• HOUR(m1) >= 11 && HOUR(m1) < 13: 11:00 ~ 13:00 (UTC) の時間範囲をキャプチャします。 • IF(condition, value_if_true, value_if_false): 条件が true の場合 (例えば、時刻が 11:00 から 13:00 (UTC) の間)、99 を返します。条件が false の場合、元のメトリクス値 (m1) を保持します。

サードパーティー APM からのアラームを抑制

アラームを抑制する方法については、サードパーティーの APM ベンダーのドキュメントを参照してください。サードパーティーの APM ベンダーの例としては、New Relic、Splunk、Dynatrace、Datadog、SumoLogic などがあります。

ワークロード変更リクエストを送信してアラームを抑制

前のセクションで説明したようにソースでアラームを抑制できない場合は、ワークロード変更リクエストを送信して、ワークロードのアラームの一部またはすべてのモニタリングを手動で抑制するように Incident Detection and Response に指示します。

ワークロード変更リクエストの作成方法の詳細については、「Incident Detection and Response でオンボードしたワークロードへの変更をリクエストする」を参照してください。ワークロード変更リクエストを発行してアラームの抑制をリクエストするときは、次の必須情報を必ず提供してください。

- ワークロード名: ワークロードの名前。
- アカウント ID: ID1、ID2、ID3 など。
- 変更の詳細: アラームの抑制
- 抑制開始時刻: 日付、時刻、タイムゾーン。
- 抑制終了時刻: 日付、時刻、タイムゾーン。

- 抑制するアラーム: 抑制する CloudWatch アラーム ARN またはサードパーティー APM イベント識別子のリスト。

アラーム抑制ワークロード変更リクエストを作成すると、Incident Detection and Response から次の通知を受け取ります。

- ワークロード変更リクエストの確認。
- アラームが抑制されたときの通知。
- モニタリングのためにアラームが再び有効になったときの通知。

チュートリアル: Metric Math 関数を使用してアラームを抑制

次のチュートリアルでは、Metric Math を使用して CloudWatch アラームを抑制する方法について説明します。

シナリオの例

次の火曜日の午前 1 時から午前 3 時 (UTC) までの間に予定されているアクティビティがあります。この時間帯の実際のデータポイントを 0 (設定されたしきい値を下回るデータポイント) に置き換える CloudWatch Metric Math 関数を作成します。

1. アラームをトリガーする基準を評価します。次のスクリーンショットは、アラーム基準の例を示しています。

   前のスクリーンショットに示したアラームは、Application Load Balancer ターゲットグループの `UnHealthyHostCount` メトリクスをモニタリングします。このアラームは、5 つのデータポイントのうち 5 つについて、`UnHealthyHostCount` メトリクスが 3 以上になると `ALARM` 状態になります。アラームは、欠落しているデータを不良 (設定されたしきい値に違反している) として扱います。
2. Metric Math 関数を作成します。

   この例では、予定されているアクティビティは、次の火曜日の午前 1 時から午前 3 時 (UTC) までの間に行われます。したがって、この時間帯の実際のデータポイントを 0 (設定されたしきい値を下回るデータポイント) に置き換える CloudWatch Metric Math 関数を作成します。

   設定する必要がある置換データポイントは、アラーム設定によって異なります。例えば、HTTP 成功率をモニタリングするアラームでしきい値が 98 未満の場合は、計画されたアクティビティ

中の実際のデータポイントを、設定されたしきい値である 100 を超える値に置き換えます。このシナリオの Metric Math 関数の例を次に示します。

```
IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)
```

上述の Metric Math 関数には、次の要素が含まれています。

- DAY(m1) == 2: 火曜日 (月曜日 = 1、日曜日 = 7) であることを確認します。
- HOUR(m1) >= 1 && HOUR(m1) < 3: 午前 1 時から午前 3 時 (UTC) の時間範囲を指定します。
- IF(condition, value_if_true, value_if_false): 条件が true の場合、関数はメトリクス値を 0 に置き換えます。それ以外の場合は、元の値 (m1) が返されます。

構文と利用可能な関数の詳細については、「Amazon CloudWatch ユーザーガイド」の「Metric Math 構文と関数」を参照してください。

3. AWS マネジメントコンソール にサインインして、CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
4. [アラーム] を選択し、Metric Math 関数を追加するアラームを見つけます。
5. Metric Math セクションで、[編集] を選択します。
6. [数式の追加]、[空の式から開始] の順に選択します。
7. 数式を入力し、[適用] を選択します。

   次の例に示すように、アラームがモニタリングする既存のメトリクスは自動的に [m1] になり、数式は [e1] になります。

8. (オプション) 次の例に示すように、メトリクス数式のラベルを編集して、その機能と作成理由を他のユーザーが理解できるようにします。

9. [m1] の選択を解除し、[e1] を選択してから、[メトリクスの選択] を選択します。これにより、基になるメトリクスを直接モニタリングする代わりに、数式をモニタリングするようにアラームが設定されます。
10. [プレビューと作成にスキップ] を選択します。
11. アラームが想定どおりに設定されていることを検証し、[アラームを更新して変更を保存] を選択します。

前の例では、Metric Math 関数が適用されていなければ、実際の UnHealthyHostCount メトリクスは計画されたアクティビティ中に報告されていたはずです。この結果、次の例に示すように、CloudWatch アラームが ALARM 状態になり、Incident Detection and Response が連動します。

