aws

ユーザーガイド

Incident Manager

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Incident Manager: ユーザーガイド

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

AWS Systems Manager Incident Manager とは? 1
主なコンポーネントと機能 1
Incident Manager を使用する利点 3
関連サービス 5
Incident Manager へのアクセス 5
Incident Manager のリージョンとクォータ 5
Incident Manager の価格 5
インシデントライフサイクル 6
アラートとエンゲージメント 7
トリアージ 8
調査と緩和 9
インシデント後分析 10
設定 11
にサインアップする AWS アカウント 11
管理アクセスを持つユーザーを作成する 12
プログラム的なアクセス権を付与する 13
Incident Manager のセットアップに必要なロール 14
はじめに 15
前提条件 15
準備ウィザード 15
クロスリージョンおよびクロスアカウントのインシデント管理 22
クロスリージョンのインシデント管理 22
クロスアカウントインシデント管理 23
ベストプラクティス 23
クロスアカウントインシデント管理のセットアップと設定 23
制限事項 25
インシデントへの準備 27
モニタリング 29
全般設定の使用 29
レプリケーションセット 30
レプリケーションセットのタグの管理 31
検出結果機能の管理 32
連絡先の使用 32
問い合わせチャネル 33

エンゲージメント計画 34
連絡先を作成 34
連絡先の詳細をアドレス帳にインポートする 36
オンコールスケジュールの操作 36
オンコールスケジュールの作成 37
既存のオンコールスケジュールの管理 42
エスカレーション計画の操作 47
ステージ 48
エスカレーション計画を作成する 48
チャットチャネルの使用 49
タスク 1: チャットチャネルの Amazon SNS トピックを作成または更新する 50
タスク 2: AWS Chatbot でチャットチャネルを作成する 51
タスク 3: Incident Manager の対応計画にチャットチャネルを追加する 54
チャットチャネルを通じた対話 54
ランブックの操作 55
ランブックワークフローの開始と実行に必要な IAM アクセス許可 57
ランブックパラメータの使用 59
ランブックを定義する 61
Incident Manager ランブックテンプレート 63
対応計画の操作 64
対応計画の作成 65
結果を使用する 71
検出結果を使用するためのサービスロールの有効化と作成 72
クロスアカウント検出結果サポートのための許可の設定 73
インシデントを作成する 74
CloudWatch アラームでインシデントを自動的に作成する 75
EventBridge イベントでインシデントを自動的に作成する 76
SaaS パートナーイベントを使用したインシデントの作成 76
AWS サービスイベントを使用したインシデントの作成 78
インシデントを手動で作成する 79
インシデント追跡 80
インシデントリスト 80
インシデントの詳細 80
トップバナー 81
インシデントのメモ 82
タブ 82

概要 ... 82
診断 ... 83
タイムライン ... 85
ランブック ... 85
エンゲージメント ... 86
関連項目 ... 87
プロパティ ... 87
インシデント後分析の実行 ... 89
分析の詳細 ... 89
概要 ... 89
メトリクス ... 89
タイムライン ... 90
Questions ... 90
アクション ... 91
チェックリスト ... 91
分析テンプレート ... 91
AWS スタンダードテンプレート ... 91
分析テンプレートを作成する ... 92
分析の作成 ... 92
フォーマット済みインシデント分析の印刷 ... 93
チュートリアル ... 94
Incident Manager でのランブックの使用 ... 94
タスク 1: ランブックを作成する ... 95
タスク 2: IAM ロールの作成 ... 98
タスク 3: ランブックを対応計画に接続する ... 100
タスク 4: 対応計画に CloudWatch アラームを割り当てる ... 101
タスク 5: 結果の検証 ... 101
セキュリティインシデントの管理 ... 102
リソースのタグ付け ... 105
セキュリティ ... 107
データ保護 ... 108
データ暗号化 ... 109
Identity and Access Management ... 111
対象者 ... 111
アイデンティティを使用した認証 ... 112
ポリシーを使用したアクセスの管理 ... 116

が IAM と AWS Systems Manager Incident Manager 連携する方法 118
アイデンティティベースポリシーの例 127
リソースベースのポリシーの例 131
サービス間の混乱した代理の防止 133
サービスリンクロールの使用 134
AWS Incident Manager の マネージドポリシー 137
トラブルシューティング 144
Incident Manager での共有連絡先と対応計画の操作 146
連絡先と対応計画を共有するための前提条件 147
関連サービス 147
連絡先または対応計画を共有する 147
共有連絡先または対応計画の共有を停止する 148
共有連絡先または対応計画を特定する 149
連絡先と対応計画の共有許可 149
請求と使用量測定 149
インスタンス制限 150
コンプライアンス検証 150
耐障害性 151
インフラストラクチャセキュリティ 152
VPC エンドポイント (AWS PrivateLink) の操作 152
Incident Manager VPC エンドポイントに関する考慮事項 153
Incident Manager 用のインターフェイス VPC エンドポイントの作成 153
Incident Manager 用の VPC エンドポイントの作成 154
設定と脆弱性の分析 154
セキュリティに関するベストプラクティス 155
Incident Manager の予防的セキュリティのベストプラクティス 155
Incident Manager の検出に関するセキュリティのベストプラクティス 157
ログ記録とモニタリング 158
Amazon CloudWatch メトリクス 158
CloudWatch コンソールでの Incident Manager のメトリクスの表示 161
メトリクスのディメンション 161
AWS CloudTrail を使用した Incident Manager API コールのログ記録 162
CloudTrail での Incident Manager 情報 162
Incident Manager のログファイルエントリについて 163
製品およびサービスの統合 166
との統合 AWS のサービス 166

その他の製品やサービスとの統合 171
PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存する 177
トラブルシューティング 183
エラーメッセージ: ValidationException – We were unable to validate the AWS Secrets Manager secret 183
その他の問題のトラブルシューティング 185
AWS 用語集 186
ドキュメント履歴 187
..... cciii

AWS Systems Manager Incident Manager とは?

AWS Systems Manager の一機能である Incident Manager は、AWS でホストされているアプリケーションに影響を与えるインシデントを軽減し、回復させるのに役立つように設計されています。

AWS のコンテキストにおいて、インシデントとは、業務運営に重大な影響を与える可能性のある、サービスの計画外の中断または品質の低下を意味します。したがって、組織にとって、インシデントを効率的に軽減して回復するための対応戦略を確立し、将来のインシデントを防ぐための措置を実行することが重要です。

Incident Manager は、以下の方法でインシデント解決にかかる時間を短縮できます。

- インシデント対応の責任者を効率的にエンゲージさせるための自動計画を提供する。
- 関連するトラブルシューティングデータを提供する。
- 定義済みのオートメーションランブックを使用して、自動対応アクションを有効にする。
- すべてのステークホルダーと協力し連絡を取る方法を提供する。

Incident Manager に組み込まれている機能とワークフローは、Amazon がほぼ設立当初から開発してきたインシデント対応のベストプラクティスに基づいています。Incident Manager は Amazon CloudWatch、AWS CloudTrail、AWS Systems Manager、Amazon EventBridge などの AWS のサービス と統合されています。

主なコンポーネントと機能

このセクションでは、インシデント対応計画のセットアップに使用する Incident Manager の機能について説明します。

対応計画

対応計画は、インシデント発生時に何を準備する必要があるかを定義するテンプレートとして機能します。これには以下のような情報が含まれます。

- インシデント発生時に対応を求められるのは誰か。
- インシデントを軽減するための確立された自動対応。
- 応答者が連絡を取り、インシデントに関する自動通知を受け取るために使用する必要があるコラボレーションツール。

インシデント検知

Amazon CloudWatch アラームおよび Amazon EventBridge イベントを設定して、AWS リソースに影響を与える条件または変更が検出されたときに、インシデントを作成できます。

ランブックオートメーションサポート

Incident Manager 内からオートメーションランブックを開始して、インシデントへの重要な対応を自動化し、最初の応答者に詳細なステップを提供します。

エンゲージメントとエスカレーション

エンゲージメント計画は、一意のインシデントが発生するたびに全員に通知するように指定します。Incident Manager に追加した個々の連絡先を指定することも、Incident Manager で作成したオンコールスケジュールを指定することもできます。また、エンゲージメント計画は、エスカレーションパスを指定して、ステークホルダーの間での可視性およびインシデント対応プロセスへの積極的な参加を確保できるようにします。

オンコールスケジュール

Incident Manager のオンコールスケジュールは、そのスケジュール用に作成する 1 つ以上の口ーテーションで構成されます。各口ーテーションには、最大 30 個の連絡先を含めることができます。オンコールスケジュールは、エスカレーション計画または対応計画に追加すると、応答者の介入が必要なインシデントが発生した場合に誰が通知を受けるかを定義します。オンコールスケジュールは、インシデント対応に必要な完全かつ冗長な 24 時間 365 日のカバレッジを確保するのに役立ちます。

アクティブコラボレーション

インシデント応答者は、AWS Chatbot クライアントとの統合を通じて、インシデントに積極的に対応します。AWS Chatbot は、Slack、Microsoft Teams、または Amazon Chime を使用する Incident Manager 用のチャットチャネルの作成をサポートします。応答者は、互いに直接連絡を取り合ったり、インシデントに関する自動通知を受け取ることができます。また、Slack および Microsoft Teams では、一部の Incident Manager のコマンドラインインターフェイス (CLI) オペレーションを直接実行できます。

インシデント診断

応答者は、インシデント発生時に、Incident Manager コンソールで最新情報を表示できます。その後、応答者は情報の変更に基づき、オートメーションランブックを使用してフォローアップ項目を作成し、それらを修正できます。

他のサービスからの検出結果

応答者のインシデント診断をサポートするために、Incident Manager の検出結果機能を有効にできます。検出結果とは、インシデント発生前後に発生した、インシデントに関連する可能性のある 1 つ以上のリソースが関与した AWS CodeDeploy デプロイおよび AWS CloudFormation スタックの更新に関する情報です。この情報があると、潜在的な原因の評価に必要な時間が短縮され、インシデントからの平均回復時間 (MTTR) を短縮できます。

インシデント後分析

インシデントが解決されたら、インシデント後分析を使用して、検出および緩和までの時間など、インシデント対応を改善するための改善点を特定します。分析は、インシデントの原因を理解するのに役立ちます。Incident Manager は、インシデント対応を改善するために使用できる推奨フォローアップアクション項目を作成します。

Incident Manager を使用する利点

インシデント検出および対応業務に Incident Manager を使用することの利点について説明します。

このセクションでは、Incident Manager 対応計画を実装することで組織が得られる利点について説明します。

問題を効率的かつ即時に診断する

設定した Amazon CloudWatch アラームおよび Amazon EventBridge イベントは、サービスの計画外の中断または品質の低下が発生した場合に、自動的にインシデントを作成することができます。

CloudWatch アラームは、複数の期間にわたってしきい値を基準としたメトリクスまたは式の値に変化があった場合、検出して報告します。EventBridge イベントは、EventBridge ルールで指定した環境、アプリケーション、またはサービスの変更の結果として作成されます。アラームまたはイベントを作成する場合、Incident Manager で作成するインシデントのアクション、およびインシデントのエンゲージメント、エスカレーション、緩和を円滑に進めるための適切な対応計画を指定できます。

Incident Manager は、CloudWatch メトリクスを使用して、インシデントに関連するメトリクスを自動的に収集および追跡する機能を提供します。CloudWatch アラームによってインシデントが作成されたときに生成される自動メトリクスに加えて、メトリクスをリアルタイムで手動で追加して、インシデントの応答者に追加のコンテキストおよびデータを提供できます。

Incident Manager インシデントタイムラインを使用して、POI を時系列で表示します。応答者は、タイムラインを使用してカスタムイベントを追加し、自分が何をしたのか、何が起こったのかを説明することもできます。自動化された POI は次のとおりです。

- CloudWatch アラームまたは EventBridge ルールはインシデントを作成します。
- インシデントメトリクスは Incident Manager に報告されます。
- 応答者はエンゲージしています。
- ランブックのステップは正常に完了しました。

効果的にエンゲージさせる

Incident Manager は、連絡先、オンコールスケジュール、エスカレーション計画、チャットチャネルを使用して、インシデント応答者をまとめます。Incident Manager で個々の連絡先を直接定義し、連絡先設定 (E メール、SMS、音声) を指定します。オンコールスケジュールのローテーションに連絡先を追加して、特定の期間に誰をインシデントにエンゲージさせるかを決定します。定義された連絡先およびオンコールスケジュールを使用して、インシデント中に適切なタイミングで必要な応答者をエンゲージさせるエスカレーション計画を作成します。

リアルタイムで協力する

インシデント中のコミュニケーションは、より迅速な解決の鍵です。Slack、Microsoft Teams、または Amazon Chime を使用するようにセットアップされた AWS Chatbot クライアントを使用すると、応答者を希望する接続チャットチャネルに集めて、直接インシデントと対話したり、相互にやり取りしたりできます。また、Incident Manager は、チャットチャネル内のインシデント応答者のリアルタイムアクションを表示し、他のユーザーにコンテキストを提供します。

サービスの復旧を自動化する

Incident Manager では、オートメーションランブックを使用することで、応答者はインシデントの解決に必要な主要タスクに集中できます。Incident Manager では、ランブックは、インシデントを解決するために実行される事前定義された一連のアクションです。必要に応じて、自動タスクの力と手動ステップを組み合わせて、応答者が影響を分析して対応できるようにします。

将来のインシデントを防ぐ

Incident Manager によるインシデント後分析により、チームはより強固な対応計画を策定し、アプリケーション全体で変更を反映させて、将来のインシデントおよびダウンタイムを防ぐことができます。インシデント後分析は、ランブック、対応計画、およびメトリクスの反復学習および改善も提供します。

関連サービス

Incident Manager は、インシデントの検出および解決、API オペレーションとの間接的な対話、インフラストラクチャの管理に役立つように、他の AWS のサービス やサードパーティのサービスおよびツールと統合されています。詳細については、「Product and service integrations with Incident Manager」を参照してください。

Incident Manager へのアクセス

Incident Manager には、次のいずれかの方法でアクセスできます。

- Incident Manager コンソール
- AWS CLI – 一般的な情報については、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の開始方法」を参照してください。Incident Manager の CLI コマンドの詳細については、「AWS CLI Command Reference」の「ssm-incidents」および「ssm-contacts」を参照してください。
- Incident Manager API - 詳細については、「AWS Systems Manager Incident Manager API Reference」を参照してください。
- AWS SDKs – 詳細については、「AWS での構築ツール」を参照してください。

Incident Manager のリージョンとクォータ

Incident Manager は、Systems Manager がサポートしているすべての AWS リージョン でサポートされているわけではありません。

Incident Manager のリージョンおよびクォータに関する情報を確認するには、「Amazon Web Services 全般のリファレンス」の「AWS Systems Manager Incident Manager エンドポイントとクォータ」を参照してください。

Incident Manager の価格

Incident Manager の使用には料金がかかりますか。詳細については、「AWSSystems Manager の料金」を参照してください。

> **Note**
>
> このサービスに関連して提供される他の AWS のサービス、AWS コンテンツ、およびサードパーティコンテンツには、別途料金がかかり、追加条件が適用される場合があります。

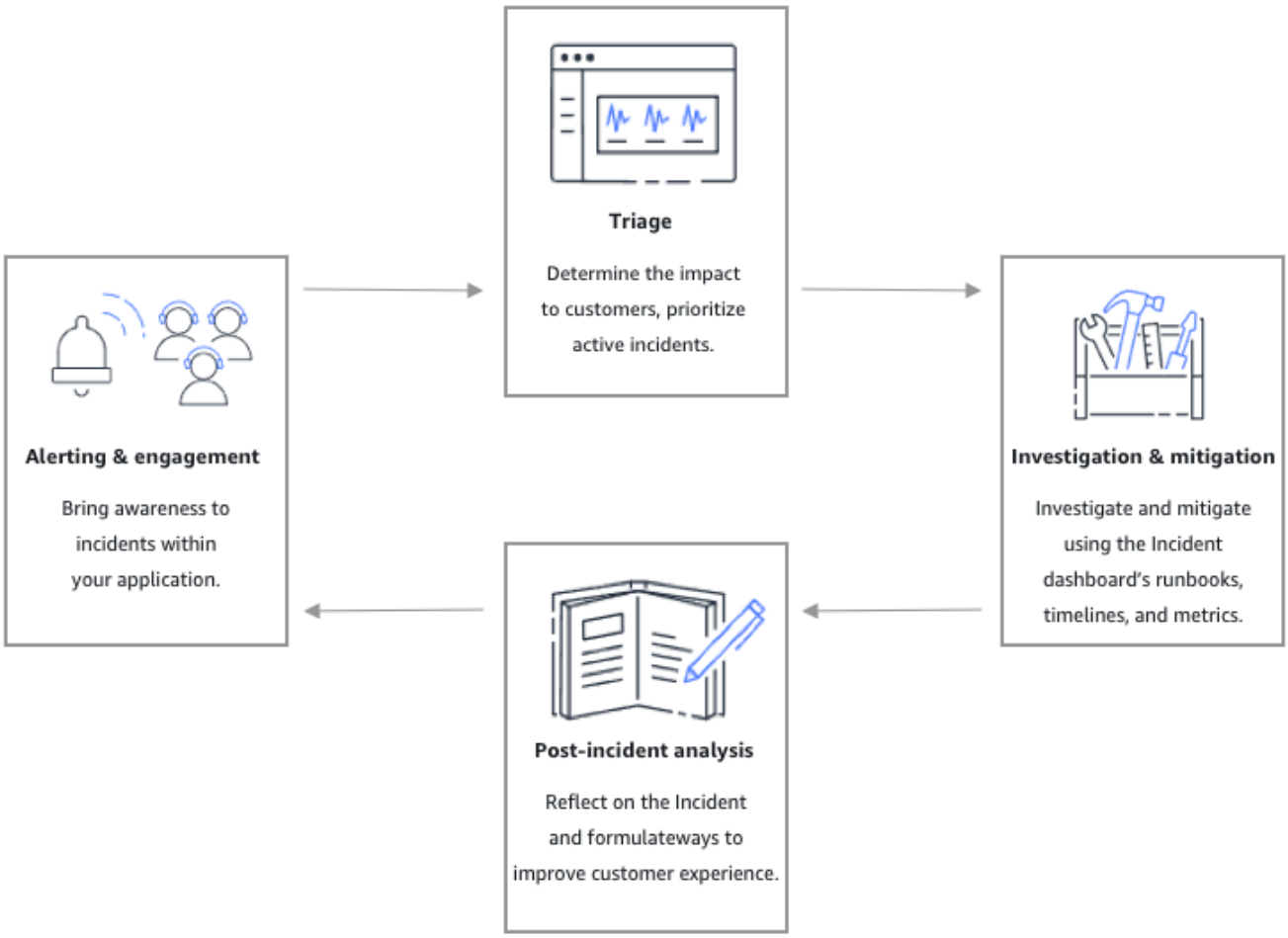
AWS 環境のコスト、セキュリティ、およびパフォーマンスの最適化に役立つサービスである Trusted Advisor の概要については、「AWS Support ユーザーガイド」の「AWS Trusted Advisor」を参照してください。

Incident Manager でのインシデントライフサイクル

AWS Systems Manager Incident Manager は、サービスの停止やセキュリティ上の脅威などのインシデントを特定して対応するためのベストプラクティスに基づいた段階的なフレームワークを提供します。Incident Manager の主な目的は、完全なインシデントライフサイクル管理ソリューションを通じて、影響を受けたサービスやアプリケーションをできるだけ早く正常に戻すことです。