Metric Math 関数を使用すると、実際のデータポイントがアクティビティ中は 0 に置き換えられ、アラームは OK 状態のままになり、Incident Detection and Response エンゲージメントの連動が抑制されます。

チュートリアル: Metric Math 関数を削除してアラーム抑制を解除

1 回限りのアクティビティに対して CloudWatch アラームを抑制する場合は、アクティビティの完了後にアラームから Metric Math 関数を削除して、アラームの定期的なモニタリングを再開します。例えば、毎週同じ曜日と時刻にインスタンスを再起動するパッチ適用ルーチンがスケジュールされている場合など、定期的なスケジュールでアラームを抑制するには、Metric Math 関数をそのままにしておきます。

次のチュートリアルでは、Metric Math 関数を削除して CloudWatch アラームの抑制を解除する方法について説明します。

1. AWS マネジメントコンソール にサインインして、CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. [アラーム] を選択し、Metric Math 関数を追加するアラームを見つけます。
3. Metric Math セクションで、[編集] を選択します。
4. アラームから抑制を削除するには、メトリクス数式の横にある [x] ボタンを選択します。
5. メトリクスを選択して実際のメトリクスのモニタリングを再開し、[メトリクスの選択] を選択します。
6. [プレビューと作成にスキップ] を選択します。
7. アラームが想定どおりに設定されていることを検証し、[アラームを更新して変更を保存] を選択します。

Incident Detection and Response からのワークロードのオフボード

AWS Incident Detection and Response からワークロードをオフボードするには、ワークロードごとに新しいサポートケースを作成します。サポートケースを作成する際は、次の点に注意してください。

- 1 つの AWS アカウントにあるワークロードをオフボードするには、ワークロードのアカウントまたは支払者アカウントからサポートケースを作成します。
- 複数の AWS アカウントにまたがるワークロードをオフボードするには、[支払者アカウント] からサポートケースを作成します。サポートケースの本文で、オフボードするすべてのアカウント ID を記載します。

> **Important**
>
> ワークロードをオフボードするサポートケースを作成するアカウントを間違えると、ワークロードをオフロードするまでに遅延が発生したり、追加情報が要求されたりする場合があります。

ワークロードをオフボードするリクエスト

1. AWS サポート センターに移動し、[ケースの作成] を選択します。
2. [技術] を選択します。
3. [サービス] で、[Incident Detection and Response] を選択します。
4. [カテゴリ] で、[ワークロードのオフボーディング] を選択します。
5. [重要度] で、[一般的なガイダンス] を選択します。
6. この変更の [件名] を入力します。例えば、次のようになります。

   [オフボード] AWS Incident Detection and Response - *workload_name*
7. この変更の [説明] を入力します。例えば、「このリクエストは AWS インシデント検出とレスポンスにオンボードされた既存のワークロードをオフボーディングするためのものです」と入力します。リクエストには、次の情報が含まれていることを確認してください。

   - ワークロード名: ワークロードの名前。
   - アカウント ID: ID1、ID2、ID3 など。
   - オフボーディングの理由: ワークロードをオフボーディングする理由を入力します。

8. [追加の連絡先 - オプション] セクションに、このオフボーディングのリクエストに関する連絡を受け取る E メール ID を入力します。
9. [Submit] を選択します。

AWS Incident Detection and Response のモニタリングとオブザーバビリティ

AWS Incident Detection and Response は、アプリケーションレイヤーから基盤となるインフラストラクチャまで、ワークロード全体のオブザーバビリティを定義するための専門的なガイダンスを提供します。モニタリングにより、何か問題があることがわかります。オブザーバビリティは、データ収集を使用して、何が問題で、なぜそれが発生したかを知らせます。

Incident Detection and Response システムは、Amazon CloudWatch や Amazon EventBridge などのネイティブ AWS のサービスを活用してワークロードに影響を与える可能性のあるイベントを検出することで、AWS ワークロードの障害やパフォーマンスの低下をモニタリングします。モニタリングは、差し迫った障害、進行中の障害、減少中の障害、潜在的な障害、またはパフォーマンスの低下を通知します。アカウントを Incident Detection and Response にオンボードするときは、Incident Detection and Response モニタリングシステムでモニタリングするアカウント内のアラームを選択し、それらのアラームをインシデント管理中に使用されるアプリケーションとランブックに関連付けます。

Incident Detection and Response では、Amazon CloudWatch やその他の AWS のサービスを使用してオブザーバビリティソリューションを構築します。AWS Incident Detection and Response は、次の 2 つの方法でオブザーバビリティをサポートします。

- ビジネス成果メトリクス: AWS Incident Detection and Response におけるオブザーバビリティは、ワークロードまたはエンドユーザーエクスペリエンスの成果をモニターする主要なメトリクスを定義することから始まります。AWS の専門家がお客様と協力し、ワークロードの目的、ユーザーエクスペリエンスに影響を与える可能性のある主要な出力または要因を理解し、これらの主要なメトリクスの低下をキャプチャするメトリクスとアラートを定義します。例えば、モバイル通話アプリケーションの主要なビジネスメトリクスは、通話セットアップの成功率 (ユーザー通話の成功率をモニタリング) であり、ウェブサイトの主要なメトリクスはページ速度です。インシデントエンゲージメントは、ビジネス成果メトリクスに基づいてトリガーされます。
- インフラストラクチャレベルのメトリクス: この段階では、アプリケーションをサポートする基盤となる AWS のサービスとインフラストラクチャを特定し、これらのインフラストラクチャサービスのパフォーマンスを追跡するためのメトリクスとアラームを定義します。これには、Application Load Balancer インスタンスの `ApplicationLoadBalancerErrorCount` などのメトリクスが含まれる場合があります。これは、ワークロードがオンボーディングされ、モニタリングがセットアップされた後に開始されます。

AWS Incident Detection and Response のオブザーバビリティの実装

オブザーバビリティは継続的なプロセスで、1 つの演習や時間枠では完了しない可能性があるため、AWS Incident Detection and Response では、次の 2 つのフェーズでオブザーバビリティを実装します。

- オンボーディングフェーズ: オンボーディング中のオブザーバビリティは、アプリケーションのビジネス成果が損なわれたときにそれを検出することに重点を置いています。このため、オンボーディングフェーズのオブザーバビリティは、アプリケーションレイヤーで主要なビジネス成果メトリクスを定義して、ワークロードの中断を AWS に通知することに重点を置いています。これにより、AWS はこのような中断に迅速に対応でき、復旧に役立ちます。これらのステップを自動化するために AWS Incident Detection and Response カスタマーコマンドラインインターフェイスを使用する方法の詳細については、「AWS Incident Detection and Response の CLI」を参照してください。
- オンボーディング後フェーズ: AWS Incident Detection and Response には、インフラストラクチャレベルのメトリクスの定義、メトリクスの調整、お客様の成熟度に応じたトレースとログの設定など、オブザーバビリティのためのプロアクティブサービスが多数用意されています。これらのサービスの実装には数か月かかる場合があり、複数のチームが関与する可能性があります。AWS Incident Detection and Response では、オブザーバビリティの設定に関するガイダンスを提供され、お客様はワークロード環境に必要な変更を実装する必要があります。オブザーバビリティ機能の実装に関する実践的なサポートが必要な場合は、テクニカルアカウントマネージャー (TAM) にリクエストしてください。

Incident Detection and Response によるインシデント管理

AWS Incident Detection and Response では、指定された Incident Manager のチームが提供する 24 時間 365 日のプロアクティブモニタリングとインシデント管理を利用できます。次の図は、アプリケーションアラームがインシデントをトリガーする際の標準インシデント管理プロセスの概要を示しています。アラーム生成、AWS Incident Manager エンゲージメント、インシデント解決、インシデント後レビューなどが含まれています。

1. アラーム生成: ワークロードでトリガーされたアラームは、Amazon EventBridge を介して AWS Incident Detection and Response にプッシュされます。AWS Incident Detection and Response は、アラームに関連付けられたランブックを自動的にプルし、Incident Manager に通知します。AWS Incident Detection and Response がモニタリングするアラームによって検出されない重大なインシデントがワークロードで発生した場合は、サポートケースを作成してインシデントへの対応をリクエストできます。インシデントへの対応のリクエストの詳細については、「インシデント対応をリクエストする」を参照してください。
2. AWS Incident Manager エンゲージメント: Incident Manager はアラームに応答し、カンファレンスコール、またはランブックで指定されているとおりにユーザーをエンゲージします。Incident Manager は、AWS のサービスの正常性を検証して、アラームがワークロードで使用される AWS のサービスの問題に関連しているかどうかを判断し、基盤となるサービスのステータスについてアドバイスします。必要に応じて、Incident Manager がユーザーに代わってケースを作成し、適切な AWS の専門家にサポートを依頼します。AWS Incident Detection and Response はアプリケーションに特化して AWS のサービス をモニタリングするため、AWS Incident Detection and Response は、AWS のサービス のイベントが宣言される前に、インシデントが AWS のサービスの問題に関連していると判断する場合があります。このシナリオでは、Incident Manager は AWS のサービス のステータスをアドバイスし、AWS のサービス のイベントインシデント管理フローをトリガーし、解決についてサービスチームにフォローアップします。提供された情報により、復旧計画や回避策を早期に実装して、AWS のサービス のイベントの影響を軽減できます。

   アラームがトリガーされてもすぐに復旧することがあります。このシナリオでは、Incident Manager は、アラームが回復したことを示すケースコレスポンデンスを送信しますが、ユーザーには連絡しません。ただし、アラームが 15 分以内に複数回トリガーされた場合、アラームが復旧した場合でも、Incident Manager はランブックの指示に従ってユーザーに連絡します。
3. インシデント解決: Incident Manager は、必要な AWS チーム全体でインシデントを調整し、インシデントが軽減または解決されるまで、適切な AWS の専門家と連携していることを確認します。

4. インシデント後レビュー (リクエストした場合): インシデント後、AWS Incident Detection and Response はリクエストに応じてインシデント後レビューを実行し、インシデント後レポートを生成できます。インシデント後レポートには、問題の説明、影響、エンゲージメントしたチーム、およびインシデントを軽減または解決するために取られた回避策またはアクションが含まれます。インシデント後レポートには、インシデントの再発の可能性を減らすため、または同様のインシデントの将来の発生の管理を改善するために使用できる情報が含まれている場合があります。インシデント後レポートは根本原因分析 (RCA) ではありません。インシデント後レポートに加えて RCA をリクエストできます。インシデント後レポートの例を次のセクションに示します。