Incident Manager は、インシデントライフサイクルのすべてのフェーズにツールとベストプラクティスを提供します。

- アラートとエンゲージメント
- トリアージ
- 調査と緩和
- インシデント後分析



アラートとエンゲージメント

インシデントライフサイクルのアラートとエンゲージメントフェーズでは、アプリケーションおよびサービス内のインシデントに対する認識の提供に重点を置いています。このフェーズは、インシデントが検出される前に開始され、アプリケーションを深く理解する必要があります。Amazon CloudWatch メトリクスを使用してアプリケーションのパフォーマンスに関するデータをモニタリングしたり、Amazon EventBridge を活用してさまざまなソース、アプリケーション、サービスからのアラートを集約したりできます。アプリケーションのモニタリングを設定したら、履歴基準外のメトリクスに関するアラートを開始できます。モニタリングのベストプラクティスについては、「モニタリング」を参照してください。

応答者のインシデント診断をサポートするために、Incident Manager の検出結果機能を有効にできます。検出結果とは、インシデント発生前後に発生した AWS CodeDeploy デプロイと AWS

CloudFormation スタックの更新に関する情報です。この情報があると、潜在的な原因の評価に必要な時間が短縮され、インシデントからの平均回復時間 (MTTR) を短縮できます。

アプリケーションのインシデントをモニタリングしているので、インシデントの際に使用するインシデント 対応計画 を定義できます。対応計画の作成の詳細については、「Incident Manager での対応計画の操作」を参照してください。Amazon EventBridge イベントまたは CloudWatch アラームは、テンプレートとして対応計画を使用してインシデントを自動的に作成できます。インシデントの作成の詳細については、「Incident Manager でのインシデントの作成」を参照してください。

対応計画では、関連する エスカレーション計画 および最初の応答者をインシデントに参加させるための エンゲージメント計画 を開始します。エスカレーションプランの設定の詳細については、エスカレーション計画を作成する を参照してください。同時に、AWS Chatbot はチャットチャネルを使用して、インシデントの詳細ページを応答者に通知します。チャットチャネルと インシデントの詳細を使用すると、チームはインシデントを通信し、トリアージすることができます。Incident Manager でのチャットチャネルのセットアップの詳細については、「タスク 2: AWS Chatbot でチャットチャネルを作成する」を参照してください。

トリアージ

トリアージとは、最初の応答者が顧客への影響を判断しようとする場合です。Incident Manager コンソールのインシデント詳細ビューには、応答者がインシデントを評価するのに役立つタイムラインとメトリクスが表示されます。インシデントの影響を評価することは、インシデントの対応時間、解決、コミュニケーションの基盤にもなります。応答者は、1 (重大) から 5 (影響なし) までの影響度評価を使用してインシデントに優先順位を付けます。

組織は、各影響度評価の正確な範囲を自由に定義できます。次の表に、各影響レベルの一般的な定義の例を示します。

影響コード	影響名	サンプルの定義スコープ
1	`Critical`	ほとんどのお客様に影響するアプリケーション全体の障害。
2	`High`	一部のお客様に影響するアプリケーション全体の障害。
3	`Medium`	お客様に影響する部分的なアプリケーション障害。

影響コード	影響名	サンプルの定義スコープ
4	Low	お客様への影響は限定的な断続的な障害。
5	No Impact	お客様は現在影響を受けていないものの、影響を回避するための緊急のアクションが必要。

調査と緩和

インシデント 詳細ビューでは、チームに Runbook、タイムライン、およびメトリクスが提供されます。インシデントの取り扱い方法については、「インシデントの詳細」を参照してください。

Runbooks 一般的に調査ステップを提供し、データを自動的に取得したり、一般的に使用されるソリューションを試すことができます。Runbooks は、チームがインシデントの緩和に役立つと判断した、明確で反復可能なステップも提供します。Runbook タブは現在の Runbook ステップに焦点を当て、過去と将来のステップを表示します。

Incident Manager は、Systems Manager 自動化と統合して Runbook を構築します。Runbook を使用して、以下のいずれかを実行します。

- インスタンスと AWS リソースの管理
- スクリプトの自動実行
- AWS CloudFormation リソースの管理

サポートされるアクションタイプの詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager Automation アクションのリファレンス」を参照してください。

[タイムライン] タブには、実行されたアクションが表示されます。タイムラインには、タイムスタンプと自動的に作成された詳細が記録されます。タイムラインにカスタムイベントを追加するには、このユーザーガイドの インシデントの詳細 ページの タイムライン セクションを 参照してください。

[診断] タブには、自動的に入力されたメトリクスと手動で追加されたメトリクスが表示されます。このビューは、インシデント中のアプリケーションのアクティビティに関する貴重な情報を提供します。

[エンゲージメント] タブでは、インシデントに連絡先を追加することができ、インシデントに関与したエンゲージメント中の連絡先に、対応を迅速化するためのリソースを提供するのに役立ちます。連絡先は、定義済みのエスカレーション計画、または個人のエンゲージメント計画に従ってエンゲージします。

チャットチャネルを使用すると、直接インシデントを操作したりチームの他の応答者と対話したりできます。AWS Chatbot を使用して、Slack、Microsoft Teams、および Amazon Chime にチャットチャネルを設定できます。Slack および Microsoft Teams チャネルでは、応答者は、多くの `ssm-incidents` コマンドを使用して、チャットチャネルから直接インシデントを操作できます。詳細については、「チャットチャネルを通じた対話」を参照してください。

インシデント後分析

Incident Manager は、インシデントを検証し、インシデントの今後の再発を防止するために必要な措置を講じ、インシデント対応活動全体を改善するためのフレームワークを提供します。改善には以下が含まれます。

- インシデントに関連したアプリケーションの変更。チームはこの時間を使用してシステムを改善し、耐障害性を高めることができます。
- インシデント対応計画への変更。時間をかけて学んだ教訓を取り入れます。
- ランブックの変更。チームは、解決に必要なステップと、自動化できるステップについて深く掘り下げることができます。
- アラートの変更。インシデント後、チームはインシデントについてより早くチームに警告するために使用できるメトリクスのクリティカルポイントに気づくことができます。

Incident Manager は、インシデントタイムラインと並んでインシデント後分析の質問とアクション項目を使用して、これらの潜在的な改善を容易にします。分析による改善の詳細については、「Incident Manager でのインシデント後分析の実行」を参照してください。

AWS Systems Manager Incident Manager のセットアップ

オペレーションの管理に使用するアカウントで AWS Systems Manager Incident Manager を設定することをお勧めします。Incident Manager を初めて使用する場合は、事前に以下のタスクを完了します。

トピック

- にサインアップする AWS アカウント
- 管理アクセスを持つユーザーを作成する
- プログラム的なアクセス権を付与する
- Incident Manager のセットアップに必要なロール

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

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

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

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

管理アクセスを持つユーザーを作成する

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

のセキュリティ保護 AWS アカウントのルートユーザー

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

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

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

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

プログラム的なアクセス権を付与する

ユーザーが の AWS 外部で を操作する場合は、プログラムによるアクセスが必要です AWS Management Console。プログラムによるアクセスを許可する方法は、 にアクセスするユーザーのタイプによって異なります AWS。

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

プログラマチックアクセス権を必要とするユーザー	目的	方法
ワークフォースアイデンティティ (IAM Identity Center で管理されているユーザー)	一時的な認証情報を使用して、、 AWS SDKs AWS CLI、または AWS APIs。	使用するインターフェイス用の手引きに従ってください。 • については AWS CLI、「 ユーザーガイド」の AWS CLI 「 を使用するための の設定 AWS IAM Identity CenterAWS Command Line Interface 」を参照してください。 • AWS SDKs 、ツール、AWS APIs「 SDK とツールのリファレンスガイド」

プログラマチックアクセス権を必要とするユーザー	目的	方法
		の「IAM Identity Center 認証」を参照してください。 AWS SDKs
IAM	一時的な認証情報を使用して、、 AWS SDKs AWS CLI、または AWS APIs。	「IAM ユーザーガイド」の「 AWS リソースでの一時的な認証情報の使用」の手順に従います。
IAM	(非推奨) 長期認証情報を使用して、、 AWS SDKs AWS CLI、または AWS APIs。	使用するインターフェイス用の手引きに従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDKs「 SDK とツールのリファレンスガイド」の「長期的な認証情報を使用した認証」を参照してください。 AWS SDKs • AWS APIsユーザーガイド」の「IAM ユーザーのアクセスキーの管理」を参照してください。

Incident Manager のセットアップに必要なロール

開始する前に、アカウントに IAM アクセス許可 `iam:CreateServiceLinkedRole` が必要です。Incident Manager は、この許可を使用して、アカウントに `AWSServiceRoleforIncidentManager` を作成します。詳細については、「Incident Manager のサービスリンクロールの使用」を参照してください。

Incident Manager の使用開始

このセクションでは、Incident Manager コンソールでの 準備 について説明します。コンソールをインシデント管理に使用する前に、コンソールで準備ウィザードを完了する必要があります。このウィザードに従って、レプリケーションセット、少なくとも 1 つの連絡先と 1 つのエスカレーション計画、および最初の対応計画を設定します。以下は、Incident Manager とインシデントのライフサイクルを理解するのに役立つガイドです。

- AWS Systems Manager Incident Manager とは?
- Incident Manager でのインシデントライフサイクル

前提条件

Incident Manager を初めて使用する場合は、「AWS Systems Manager Incident Manager のセットアップ」を参照してください。オペレーションの管理に使用するアカウントで Incident Manager を設定することをお勧めします。

Incident Manager の準備ウィザードを開始する前に、Systems Manager の高速セットアップを完了することをお勧めします。Systems Manager 高速セットアップ を使用して、頻繁に使用するサービスや機能を推奨されるベストプラクティスで設定します。Incident Manager は、Systems Manager の機能を使用して AWS アカウント に関連するインシデントを管理しますので、Systems Manager を最初に設定することによる利点があります。

準備ウィザード

Incident Manager を初めて使用する際には、Incident Manager サービスのホームページから準備ウィザードにアクセスできます。初回設定の完了後に準備ウィザードにアクセスするには、インシデントリストページで [準備] を選択します。