> **Important**
>
> 以下のレポートテンプレートは一例です。

```
Post ** Incident ** Report ** Template
Post Incident Report - 0000000123
Customer: Example Customer
AWS #### case ID(s): 0000000000
Customer internal case ID (if provided): 1234567890
Incident start: 2023-02-04T03:25:00 UTC
Incident resolved: 2023-02-04T04:27:00 UTC
Total Incident time: 1:02:00 s
Source Alarm ARN: arn:aws:cloudwatch:us-east-1:000000000000:alarm:alarm-prod-workload-
impaired-useast1-P95

Problem Statement:
Outlines impact to end users and operational infrastructure impact.
 Starting at 2023-02-04T03:25:00 UTC, the customer experienced a large scale outage
 of their workload that lasted one hour and two minutes and spanning across all
 Availability Zones where the application is deployed. During impact, end users were
 unable to connect to the workload's Application Load Balancers (ALBs) which service
 inbound communications to the application.

Incident Summary:

Summary of the incident in chronological order and steps taken by AWS Incident Managers
 to direct the incident to a path to mitigation.
  At 2023-02-04T03:25:00 UTC, the workload impairments alarm triggered a critical
 incident for the workload. AWS Incident Detection and Response Managers responded to
 the alarm, checking AWS service health and steps outlined in the workload’s runbook.
```

```
 At 2023-02-04T03:28:00 UTC, ** per the runbook, the alarm had not recovered and the
Incident Management team sent the engagement email to the customer's Site Reliability
Team (SRE) team, created a troubleshooting bridge, and an #### support case on behalf
of the customer.
 At 2023-02-04T03:32:00 UTC, ** the customer's SRE team, and #### Engineering joined
the bridge. The Incident Manager confirmed there was no on-going AWS impact to
services the workload depends on. The investigation shifted to the specific resources
in the customer account.
 At 2023-02-04T03:45:00 UTC, the Cloud Support Engineer discovered a sudden increase
in traffic volume was causing a drop in connections. The customer confirmed this
ALB was newly provisioned to handle an increase in workload traffic for an on-going
promotional event.
 At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry logic. The
Incident Manager worked with the Cloud Support Engineer to raise an escalation a
higher support level to quickly scale the ALB per the runbook.
 At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activities. The
back-off/retry logic yields mild recovery but timeouts are still being seen for some
clients.
By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alarms return to
pre-incident levels. Connection timeouts subside.
 At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, after 10 minutes
of recovery monitoring. Full mitigation is agreed upon between AWS and the customer.

Mitigation:
Describes what was done to mitigate the issue. NOTE: this is not a Root Cause Analysis
 (RCA).
  Back-off and retries yielded mild recovery. Full mitigation happened after escalation
 to ALB support team (per runbook) to scale the newly provisioned ALB.

Follow up action items (if any):
Action items to be reviewed with your Technical Account Manager (TAM), if required.
Review alarm thresholds to engage AWS Incident Detection and Response closer to the
 time of impact.
Work with AWS #### and TAM team to ensure newly created ALBs are pre-scaled to
 accommodate expected spikes in workload traffic.
```

トピック

- アプリケーションチームの AWS Support Center Consoleへのアクセス権をプロビジョニングする
- インシデント対応をリクエストする
- AWS Support App in Slack で Incident Detection and Response のサポートケースを管理する

アプリケーションチームの AWS Support Center Consoleへのアクセス権をプロビジョニングする

AWS Incident Detection and Response は、インシデントのライフサイクル中に サポート ケースを通じて通信します。Incident Manager に対応するには、チームは サポート センターにアクセスできる必要があります。

アクセスのプロビジョニングの詳細については、「サポート ユーザーガイド」の「サポート センターへのアクセスの管理」を参照してください。

インシデント対応をリクエストする

ワークロードで重大なインシデントが発生しても、AWS Incident Detection and Response でモニタリングしているアラームで検出されなかった場合は、サポートケースを作成してインシデント対応をリクエストできます。オンボーディング中のワークロードを含め、AWS Incident Detection and Response にサブスクライブしているワークロードに関するインシデント対応は、AWS Support Center Console、AWS サポート API、または AWS Support App in Slack を使用してリクエストできます。

次の図は、Incident Detection and Response チームにインシデント支援をリクエストした AWS のお客様のエンドツーエンドのワークフローを示しています。最初のリクエストから調査、緩和、解決までのステップが詳しく示されています。

ワークロードに影響しているアクティブなインシデントのインシデント対応をリクエストするには、サポート ケースを作成します。サポートケースを作成すると、AWS Incident Detection and Response は、ワークロードの復旧を加速するために必要な、AWS の専門家とのカンファレンスブリッジにお客様をつなぎます。

AWS Support Center Console を使用してインシデント対応をリクエストする

インシデント対応をリクエストするには、次の手順を実行します。

1. AWS Support Center Console を開き、新しいサポートケースを作成します。
2. [件名] に、インシデントの簡単な概要を入力します。例えば、`AWS Incident Detection and Response - Active Incident - workload_name`。

3. [説明] に、インシデントの詳細を入力します。サポートケースには、次の詳細を含めることをお勧めします。

   - 影響を受ける AWS リソース ARN、ワークロード名、およびその関数
   - ビジネスへの影響の説明
   - (オプション) 任意の会議ブリッジ URL。ブリッジの詳細を指定しない場合、AWS Incident Detection and Response は AWS 会議ブリッジを作成し、ブリッジの URL を含む招待を送信します。

4. (オプション) スクリーンショットやログの抜粋など、インシデントの説明に役立つファイルを添付します。
5. 次のケース分類フィールドを設定します。

   - ケースタイプ: テクニカル
   - サービス: Incident Detection and Response
   - カテゴリ: アクティブなインシデント
   - 重要度: ビジネスクリティカルなシステム停止

6. 影響を受ける AWS のサービス、影響を受ける AWS リージョン、ビジネスへの影響、影響の開始時間、影響を受けるリソースなど、AWS Incident Detection and Response が AWS のエキスパートをより迅速にエンゲージできるように、追加のコンテキストを提供します。
7. [Submit] を選択してください。
8. AWS Incident Detection and Response は 5 分以内にケースを確認し、適切な AWS の専門家とカンファレンスブリッジに参加します。

AWS サポート API を使用してインシデント対応をリクエストする

サポートケースは、AWS サポート API を使用してプログラムで作成できます。詳細については、「AWS サポート ユーザーガイド」の「AWS サポート API について」を参照してください。

AWS Support App in Slack を使用してインシデント対応をリクエストする

AWS Support App in Slack を使用してインシデント対応をリクエストするには、次の手順を実行します。

1. AWS Support App in Slack を設定した Slack チャネルを開きます。
2. 次のコマンドを入力します。

```
/awssupport create
```

3. このインシデントの [件名] を入力します。AWS Incident Detection and Response - アクティブなインシデント - workload_name を入力します。
4. このインシデントの [問題の説明] を入力します。次の詳細情報を入力します。

   技術情報:

   影響を受けるサービス:

   影響を受けるリソース:

   影響を受けるリージョン:

   ワークロード名:

   ビジネス情報:

   ビジネスへの影響の説明:

   [オプション] カスタマーブリッジの詳細:
5. [次へ] を選択します。

6. [問題のタイプ] で、[テクニカルサポート] を選択します。
7. [サービス] で、[インシデントの検出と対応] を選択します。
8. [カテゴリ] で、[アクティブインシデント] を選択します。
9. [重要度] で、[ビジネスクリティカルなシステムのダウン] を選択します。

10. オプションで、[通知する追加の連絡先] フィールドに最大 10 件の追加の連絡先をカンマで区切って入力します。これらの追加の連絡先は、このインシデントに関する E メール連絡のコピーを受信します。

11. [Review] (レビュー) を選択します。
12. 自分にのみ表示される新しいメッセージが Slack チャネルに表示されます。ケースの詳細を確認し、[ケースを作成] を選択します。

13.ケース ID は、AWS Support App in Slack からの新しいメッセージで提供されます。

14.Incident Detection and Response は 5 分以内にケースを確認し、適切な AWS の専門家とのカンファレンスブリッジにつなげます。

15.Incident Detection and Response からの連絡が、ケースのスレッドで更新されます。

AWS Support App in Slack で Incident Detection and Response のサポートケースを管理する

AWS Support App in Slack を使用すると、Slack での サポート ケースの管理、AWS Incident Detection and Response ワークロードでの新しいアラームによって開始されたインシデントに関する通知の受信、インシデント応答リクエストの作成ができます。

AWS Support App in Slack を設定するには、「サポート ユーザーガイド」に示されている手順に従ってください。

> **Important**
>
> - ワークロードでのすべてのアラームによって開始されたインシデントの通知を Slack で受信するには、AWS Incident Detection and Response にオンボードしたワークロードのすべてのアカウントで AWS Support App in Slack を設定する必要があります。サポートケースは、ワークロードアラームが発生したアカウントで作成します。
> - インシデント時にユーザーに代わって複数の重要度の高いサポートケースを開いて、サポート リゾルバーをエンゲージできます。Slack チャネルの通知設定に一致する、インシデント中に開いたすべてのサポートケースに関する通知を Slack で受け取ります。
> - AWS Support App in Slack を通じて受信した通知は、インシデント中に AWS Incident Detection and Response で E メールまたは電話を介してエンゲージしたワークロードの初回連絡先とエスカレーション連絡先を置き換えるものではありません。

トピック

- Slack でのアラームによって開始されたインシデントの通知
- Slack でインシデント対応リクエストを作成する

Slack でのアラームによって開始されたインシデントの通知

Slack チャネルで AWS Support App in Slack を設定すると、AWS Incident Detection and Response でモニタリングしているワークロードでのアラームによって開始されたインシデントの通知を受け取ります。

次の例は、アラームによって開始されたインシデントの通知が Slack にどのように表示されるかを示しています。

通知の例

アラームによって開始されたインシデントが AWS Incident Detection and Response によって確認されると、次のような通知が Slack で生成されます。