1. Incident Manager コンソールを開きます。
2. Incident Manager サービスのホームページで、準備を選択します。

全般設定

1. [全般設定] で、[ファイル] を選択します。

2. 利用規約を読みます。Incident Manager の利用規約に同意する場合は、「私は Incident Manager の利用規約を読み、同意します」を選択し、[次へ] を選択します。
3. [リージョン] 領域に、現在の AWS リージョン がレプリケーションセットの最初のリージョンとして表示されます。レプリケーションセットにリージョンを追加するには、リージョンのリストから選択します。

   2 つ以上のリージョンを含めることをお勧めします。1 つのリージョンが一時的に利用できなくなった場合に、インシデント関連のアクティビティを別のリージョンに転送できます。

   > **Note**
   >
   > レプリケーションセットを作成すると、アカウントに `AWSServiceRoleforIncidentManager` サービスリンクロールが作成されます。このロールの詳細については、「Incident Manager のサービスリンクロールの使用」を参照してください。

4. レプリケーションセットの暗号化をセットアップするには、以下のいずれかを実行します。

   > **Note**
   >
   > すべての Incident Manager リソースは暗号化されます。データ暗号化の詳細については、「Incident Manager でのデータ保護」を参照してください。Incident Manager レプリケーションセットの詳細については、「Incident Manager レプリケーションセットの使用」を参照してください。

   - AWS 所有キーを使用するには、[AWS 所有キーを使用] を選択します。
   - 自己所有の AWS KMS キーを使用するには、[既存の AWS KMS key キーを選択] を選択します。ステップ 3 で選択した各リージョンについて、AWS KMS キーを選択するか、AWS KMS Amazon リソースネーム (ARN) を入力します。

     > **Tip**
     >
     > 使用できる AWS KMS key がない場合は、[AWS KMS key の作成] を選択します。

5. (オプション) [タグ] 領域で、1 つ以上のタグをレプリケーションセットに追加します。タグには、キーと、オプションで値が含まれます。

タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。

6. (オプション) [サービスアクセス] 領域で、検出結果機能を有効にするには、[このアカウントに検出結果のサービスロールを作成する] チェックボックスをオンにします。

   検出結果とは、インシデントが作成されたのとほぼ同時期に発生したコードのデプロイまたはインフラストラクチャの変更に関する情報です。検出結果は、インシデントの潜在的な原因として調査できます。これらの潜在的な原因に関する情報は、インシデントのインシデント詳細ページに追加されます。こうしたデプロイや変更に関する情報がすぐに手元にあれば、対応者はこの情報を手動で検索する必要がありません。

   > **Tip**
   >
   > 作成するロールに関する情報を表示するには、[許可を表示] を選択します。

7. [Create] (作成) を選択します。

   レプリケーションセットと回復性の詳細については、「の耐障害性 AWS Systems Manager Incident Manager」を参照してください。

連絡先 (オプション)

1. 問い合わせの作成 を選択します。

   Incident Manager は、インシデント中にお問い合わせにエンゲージします。お問い合わせの詳細については、「Incident Manager での連絡先の操作」を参照してください。

2. [名前] には、連絡先の名前を入力します。
3. [一意のエイリアス] には、この連絡先を識別するエイリアスを入力します。
4. [連絡先チャネル] セクションで、次の手順を実行し、インシデント発生時の連絡先のエンゲージ方法を定義します。

   a. [タイプ] には、[E メール]、[SMS]、または [音声] を選択します。

   b. [チャネル名] には、チャネルを識別するのに役立つ一意の名前を入力します。

   c. [詳細] には、連絡先の E メールアドレスまたは電話番号を入力します。

電話番号は 9～15 文字で、+ の後に国コードとサブスクライバー番号を続ける必要があります。

d. 別の問い合わせチャネルを作成するには、新しい問い合わせチャネルを追加するを選択します。連絡先ごとに少なくとも 2 つのチャネルを定義することをお勧めします。

5. [エンゲージメントプラン] 領域では、以下の手順を実行し、連絡先への通知に使用するチャネルと、各チャネルで承認を待機する時間を定義します。インシデント中に連絡先にエンゲージするのに使用する連絡先チャネルを選択します。

> **Note**
>
> エンゲージメント計画には少なくとも 2 つのデバイスを定義することをお勧めします。

a. [連絡先チャネル名] には、[連絡先チャネル] 領域で指定したチャネルを選択します。

b. [エンゲージメント時間 (分)] には、連絡先チャネルにエンゲージするまでの待ち時間を分単位で入力します。

エンゲージメントの開始時にエンゲージするデバイスを少なくとも 1 つ選択し、待機時間を **0** (ゼロ) 分に指定することをお勧めします。

c. エンゲージメント計画に問い合わせチャネルを追加するには、エンゲージメントを追加するを選択します。

6. (オプション) [タグ] 領域で、連絡先に 1 つ以上のタグを追加します。タグには、キーと、オプションで値が含まれます。

タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。

7. 連絡先レコードを作成し、定義された連絡先チャネルにアクティベーションコードを送信するには、[次へ] を選択します。

8. (オプション) 連絡先チャネルのアクティベーションページで、各チャネルに送信されたアクティベーションコードを入力します。

すぐにコードを入力できない場合は、後で新しいアクティベーションコードを生成できます。

9. Incident Manager にすべてのお問い合わせを追加するまで、ステップ 4 を繰り返します。

10. 連絡先をすべて入力したら、[完了] を選択します。

(オプション) エスカレーション計画

1. エスカレーション計画の作成を選択します。

   エスカレーション計画は、インシデント中にお問い合わせを通じてエスカレーション し、Incident Manager がインシデント中に正しい応答者をエンゲージできるようにします。エスカレーション計画の詳細については、「Incident Manager でのエスカレーション計画の操作」を参照してください。
2. [名前] にエスカレーション計画の一意の名前を入力します。
3. [エイリアス] には、エスカレーション計画の識別に役立つ一意のエイリアスを入力します。
4. [ステージ 1] 領域で、以下を実行します。

   a. [エスカレーションチャネル] には、エンゲージに使用する連絡先チャネルを選択します。

   b. 連絡先がエスカレーション計画のステージの進行を停止できるようにする場合は、[プランの進行停止を承認] を選択します。

   c. ステージにチャネルをさらに追加するには、[エスカレーションチャネルを追加してください] を選択します。
5. エスカレーション計画に新しいステージを作成するには、[ステージの追加] を選択し、ステージの詳細を追加します。
6. (オプション) [タグ] 領域で、1 つ以上のタグをエスカレーション計画に追加します。タグには、キーと、オプションで値が含まれます。

   タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。
7. エスカレーション計画の作成を選択します。

対応計画

1. 対応計画の作成を選択します。対応計画を使用して、作成した連絡先とエスカレーション計画をまとめます。この開始ウィザード中、特に対応計画を初めて設定する場合は、以下のセクションは省略可能です。

   - チャットチャネル
   - ランブック
   - エンゲージメント

- サードパーティ統合

これらの要素を後で対応計画に追加する方法については、「Incident Manager でのインシデントへの準備」を参照してください。

2. [名前] に、この対応計画の一意の識別可能な名前を入力します。この名前は、対応計画 ARN の作成、または表示名のない対応計画に使用されます。
3. (オプション) [表示名] に、インシデントを作成するときにこの対応計画を識別するのに役立つ名前を入力します。
4. [タイトル] に、この対応計画に関連するインシデントのタイプを識別するのに役立つタイトルを入力します。指定する値は、各インシデントのタイトルに含まれます。インシデントを発生させたアラームまたはイベントもタイトルに追加されます。
5. [影響] では、この対応計画に関連するインシデントが及ぼすことが想定される影響レベル (**`Critical`** や**`Low`** など) を選択します。
6. (オプション) [概要] に、インシデントの概要を示す簡単な説明を入力します。Incident Manager は、インシデント中に概要に関連情報を自動的に入力します。
7. (オプション) [重複排除文字列] は、重複排除文字列を入力します。Incident Manager は、この文字列を使用して、同じ根本原因が同じアカウントに複数のインシデントを作成しないようにします。

   重複排除文字列は、システムがインシデントの重複をチェックするために使用する用語またはフレーズです。重複排除文字列を指定すると、Incident Manager はインシデントを作成するときに `dedupeString` フィールドに同じ文字列が含まれる未解決のインシデントを検索します。重複が検出されると、Incident Manager は新しいインシデントを既存のインシデントに重複排除します。

   > **Note**
   >
   > デフォルトでは、Incident Manager は同じ Amazon CloudWatch アラームまたは Amazon EventBridge イベントによって作成された複数のインシデントを自動的に重複排除します。これらのリソースタイプの重複を避けるために、独自の重複排除文字列を入力する必要はありません。

8. (オプション) [タグ] 領域で、1 つ以上のタグを対応計画に追加します。タグには、キーと、オプションで値が含まれます。

タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。

9. [エンゲージメント] ドロップダウンから、インシデントに適用する連絡先とエスカレーション計画を選択します。
10. 対応計画の作成を選択します。

対応計画を作成したら、Amazon CloudWatch アラームまたは Amazon EventBridge イベントを対応計画に関連付けることができます。これにより、アラームまたはイベントに基づいてインシデントが自動的に作成されます。詳細については、「Incident Manager でのインシデントの作成」を参照してください。

Incident Manager でのクロスリージョンおよびクロスアカウントのインシデント管理

AWS Systems Manager の一機能である Incident Manager を、複数の AWS リージョン およびアカウントと連携するように設定できます。このセクションでは、クロスリージョンおよびクロスアカウントのベストプラクティス、セットアップ手順、既知の制限事項について説明します。

トピック

- クロスリージョンのインシデント管理
- クロスアカウントインシデント管理

クロスリージョンのインシデント管理

Incident Manager は、複数の AWS リージョン で自動および手動によるインシデント作成をサポートしています。[準備] ウィザードを使用して Incident Manager で初めてオンボードする場合、レプリケーションセットには最大 3 つの AWS リージョン を指定できます。Amazon CloudWatch アラームまたは Amazon EventBridge イベントによって自動的に作成されたインシデントの場合、Incident Manager はイベントルールまたはアラームと同じ AWS リージョン にインシデントを作成しようとします。Incident Manager が AWS リージョン で利用できない場合、CloudWatch または EventBridge は、レプリケーションセットで指定されている使用可能なリージョンのいずれかにインシデントを自動的に作成します。

> **Important**
>
> 次の重要な詳細に留意してください。
>
> - レプリケーションセットには、少なくとも 2 つの AWS リージョン を指定することをお勧めします。リージョンを少なくとも 2 つ指定しないと、Incident Manager が使用できない間、システムはインシデントを作成できません。
> - クロスリージョンフェイルオーバーによって作成されたインシデントは、対応計画で指定されているランブックを呼び出しません。

Incident Manager を使用したオンボーディングおよび追加リージョンの指定の詳細については、「Incident Manager の使用開始」を参照してください。

クロスアカウントインシデント管理

Incident Manager は、AWS Resource Access Manager (AWS RAM) を使用して、管理アカウントおよびアプリケーションアカウントで Incident Manager リソースを共有します。このセクションでは、クロスアカウントのベストプラクティス、Incident Manager のクロスアカウント機能の設定方法、および Incident Manager でのクロスアカウント機能の既知の制限について説明します。

管理アカウントは、オペレーション管理を実行するアカウントです。組織の設定では、管理アカウントは、対応計画、連絡先、エスカレーション計画、ランブック、およびその他の AWS Systems Manager リソースを所有します。

アプリケーションアカウントは、アプリケーションを構成するリソースを所有するアカウントです。これらのリソースは、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、または AWS クラウド でアプリケーションを構築するために使用するその他のリソースです。アプリケーションアカウントは、Incident Manager でインシデントを作成する Amazon CloudWatch アラームと Amazon EventBridge イベントも所有しています。

AWS RAM は、リソース共有を使用して、アカウント間でリソースを共有します。対応計画と連絡先リソースは、AWS RAMのアカウント間で共有できます。これらのリソースを共有することで、アプリケーションアカウントと管理アカウントはエンゲージメントやインシデントと対話できます。対応計画を共有すると、その対応計画を使用して作成された過去と今後のインシデントがすべて共有されます。連絡先の共有は、連絡先または対応計画の過去と今後のすべてのエンゲージメントを共有します。

ベストプラクティス

アカウント間で Incident Manager リソースを共有する場合は、次のベストプラクティスに従います。

- 対応計画と連絡先を使用して、リソース共有を定期的に更新します。
- リソース共有プリンシパルを定期的に確認します。
- 管理アカウントで Incident Manager、ランブック、チャットチャネルを設定します。

クロスアカウントインシデント管理のセットアップと設定

次のステップでは、Incident Manager リソースを設定· 構成し、クロスアカウント機能に使用する方法について説明します。過去に、クロスアカウント機能用にいくつかのサービスとリソースを設定し

たことがあるかもしれません。クロスアカウントリソースを使用して最初のインシデントを開始する前に、このステップを要件のチェックリストとして使用してください。

1. (オプション) AWS Organizationsを使用して組織と組織単位を作成します。「AWS Organizations ユーザーガイド」の「チュートリアル: 組織の作成と設定」のステップに従います。
2. (オプション) Systems Manager Quick Setup 機能を使用して、クロスアカウントのランブックを設定する際に使用する正しい AWS Identity and Access Management ロールをセットアップします。詳細については、「AWS Systems Manager ユーザーガイド」の「Quick Setup」を参照してください。
3. 「AWS Systems Manager ユーザーガイド」の「複数の AWS リージョン とアカウントでのオートメーションの実行」にリストされている手順に従って、Systems Manager オートメーションドキュメントにランブックを作成します。ランブックは、管理アカウントまたはアプリケーションアカウントのいずれかで実行できます。ユースケースに応じて、インシデント中にランブックを作成・表示するのに必要なロールに応じて、適切な AWS CloudFormation テンプレートをインストールする必要があります。
   - 管理アカウントでランブックを実行します。管理アカウントは、AWS-SystemsManager-AutomationReadOnlyRole CloudFormation テンプレートをダウンロードしてインストールする必要があります。AWS-SystemsManager-AutomationReadOnlyRoleをインストールする際には、すべてのアプリケーションアカウントのアカウント ID を指定してください。このロールにより、アプリケーションアカウントはインシデントの詳細ページからランブックのステータスを読み取ることができます。アプリケーションアカウントは、AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation テンプレートをインストールする必要があります。インシデントの詳細ページでは、このロールを使用して、管理アカウントから自動化ステータスを取得します。
   - アプリケーションアカウントでランブックを実行します。管理アカウントは、AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation テンプレートをダウンロードしてインストールする必要があります。このロールは、管理アカウントがアプリケーションアカウント内のランブックのステータスを読み取ることを許可します。アプリケーションアカウントは、AWS-SystemsManager-AutomationReadOnlyRole CloudFormationテンプレートをダウンロードしてインストールする必要があります。AWS-SystemsManager-AutomationReadOnlyRoleをインストールする際には、管理アカウントやその他のアプリケーションアカウントのアカウント ID を指定してください。管理アカウントおよびその他のアプリケーションアカウントは、ランブックのステータスを読み取るために、このロールを引き受けます。

4. (オプション) 組織の各アプリケーションアカウントで、AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole CloudFormation テンプレートをダウンロードしてインストールします。AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole をインストールする際には、管理アカウントのアカウント ID を指定してください。このロールは、Incident Manager が AWS CodeDeploy デプロイおよび AWS CloudFormation スタックの更新に関する情報にアクセスするために必要なアクセス許可を付与します。検出結果機能が有効になっている場合、この情報はインシデントの検出結果として報告されます。詳細については、「Incident Manager での検出結果の使用」を参照してください。
5. 連絡先、エスカレーションプラン、チャットチャネル、および応答プランを設定して作成するには、「Incident Manager でのインシデントへの準備」で説明されているステップに従います。
6. 連絡先や対応計画のリソースを既存のリソース共有または新規のリソース共有に AWS RAMで追加できます。詳細については、「AWS RAM ユーザーガイド」の「AWS RAM の使用開始」を参照してください。対応計画を AWS RAM に追加すると、アプリケーションアカウントが、対応計画を使用して作成されたインシデントとインシデントダッシュボードにアクセスできるようになります。また、アプリケーションアカウントは、CloudWatch のアラームや EventBridge のイベントを対応計画に関連付けることができるようになります。連絡先とエスカレーション計画を AWS RAM に追加すると、アプリケーションアカウントがインシデントダッシュボードからエンゲージメントを表示し、連絡先をエンゲージできるようになります。
7. クロスアカウントクロスリージョン機能を CloudWatch コンソールに追加します。ステップおよび情報については、「Amazon CloudWatch ユーザーガイド」の「クロスアカウントクロスリージョン CloudWatch コンソール」を参照してください。この機能を追加すると、作成したアプリケーションアカウントと管理アカウントが、インシデントと分析ダッシュボードのメトリクスの表示と編集ができるようになります。
8. クロスアカウントの Amazon EventBridge イベントバスを作成します。ステップおよび情報については、「AWS アカウント間での Amazon EventBridge イベントの送受信」を参照してください。次に、このイベントバスを使用して、アプリケーションアカウントのインシデントを検出し、管理アカウントにインシデントを作成するイベントルールを作成できます。

制限事項

Incident Manager のクロスアカウント機能の既知の制限事項を次に示します。

- インシデント後分析を作成したアカウントが、その分析を表示および変更できる唯一のアカウントです。アプリケーションアカウントを使用してインシデント後分析を作成した場合、そのアカウン

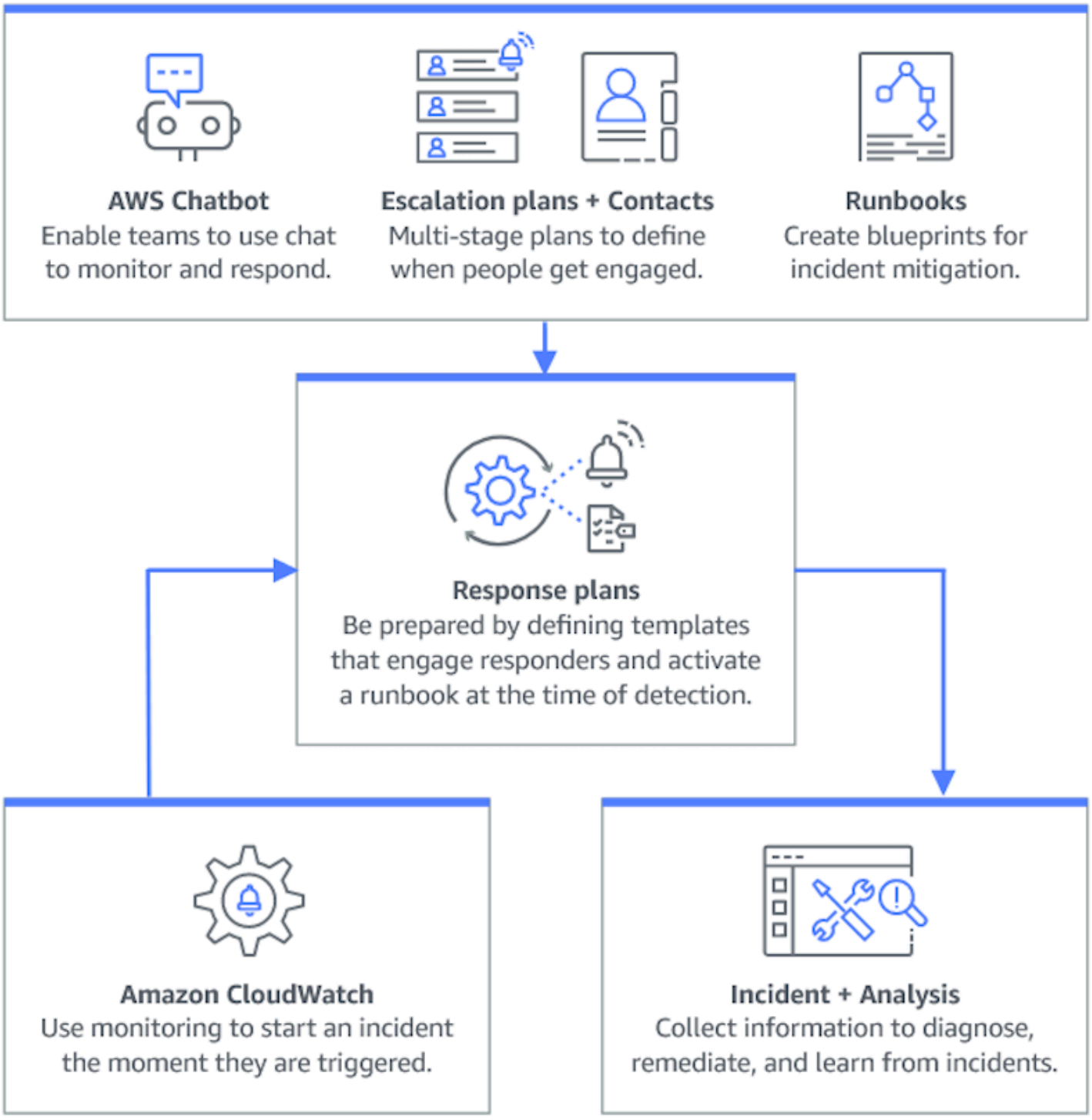
トのメンバーだけがその分析を表示および変更できます。管理アカウントを使用してインシデント後分析を作成した場合も同様です。