AWS Incident Detection and Response によって追加された完全な連絡内容を表示するには、[詳細を表示] を選択します。

AWS Incident Detection and Response からの以降の更新はケースのスレッドに表示されます。

[詳細を表示] を選択して、AWS Incident Detection and Response によって追加された連絡内容の全文を表示します。

Slack でインシデント対応リクエストを作成する

AWS Support App in Slack でインシデント対応リクエストを作成する手順については、「インシデント対応をリクエストする」を参照してください。

Incident Detection and Response でのレポート作成

AWS Incident Detection and Response では、サービスの設定方法、インシデントの履歴、Incident Detection and Response サービスのパフォーマンスを、それぞれ理解するのに役立つ運用データとパフォーマンスデータを提供しています。このページでは、設定データ、インシデントデータ、パフォーマンスデータなど、使用可能なデータの種類について説明します。

設定データ

- オンボーディングされたすべてのアカウント
- すべてのアプリケーションの名前
- 各アプリケーションに関連付けられたアラーム、ランブック、サポートプロファイル

インシデントデータ

- 各アプリケーションにおけるインシデントの日付、数、期間
- 特定のアラームに関連するインシデントの日付、数、期間
- インシデント後レポート

パフォーマンスデータ

- サービスレベル目標 (SLO) のパフォーマンス

必要な運用データおよびパフォーマンスデータについては、テクニカルアカウントマネージャーにお問い合わせください。

Incident Detection and Response のセキュリティと回復性

サポート でのデータ保護には、AWS 責任共有モデルが適用されます。このモデルで説明されているように、「AWS」 は、「AWS クラウド」 のすべてを実行するグローバルインフラストラクチャを保護する責任があります。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。このコンテンツには、使用される AWS のサービス のセキュリティ設定と管理タスクが含まれます。

データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。

欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿されたAWS 責任共有モデルおよび GDPR のブログを参照してください。

データ保護の目的で、AWS アカウントの認証情報を保護し、個々のユーザーアカウントを AWS Identity and Access Management (IAM) で設定することをお勧めします。この方法により、それぞれの職務を遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、次の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- Secure Sockets Layer/Transport Layer Security (SSL/TLS) 証明書を使用して AWS リソースと通信します。TLS 1.2 以降が推奨されます。詳細については、「SSL/TLS 証明書とは何ですか?」を参照してください。
- AWS CloudTrail で API とユーザーアクティビティロギングを設定します。詳細については、AWS CloudTrail を参照してください。
- AWS のサービス 内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- Amazon Macie などのアドバンストマネージドセキュリティサービスを使用します。これは、Amazon S3 に保存されている個人データの検出と保護を支援します。Amazon Macie に関する情報については、「Amazon Macie」を参照してください。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 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 エンドポイントの情報については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

顧客の E メールアドレスなどの機密情報やセンシティブ情報は、タグや [名前] フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これは、コンソール、API、AWS CLI、または AWS SDK で サポート または他の AWS のサービスを使用する場合も同様です。タグまたは名前に使用する自由記入欄に入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへ URL を供給する場合は、そのサーバーへのリクエストを検証するために、認証情報を URL に含めないことを強くお勧めします。

AWS Incident Detection and Response によるアカウントへのアクセス

AWS Identity and Access Management (IAM) は、AWS リソースへのアクセスを安全に管理するためのウェブサービスです。IAM を使用して、誰を認証 (サインイン) し、誰にリソースの使用を認可する (アクセス許可を付与する) かを制御します。

AWS Incident Detection and Response およびアラームデータ

デフォルトでは、Incident Detection and Response は、アカウント内のすべての CloudWatch アラームの Amazon リソースネーム (ARN) と状態を受信し、オンボーディングされたアラームが ALARM 状態に変わったときにインシデント検出と対応プロセスを開始します。Incident Detection and Response がアカウントから受け取るアラームに関する情報をカスタマイズする場合は、テクニカルアカウントマネージャーにお問い合わせください。

ドキュメント履歴

以下の表に、IDR ガイドの前回のリリース以降に行われた重要な変更を示します。

変更	説明	日付
APM の統合における Amazon SNS の標準トピックについて明確化	サードパーティーの APM アラームを AWS Incident Detection and Response と統合する場合に、お客様が (FIFO ではなく) Amazon Simple Notification Service の標準トピックを作成する必要があることを明確化しました。 詳細については、「Amazon SNS を直接統合した APM からアラームを取り込む」を参照してください。	2026 年 5 月 26 日
ゲームデーのオプション化、オンボーディングアンケートの簡素化、およびランブック開発の更新	アラームテスト (ゲームデー) を更新し、稼働後のオプションとしました。これには、スケジュールされたゲームデーまたはオフラインアラームテストの 2 つのテストオプションがあります。ワークロードオンボーディングとアラームの取り込みのアンケートを簡略化しました。ランブックの開発を更新し、AWS Systems Manager ドキュメントへの参照を削除しました。 詳細については、Incident Detection and Response でオンボードしたワークロードをテストする、Incident Detection and Response でのワークロードのオンボーディングとアラーム取り込みのアンケート (例外パス)、および Incident Detection and Response でインシデントに対応するためのランブックと対応計画を作成する を参照してください。	2026 年 5 月 26 日
インシデント対応をリクエストする手順を更新	現在の AWS Support Center Console UI と一致するようにインシデント対応をリクエストする	2026 年 5 月 12 日

変更	説明	日付
	手順を更新し、ブリッジ URL のガイダンスを追加して、古いスクリーンショットを削除しました。 詳細については、「AWS Support Center Console を使用してインシデント対応をリクエストする」を参照してください。	
CLI ファーストアプローチへのオンボーディングを更新	「開始方法」の章を更新して、AWS Incident Detection and Response カスタマーコマンドラインインターフェイスを主要なボーディング方法として昇格させ、デフォルトのオンボーディングパスとしてのワークロードオンボーディングのアンケートとアラーム取り込みのアンケートを廃止しました。アンケートは、IDR CLI を使用できないお客様に対する特例のオプションとして、引き続き利用可能になっています。 詳細については、「Incident Detection and Response へのワークロードのオンボード」および「アラームの取り込み」を参照してください。	2026 年 5 月 12 日
日本語アンケートのリンクを追加	ワークロードオンボーディングとアラーム取り込みのアンケートの日本語ダウンロードリンクを追加しました。 詳細については、「Incident Detection and Response でのワークロードのオンボーディングとアラーム取り込みのアンケート (例外パス)」を参照してください。	2026 年 4 月 20 日

変更	説明	日付
アーキテクチャリファレンスを更新	アーキテクチャ図への参照を削除し、アーキテクチャの詳細に置き換えました。 詳細については、「Incident Detection and Response のアーキテクチャ」および「Incident Detection and Response でのワークロードについて」を参照してください。	March 31, 2026
Incident Detection and Response にオンボードされたワークロードのテストを更新	テスト中にアラーム状態を変更する前に CloudWatch アラームアクションを無効にする方法に関する情報を追加しました。 詳細については、「Incident Detection and Response でオンボードしたワークロードをテストする」を参照してください。	2026 年 3 月 2 日
Incident Detection and Response によるインシデント管理を更新	アラーム動作の繰り返しとインシデントマネージャーの関与に関する情報を追加しました。 詳細については、「Incident Detection and Response によるインシデント管理」を参照してください。	2026 年 3 月 2 日
Metric Math 関数を使用して CloudWatch アラームを抑制するセクションの手順を更新	Metric Math 関数を使用して CloudWatch アラームを抑制するセクションの手順を更新しました。 詳細については、「アラームソースでアラームを抑制」を参照してください。	2026 年 2 月 3 日
サポートされている言語として韓国語を追加	サポートされている言語として韓国語を追加しました。 詳細については、「Incident Detection and Response が利用可能なリージョン」を参照してください。	2026 年 1 月 22 日

変更	説明	日付
サポートされている言語として標準中国語を追加	サポートされている言語として標準中国語を追加しました。 詳細については、「Incident Detection and Response が利用可能なリージョン」を参照してください。	2026 年 1 月 13 日
新しいセクション「AWS Incident Detection and Response カスタマーコマンドラインインターフェイス」を追加	IDR CLI セクションを追加し、「開始方法」の章を更新して AWS Incident Detection and Response カスタマーコマンドラインインターフェイスに関する情報を追加しました。 詳細については、「CLI for AWS Incident Detection and Response」を参照してください。	2025 年 12 月 8 日
更新済みのセクション: Incident Detection and Response のワークロードのオンボーディングとアラームの取り込みに関するアンケートおよび Incident Detection and Response を開始する	AWS のサービス イベント処理プロセスは、AWS Incident Detection and Response の一部ではなくなりました。このユーザーガイドのセクションが更新され、このプロセスへの参照が削除されました。AWS Service Health Dashboard を通じて、引き続きサービスイベント通知を受け取ります。AWS Incident Detection and Response のお客様は、インシデント対応リクエストを使用して、必要に応じてサービスイベント中にサポートを受けることができます。詳細については、「インシデント対応をリクエストする」を参照してください。	2025 年 10 月 14 日

変更	説明	日付
「サービスイベントのインシデント管理」セクションを削除しました。	AWS のサービス イベント処理プロセスは、AWS Incident Detection and Response の一部ではなくなりました。ユーザーガイドのこのセクションは、この変更を反映するために削除されました。AWS Service Health Dashboard を通じて、引き続きサービスイベント通知を受け取ります。AWS Incident Detection and Response のお客様は、インシデント対応リクエストを使用して、必要に応じてサービスイベント中にサポートを受けることができます。詳細については、「インシデント対応をリクエストする」を参照してください。	2025 年 10 月 14 日
更新済みのセクション: Incident Detection and Response が利用可能なリージョン	AWS Incident Detection and Response が AWS GovCloud (米国東部) および AWS GovCloud (米国西部) で利用可能になりました。詳細については、Incident Detection and Response が利用可能なリージョンを参照してください。	2025 年 10 月 5 日
更新済みのセクション: Incident Detection and Response のワークロードのオンボーディングとアラームの取り込みに関するアンケート	アラームのマトリクステーブルのサンプル E メールアドレスを更新しました。	2025 年 8 月 26 日
更新したセクション: ワークロードを AWS Incident Detection and Response にサブスクライブする	[ケースを作成] ウィンドウの [説明] セクションで、[サブスクリプション開始日] フィールドへの参照を削除しました。 更新したセクション: ワークロードを AWS Incident Detection and Response にサブスクライブする	2025 年 8 月 4 日