- アプリケーションアカウントで実行されるオートメーションドキュメントでは、タイムラインイベントは入力されません。アプリケーションアカウントで実行されるオートメーションドキュメントの更新は、インシデントの [ランブック] タブに表示されます。

- Amazon Simple Notification Service トピックは、クロスアカウントで使用できません。Amazon SNS トピックは、それを使用する対応計画と同じリージョンおよびアカウントで作成する必要があります。管理アカウントを使用して、すべての SNS トピックと対応計画を作成することをお勧めします。
- エスカレーション計画は、同じアカウントの連絡先を使用してのみ作成できます。共有されている連絡先は、アカウントのエスカレーション計画に追加できません。
- 対応計画、インシデントレコード、連絡先に適用されたタグは、リソース所有者アカウントからのみ表示および変更できます。

Incident Manager でのインシデントへの準備

インシデントの計画は、インシデントのライフサイクルのずっと前に始まります。インシデントの準備をするには、対応計画を作成する前に、次の各トピックを検討してください。モニタリング、連絡先、エスカレーション計画、チャットチャネル、ランブックを使用して、対応を自動化する対応計画を作成します。



トピック

- モニタリング
- 全般設定の使用
- Incident Manager での連絡先の操作

- Incident Manager でのオンコールスケジュールの操作
- Incident Manager でのエスカレーション計画の操作
- Incident Manager でのチャットチャネルの操作
- Incident Manager での Systems Manager Automation ランブックの操作
- Incident Manager での対応計画の操作
- Incident Manager での検出結果の使用

モニタリング

AWS ホストアプリケーションの健全性をモニタリングすることは、アプリケーションの稼働時間とパフォーマンスを確保する上で重要です。モニタリングソリューションを決定するときは、次の点を考慮してください。

- 機能の重要度 — システムに障害が発生した場合、ダウンストリームユーザーへの影響はどの程度重要になるか。
- エラーの共通性 - システムが故障する頻度はどの程度か。頻繁な介入を必要とするシステムは注意深くモニタリングする必要があります。
- レイテンシーの増加 — タスクを完了するための時間がどれだけ増加または減少したか。
- クライアント側とサーバー側のメトリクス — クライアントとサーバー上の関連メトリック間に不一致があるか。
- 依存関係障害 — チームで準備できる、また準備すべき障害。

応答計画を作成した後、モニタリングソリューションを使用して、環境内でインシデントが発生したときにインシデントを自動的に追跡できます。インシデントの追跡と作成の詳細については、「Incident Manager でのインシデントの追跡」を参照してください。

安全性、高パフォーマンス、耐障害性、効率性に優れたインフラストラクチャアプリケーションとワークロードのアーキテクチャの設計の詳細については、AWS Well-Architected」ホワイトペーパーを参照してください。

全般設定の使用

Incident Manager のオンボーディングウィザードを完了すると、設定ページで特定のオプションを管理できます。これらのオプションには、レプリケーションセット、レプリケーションセットに適用されたタグ、および検出結果機能が含まれます。

トピック

- Incident Manager レプリケーションセットの使用
- レプリケーションセットのタグの管理
- 検出結果機能の管理

Incident Manager レプリケーションセットの使用

Incident Manager のレプリケーションセットは、データを多くの AWS リージョン に複製し、リージョン間の冗長性を高め、Incident Manager が異なるリージョンのリソースにアクセスできるようにし、ユーザーのレイテンシーを短縮します。レプリケーションセットは、AWS マネージドキー またはお客様独自のカスタマーマネージドキーでデータを暗号化するためにも使用されます。すべての Incident Manager リソースは、デフォルトで暗号化されます。リソースの暗号化の詳細については、「Incident Manager でのデータ保護」を参照してください。Incident Manager を使用するには、まず準備 ウィザードを使用してレプリケーションセットを作成します。Incident Manager での準備の詳細については、準備ウィザード を参照してください。

レプリケーションセットの編集

Incident Manager の設定ページを使用して、レプリケーションセットを編集できます。リージョンの追加、リージョンの削除、およびレプリケーションセットの削除保護の有効化または無効化を行うことができます。データの暗号化に使用されるキーは編集できません。キーを変更するには、レプリケーションセットを削除して再作成します。

リージョンの追加

1. Incident Manager コンソールを開き、左のナビゲーションペインから [設定] を選択します。
2. [リージョンの追加] を選択します。
3. リージョンを選択します。
4. [Add] (追加) を選択します。

リージョンの削除

1. Incident Manager コンソールを開き、左のナビゲーションペインから [設定] を選択します。
2. 削除するリージョンを選択します。
3. [Delete] (削除) をクリックします。
4. テキストボックスに「削除」と入力し、[削除] を選択します。

レプリケーションセットの削除

レプリケーションセットの最後のリージョンを削除すると、レプリケーションセット全体が削除されます。最後のリージョンを削除する前に、削除保護 を 設定 でトグリングして無効にしてください。レプリケーションセットを削除した後、準備ウィザードを使用して新しいレプリケーションセットを作成できます。

レプリケーションセットからリージョンを削除するには、そのリージョンを作成してから 24 時間待ちます。作成後 24 時間以内にレプリケーションセットからリージョンを削除しようとすると失敗します。

レプリケーションセットを削除すると、Incident Manager のすべてのデータが削除されます。

レプリケーションセットを削除する

1. Incident Manager コンソールを開き、左のナビゲーションペインから [設定] を選択します。
2. レプリケーションセットの最後のリージョンを選択します。
3. [Delete] (削除) をクリックします。
4. テキストボックスに「削除」と入力し、[削除] を選択します。

レプリケーションセットのタグの管理

タグは、リソースに割り当てるオプションのメタデータです。タグを使用して、目的、所有者、環境などのさまざまな方法でリソースを分類します。

レプリケーションセットのタグを管理するには

1. Incident Manager コンソールを開き、左のナビゲーションペインから [設定] を選択します。
2. [タグ] 領域で [編集] を選択します。
3. タグを追加するには、次の操作を行います。
    a. [新しいタグを追加] をクリックします。
    b. タグのキーと、オプションで値を入力します。
    c. [Save (保存)] を選択します。
4. タグを削除するには、次の操作を行います。
    a. 削除するタグの下にある [削除] を選択します。

b. [Save (保存)] を選択します。

検出結果機能の管理

検出結果機能は、インシデント発生後すぐに、組織内の応答者がインシデントの潜在的な根本原因を特定するのに役立ちます。現在、Incident Manager は AWS CodeDeploy のデプロイと AWS CloudFormation スタックの更新に関する検出結果を提供しています。

検出結果をクロスアカウントでサポートするには、この機能を有効にした後に、組織内の各アプリケーションアカウントで追加の設定手順を完了する必要があります。

この機能を使用するには、ユーザーの代わりにデータにアクセスするために必要なアクセス許可を含むサービスロールを Incident Manager で作成します。

検出結果機能を有効にするには

1. Incident Manager コンソールを開き、左のナビゲーションペインから [設定] を選択します。
2. [検出結果] 領域で、[サービスロールを作成] を選択します。
3. 作成するサービスロールに関する情報を確認してから、[作成] を選択します。

検出結果機能を無効にするには

検出結果機能の使用を停止するには、`IncidentManagerIncidentAccessServiceRole` ロールが作成された各アカウントからこのロールを削除します。

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左のナビゲーションペインで、[Roles] (ロール) を選択します。
3. 検索ボックスに「**`IncidentManagerIncidentAccessServiceRole`**」と入力します。
4. ロールの名前を選択し、[削除] を選択します。
5. ダイアログボックスにロール名を入力してロールを削除することを確認したら、[削除] を選択します。

Incident Manager での連絡先の操作

AWS Systems Manager Incident Manager 連絡先はインシデントに対する応答者です。連絡先は、Incident Manager がインシデント中に関与できる複数のチャネルを持つことができます。連絡先

のエンゲージメント計画を定義して、Incident Manager が連絡先をエンゲージする方法とタイミングを定義できます。

トピック

- 問い合わせチャネル
- エンゲージメント計画
- 連絡先を作成
- 連絡先の詳細をアドレス帳にインポートする

問い合わせチャネル

問い合わせチャネルは、Incident Manager がお問い合わせをエンゲージするために使用するさまざまな方法です。

Incident Manager は、次の問い合わせチャネルをサポートしています。

- Email(メール)
- ショートメッセージサービス (SMS、Short Message Service)
- 音声

問い合わせチャネルのアクティベーション

プライバシーとセキュリティを保護するために、Incident Manager はお問い合わせを作成するときにデバイスアクティベーションコードを送信します。インシデント中にデバイスを操作するには、まずデバイスをアクティベーションする必要があります。これを行うには、お問い合わせの作成ページでデバイスのアクティベーションコードを入力します。