変更	説明	日付
新しい機能: Incident Detection and Response との連動によるアラームの抑制	[マネージドワークロード] に、アラームを一時的またはスケジュールに従って抑制する方法に関する情報を提供する新しいセクションを追加しました。 新規セクション: Incident Detection and Response との連動によるアラームの抑制	2025 年 4 月 9 日
AWS Support Center Console を使用してインシデント対応をリクエストする手順を更新	[問題の説明] フィールドに入力する情報の詳細を追加しました。 更新済みのセクション: インシデント対応をリクエストする	2025 年 2 月 6 日
他の AWS リージョンの追加	「Incident Detection and Response が利用可能なリージョン」セクションに他の AWS リージョンが追加されました。 更新済みのセクション: Incident Detection and Response が利用可能なリージョン	2024 年 11 月 1 日
「AWS Support App in Slack で Incident Detection and Response のサポートケースを管理する」ページの更新	「インシデント管理」ページを移動して、テキストを改訂し、スクリーンショットを置き換えました。 更新済みのセクション: AWS Support App in Slack で Incident Detection and Response のサポートケースを管理する	2024 年 10 月 10 日
AWS Support App in Slack の新しいページを追加 AWS Incident Detection and Response によるインシデント管理を更新	AWS Support App in Slack の新しいページを追加 AWS Incident Detection and Response によるインシデント管理を更新し、新しいセクション「AWS Support App in Slack を使用してインシデント対応をリクエストする」を追加しました。	2024 年 9 月 10 日

変更	説明	日付
アカウントのサブスクリプションの更新	「アカウントのサブスクリプション」セクションを更新し、アカウントのサブスクライブをリクエストしたときにサポートケースを開く場所の詳細を追加しました。 更新したセクション: ワークロードを AWS Incident Detection and Response にサブスクライブする	2024 年 6 月 12 日
新しいセクションを追加: ワークロードのオフボード	「ワークロードのオフボード」セクションを「開始方法」に追加し、ワークロードのオフボードに関する情報を追加しました。 詳細については、「Incident Detection and Response からのワークロードのオフボード」を参照してください。	2024 年 3 月 28 日
アカウントのサブスクリプションの更新	「アカウントのサブスクリプション」セクションを更新し、ワークロードのオフボードに関する情報を追加しました。 詳細については、「ワークロードを AWS Incident Detection and Response にサブスクライブする」を参照してください。	2024 年 3 月 28 日
テストの更新	「テスト」セクションを更新し、オンボーディングプロセスの最後の手順として障害対応テストに関する情報を追加しました。 更新済みのセクション: Incident Detection and Response でオンボードしたワークロードをテストする	2024 年 2 月 29 日

変更	説明	日付
AWS Incident Detection and Response とはの更新	「AWS Incident Detection and Response とは」セクションを更新しました。 更新済みのセクション: AWS Incident Detection and Response とは	2024 年 2 月 19 日
アンケートセクションの更新	ワークロードオンボーディングのアンケートを更新し、アラームの取り込みのアンケートを追加しました。セクションの名前を「オンボーディングのアンケート」から「ワークロードオンボーディングとアラームの取り込みのアンケート」に変更しました。	2024 年 2 月 2 日
AWS のサービスイベントとオンボーディング情報の更新	いくつかのセクションを更新し、オンボーディングに関する新しい情報を追加しました。 更新済みのセクション: • Incident Detection and Response へのワークロードのオンボード • ワークロードを AWS Incident Detection and Response にサブスクライブする 新規セクション • アプリケーションチームの AWS Support Center Consoleへのアクセス権をプロビジョニングする	2024 年 1 月 31 日
関連情報セクションの追加	「アクセスプロビジョニング」に「関連情報」セクションを追加しました。 更新済みのセクション: Incident Detection and Response にアラームを取り込むためのアクセスをプロビジョニングする	2024 年 1 月 17 日

変更	説明	日付
更新された手順の例	「例: Datadog と Splunk からの通知の統合」の手順 2、3、4 のプロセスを更新しました。 更新されたセクション: 例: Datadog と Splunk からの通知の統合	2023 年 12 月 21 日
紹介グラフィックとテキストの更新	「Amazon EventBridge と直接統合されている APM からアラームを取り込む」のグラフィックを更新しました。 更新済みのセクション: Incident Detection and Response でインシデントに対応するためのランブックと対応計画を作成する	2023 年 12 月 21 日
ランブックテンプレートの更新	「AWS Incident Detection and Response のランブックの開発」のランブックテンプレートを更新しました。 更新済みのセクション: Incident Detection and Response でインシデントに対応するためのランブックと対応計画を作成する	2023 年 12 月 4 日
アラーム設定の更新	アラーム設定を更新し、CloudWatch のアラーム設定に関する詳細情報を含めました。 新しいセクション: Incident Detection and Response でビジネスニーズに合った CloudWatch アラームを作成する 新しいセクション: CloudFormation テンプレートを使用して Incident Detection and Response で CloudWatch アラームを作成する 新しいセクション: Incident Detection and Response における CloudWatch アラームのユースケースの例	2023 年 9 月 28 日

変更	説明	日付
開始方法の更新	ワークロード変更リクエストの開始方法に関する情報を更新しました。 新規セクション: Incident Detection and Response でオンボードしたワークロードへの変更をリクエストする 更新したセクション: ワークロードを AWS Incident Detection and Response にサブスクライブする	2023 年 9 月 5 日
「開始方法」の新しいセクション	AWS Incident Detection and Response に アラートの取り込みを追加しました。	2023 年 6 月 30 日
元のドキュメント	AWS Incident Detection and Response の初回発行	2023 年 3 月 15 日