Incident Manager の特定の機能には、問い合わせチャネルに通知を送信する機能が含まれます。これらの機能を使用することにより、このサービスがサービスの中断やその他のイベントに関する通知を、指定されたワークフローに含まれる連絡先チャネルに送信することに同意したものとみなされます。これには、オンコールスケジュールのローテーションの一環として連絡先に送信される通知が含まれます。通知は、連絡先の詳細の指定どおりに、E メール、SMS メッセージ、または音声通話で送信されることがあります。これらの機能を使用して、Incident Manager に提供した連絡先チャネルを追加する権限があることを確認します。

オプトアウト

これらの通知は、モバイルデバイスを問い合わせチャネルとして削除することで、いつでもキャンセルできます。個々の通知受信者は、お問い合わせからデバイスを削除することで、いつでも通知をキャンセルできます。

お問い合わせから問い合わせチャネルを削除するには

1. Incident Manager コンソール に移動し、左のナビゲーションから お問い合わせ を選択します。
2. 削除する問い合わせチャネルをがあるお問い合わせを選択し、 編集を選択します。
3. 削除する問い合わせチャネルの横にある 削除 を選択します。
4. [更新] を選択します。

問い合わせチャネルの非アクティブ化

デバイスを非アクティブ化するには、UNSUBSCRIBEと返信します。UNSUBSCRIBE と返信すると、Incident Manager はデバイスを操作できなくなります。

問い合わせチャネルの再アクティベーション

1. Incident Manager からのメッセージに START と返信します。
2. Incident Manager コンソール に移動し、左のナビゲーションから お問い合わせ を選択します。
3. 削除する問い合わせチャネルをがあるお問い合わせを選択し、 編集を選択します。
4. サービスのアクティベーションを選択します。
5. Incident Manager からデバイスに送られてきた アクティベーションコード を入力します。
6. [アクティブ化] を選択します。

エンゲージメント計画

エンゲージメント計画は、Incident Manager が問い合わせチャネルをいつエンゲージメントするかを定義します。問い合わせチャネルは、エンゲージメントの開始から異なる段階で複数回エンゲージメントできます。エンゲージメント計画は、エスカレーション計画または対応計画で使用できます。エスカレーション計画の詳細については、「Incident Manager でのエスカレーション計画の操作」を参照してください。

連絡先を作成

連絡先を作成するには、以下のステップを使用します。

1. Incident Manager コンソール を開き、左のナビゲーションから お問い合わせ を選択します。
2. 問い合わせの作成 を選択します。
3. お問い合わせのフルネームを入力し、一意で識別可能なエイリアスを指定します。
4. 問い合わせチャネルを定義します。2 つ以上の異なるタイプの問い合わせチャネルを使用することをおすすめします。

   a. タイプ (E メール、SMS、音声) を選択します。

   b. 問い合わせチャネルの識別可能な名前を入力します。

   c. E メール: arosalez@example.com のような問い合わせチャネルの詳細を提供してください。
5. 複数の問い合わせチャネルを定義するには、問い合わせチャネルの追加を選択します。追加された新しい問い合わせチャネルごとに、ステップ 4 を繰り返します。
6. エンゲージメント計画を定義します。

   > **Important**
   > 連絡先をエンゲージするには、エンゲージメント計画を定義する必要があります。

   a. 問い合わせチャネル名を選択します。

   b. Incident Manager がこの問い合わせチャネルに参加するまでのエンゲージメントの開始から待機する分数を定義します。

   c. 別の問い合わせチャネルを追加するには、エンゲージメントの追加を選択します。
7. エンゲージメント計画を定義してから、作成を選択します。Incident Manager は、定義された各問い合わせチャネルにアクティベーションコードを送信します。
8. (オプション) 問い合わせチャネルをアクティベーションするには、Incident Manager が定義した各問い合わせチャネルに送信したアクティベーションコードを入力します。
9. (オプション) 新しいアクティベーションコードを送信するには、新しいコードを送信するを選択します。
10. [終了] を選択します。

お問い合わせを定義し、その問い合わせチャネルをアクティベーションしたら、エスカレーション計画にお問い合わせを追加して、エスカレーションのチェーンを形成できます。エスカレーション計画の詳細については、「Incident Manager でのエスカレーション計画の操作」を参照してください。直

接エンゲージメントの対応計画にお問い合わせを追加できます。対応計画の作成の詳細については、「Incident Manager での対応計画の操作」を参照してください。

連絡先の詳細をアドレス帳にインポートする

インシデントが作成されると、Incident Manager は音声通知または SMS 通知を使用して応答者に通知できます。呼び出しまたは SMS 通知が Incident Manager からのものであることを応答者に確認してもらうため、すべての応答者が Incident Manager の仮想カード形式 (.vcf) ファイルをモバイルデバイスのアドレス帳にダウンロードすることをお勧めします。ファイルは Amazon CloudFront でホストされており、AWS 商用パーティションで利用できます。

Incident Manager .vcf ファイルをダウンロードするには

1. モバイル端末で、以下の URL を選択または入力します: https://d26vhuvd5b89k2.cloudfront.net/aws-incident-manager.vcf。
2. ファイルをモバイルデバイスのアドレス帳に保存またはインポートします。

Incident Manager でのオンコールスケジュールの操作

Incident Manager のオンコールスケジュールでは、オペレータの介入が必要なインシデントが発生した場合に通知するユーザーを定義します。オンコールスケジュールは、そのスケジュール用に作成する 1 つまたは複数のローテーションで構成されます。各ローテーションには、最大 30 個の連絡先を含めることができます。

オンコールスケジュールを作成したら、エスカレーション計画にエスカレーションとして含めることができます。そのエスカレーション計画に関連するインシデントが発生すると、Incident Manager はスケジュールに従ってオンコールのオペレータに通知します。その後、この連絡先はエンゲージメントを確認できます。エスカレーション計画では、エスカレーションの複数のステージにわたって、1 つ以上のオンコールスケジュールおよび 1 つ以上の個別の連絡先を指定できます。詳細については、「Incident Manager でのエスカレーション計画の操作」を参照してください。

> **Tip**
>
> ベストプラクティスとして、エスカレーション計画のエスカレーションチャネルとして連絡先およびオンコールスケジュールを追加することをお勧めします。次に、対応計画のエンゲージメントとしてエスカレーション計画を選択する必要があります。このアプローチは、組織内のインシデント対応に対して最大限のカバレッジを提供します。

各オンコールスケジュールは最大 8 つのローテーションをサポートします。ローテーションは重複させることも、同時に実行することもできます。これにより、インシデント発生時に対応するよう通知されるオペレータの数が増えます。連続して実行するローテーションを作成することもできます。これにより、同じサービスをサポートするグループが世界中に存在する「フォローザサン」インシデント管理のようなシナリオが可能になります。

このセクションのトピックは、インシデント対応業務のオンコールスケジュールの作成と管理に役立ちます。

トピック

- Incident Manager でのオンコールスケジュールとローテーションの作成
- Incident Manager での既存のオンコールスケジュールの管理

Incident Manager でのオンコールスケジュールとローテーションの作成

連絡先のローテーションを 1 つ以上含むオンコールスケジュールを作成し、シフト中にインシデントに対応できるようにします。

開始する前に

オンコールスケジュールを作成する前に、スケジュールのローテーションに追加する連絡先を事前に作成していることを確認してください。詳細については、「Incident Manager での連絡先の操作」を参照してください。

夏時間 (DST、Daylight Savings Time) 変更の考慮

ローテーションを作成するときは、このローテーションに指定するシフトカバレッジ時間および日付の基準となるグローバルタイムゾーンを指定します。Internet Assigned Numbers Authority (IANA) によって定義された任意のタイムゾーンを使用できます。例: `America/Los_Angeles`、`UTC`、および `Asia/Seoul`。オンコールスケジュールに複数のローテーションを追加できます。ただし、各ローテーションの応答者が地理的に異なるタイムゾーンにいる場合は、各ローテーションが DST の変更の対象となる可能性があることに注意してください。

例えば、`America/Los_Angeles` と `Europe/Dublin` では異なる DST スケジュールが適用されます。そのため、これら 2 つのゾーンの時差は、その年の時期によって 6 時間から 8 時間まで変動する可能性があります。例えば、フォローザサンオンコールスケジュールでは、`America/Los_Angeles` および `Europe/Dublin` タイムゾーンにそれぞれ 1 つのローテーションがあるとします。この例では、DST の変更により、1 時間のシフトギャップまたは 1 時間のシフト重複がスケジュールに含まれることがあります。

このような状況を避けるため、以下のアプローチを推奨します。

1. オンコールスケジュールでのローテーションすべてに 1 つのタイムゾーンを使用します。
2. 特定のタイムゾーン外の応答者を割り当てる場合は、現地時間を計算します。

各ローテーションをローカルタイムゾーンに割り当てる場合は、DST の前にスケジュールを確認してください。次に、必要に応じてローテーションシフト時間を調整して、DST の変更が有効になる前に、オンコールカバレッジに意図しないギャップや重複が生じないようにします。

オンコールスケジュールを作成するには

1. Incident Manager コンソールを開きます。
2. 左のナビゲーションで [オンコールスケジュール] を選択します。
3. [オンコールスケジュールを作成] を選択します。
4. [スケジュール名] には、スケジュールを識別するのに役立つ名前 (**MyApp Primary On-call Schedule** など) を入力します。
5. [スケジュールエイリアス] には、現在の AWS リージョン では一意のエイリアス (**my-app-primary-on-call-schedule** など) を入力します。
6. (オプション) [タグ] 領域で、1 つ以上のタグキーの名前および値のペアをオンコールスケジュールに適用します。

   タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。例えば、スケジュールにタグを付けて、実行期間、含まれるオペレータのタイプ、サポートするエスカレーション計画を識別できます。Incident Manager リソースへのタグ付けの詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。
7. 続いて、オンコールスケジュールに 1 つ以上のローテーションを追加します。

Incident Manager でオンコールスケジュールのローテーションを作成する

オンコールスケジュールのローテーションは、シフトがいつ有効になるかを指定します。また、シフト交代制の連絡先も指定します。1 つのオンコールスケジュールに最大 8 つのローテーションを含めることができます。

Incident Manager で連絡先として作成した任意の個人をローテーションに追加できます。連絡先の管理については、「Incident Manager での連絡先の操作」を参照してください。

ローテーションを設定すると、ページ右側の [プレビュー] カレンダーで全体のスケジュールがどのように表示されるかを確認できます。

オンコールスケジュールのローテーションを作成するには

1. [オンコールスケジュールの作成] ページの [ローテーション 1] セクションで、[ローテーション名] に、ローテーションを識別する名前 (**`00:00 - 7:59 Support`** または **`Dublin Support Group`**) を入力します。
2. [開始日] には、このローテーションが有効になる日付を `YYYY/MM/DD` 形式 (`2023/07/14` など) で入力します。
3. [タイムゾーン] には、このローテーションで指定したシフトカバレッジ時間および日付の基準となるグローバルタイムゾーンを選択します。

   Internet Assigned Numbers Authority (IANA) によって定義された任意のタイムゾーンを使用できます。例:「America/Los_Angeles」、「UTC」、または「Asia/Seoul」。詳細については、IANA ウェブサイトの「タイムゾーンデータベース」を参照してください。

   > **Warning**
   >
   > 各ローテーションは独自のタイムゾーンに基づくことができます。ただし、選択したタイムゾーンで夏時間が変更されると、意図したカバレッジウィンドウに影響する可能性があります。詳細については、このトピックで先述した「夏時間 (DST、Daylight Savings Time) 変更の考慮」を参照してください。

4. [ローテーション開始時刻] には、このローテーションの開始時刻を 24 時間 `hh:mm` 形式 (`16:00` など) で入力します。

   指定したタイムゾーンと異なるタイムゾーンにいる連絡先の現地時間の違いに注意してください。例えば、`America/Los_Angeles` をタイムゾーンとして、`00:00` をローテーション開始時間としてそれぞれ選択した場合、アイルランドのダブリンでは 08:00、インドのムンバイでは 13:30 になります。

5. [ローテーション終了時刻] には、このローテーションの終了時刻を 24 時間 `hh:mm` 形式 (`23:59` など) で入力します。

   > **Note**
   >
   > ローテーションの開始から終了までの時間は 30 分以上でなければなりません。

6. (オプション) ローテーションの長さを 24 時間に設定するには、[24 時間カバレッジ] を選択し、[ローテーション開始時刻] フィールドにこのローテーションの開始時刻を入力します。[ローテーション終了時刻] の値は自動的に更新されます。

   例えば、オンコールを 24 時間カバレッジにして、午前 11 時にシフトを変更する場合は、[24 時間カバレッジ] を選択し、開始時間として **`11:00`** を入力します。
7. [有効日数] には、このローテーションが有効な曜日を選択します。例えば、オンコール計画に週末のカバレッジを含めない場合は、[日曜日] と [土曜日] を除くすべての日を選択します。
8. 続けて連絡先をローテーションに追加します。

Incident Manager でオンコールスケジュールのローテーションに連絡先を追加する

オンコールスケジュールのローテーションごとに、1 人以上の連絡先を合計 30 人まで追加できます。Incident Manager の設定で設定されている連絡先から選択します。

連絡先をローテーションに追加すると、その連絡先はオンコール業務の一環として通知を受け取ることがあります。通知は、連絡先の詳細の指定どおりに、E メール、SMS、または音声通話で送信されることがあります。

連絡先の管理および連絡先の通知オプションについては、「Incident Manager での連絡先の操作」を参照してください。

オンコールスケジュールのローテーションに連絡先を追加するには

1. [オンコールスケジュールの作成] ページのローテーションの [連絡先] セクションで、[連絡先を追加または削除する] を選択します。
2. [連絡先の追加または削除] ダイアログボックスで、ローテーションに含める連絡先のエイリアスを選択します。

   連絡先を選択する順序は、ローテーションスケジュールで最初にリストされた順序です。連絡先を追加した後で順序を変更できます。
3. [確認] を選択します。
4. 連絡先の順序を変更するには、そのユーザーのラジオボタンを選択し、Up
   ( )
   ボタンと Down
   ( )
   ボタンを使用して連絡先の順序を更新します。

5. 続けて、ローテーションに対して個々のシフトの繰り返しおよび長さを指定してください。

Incident Manager でシフトの繰り返しと長さを指定し、ローテーションにタグを追加する

シフト繰り返しは、ローテーション内の連絡先がオンコールに出入りする頻度を指定します。繰り返しの長さは、日数、週数、または月数で指定できます。

シフトの繰り返しと長さを指定し、ローテーションにタグを追加するには

1. [オンコールスケジュールの作成] ページのローテーションの [繰り返し設定] セクションで、以下の操作を行います。

   - [シフトの繰り返しタイプ] では、`Daily`、`Weekly`、および `Monthly` から選択して、各オンコールのシフトの継続期間が日単位、週単位、または月単位のいずれかであるかを指定します。
   - [シフトの長さ] には、シフトの継続日数、週数、または月数を入力します。

     例えば、`Daily` を選択して **1** を入力した場合、各連絡先のオンコールシフトは 1 日続きます。`Weekly` を選択して **3** を入力した場合、各連絡先のオンコールシフトは 3 週間続きます。
2. (オプション) [タグ] 領域で、1 つ以上のタグキーの名前と値のペアをローテーションに適用します。

   タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。例えば、ローテーションにタグを付けて、割り当てられた連絡先の場所、提供される予定のカバレッジのタイプ、サポートするエスカレーション計画を特定できます。Incident Manager リソースへのタグ付けの詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。
3. (推奨) カレンダーのプレビューを使用して、オンコールスケジュールのカバレッジに意図しないギャップがないことを確認します。
4. [Create] (作成) を選択します。

オンコールスケジュールをエスカレーション計画のエスカレーションチャネルとして追加できるようになりました。詳細については、エスカレーション計画を作成するを参照してください。

Incident Manager での既存のオンコールスケジュールの管理

このセクションの内容は、作成済みのオンコールスケジュールの操作に役立ちます。

トピック

- オンコールスケジュールの詳細を表示する
- オンコールスケジュールの編集
- オンコールスケジュールのコピー
- オンコールスケジュールローテーションに対する上書きの作成
- オンコールスケジュールを削除する

オンコールスケジュールの詳細を表示する

[オンコールスケジュールの詳細を表示] ページでは、オンコールスケジュールの概要をひとめで確認できます。このページには、現在誰がオンコールで、次に誰がオンコールになるかについての情報も含まれています。このページには、特定の時間にどの連絡先がオンコールであるかを示すカレンダービューがあります。

オンコールスケジュールの詳細を表示するには

1. Incident Manager コンソールを開きます。
2. 左のナビゲーションで [オンコールスケジュール] を選択します。
3. オンコールスケジュールを表示する行で、以下のいずれかを実行します。

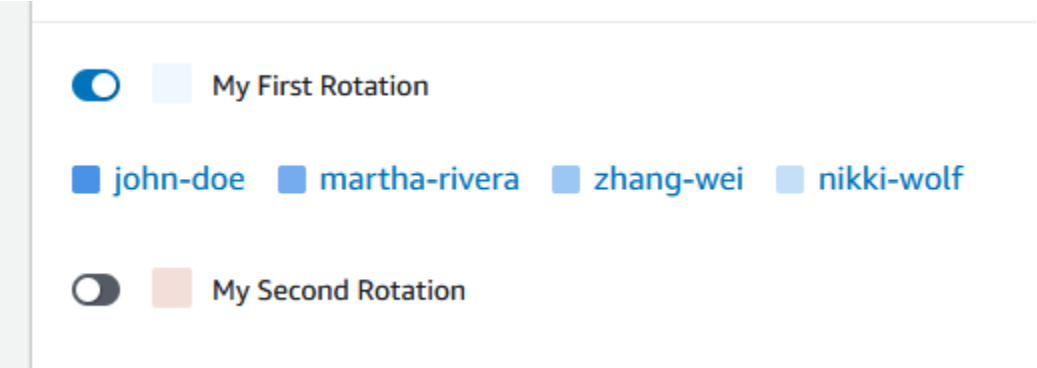
   - カレンダーの概要ビューを開くには、スケジュールエイリアスを選択します。

     -または-

     行のラジオボタンを選択し、[表示] を選択します。
   - スケジュールのカレンダービューを開くには、[カレンダーを表示]

     を選択します。

     カレンダービューで、スケジュールの特定の日付の連絡先の名前を選択すると、割り当てられたシフトの詳細を確認したり、上書きを作成したりできます。
   - カレンダー内の特定のローテーションの表示をオンまたはオフにするには、ローテーション名の横にあるスイッチを選択します。



オンコールスケジュールの編集

オンコールスケジュールおよびそのローテーションの設定を更新できますが、以下の詳細は更新できません。

- スケジュールエイリアス
- ローテーション名
- ローテーション開始日

これらの値を変更できる新しいカレンダーの基礎として既存のカレンダーを使用するには、代わりにカレンダーをコピーできます。詳細については、オンコールスケジュールのコピーを参照してください。

オンコールスケジュールを編集するには

1. Incident Manager コンソールを開きます。
2. 左のナビゲーションで [オンコールスケジュール] を選択します。
3. 次のいずれかを実行します。
    - 編集するオンコールスケジュールの行にあるラジオボタンを選択し、[編集] を選択します。
    - オンコールスケジュールのスケジュールエイリアスを選択して [オンコールスケジュールの詳細を表示] ページを開き、[編集] を選択します。
4. オンコールスケジュールおよびそのローテーションに必要な変更を加えます。開始時刻、終了時刻、連絡先、および繰り返しなどのローテーション設定オプションを変更できます。必要に応じて、スケジュールのローテーションを追加または削除できます。変更を加えると、カレンダーのプレビューに反映されます。

ページ上のオプションの使用方法については、「Incident Manager でのオンコールスケジュールとローテーションの作成」を参照してください。

5. [更新] を選択します。

> **Important**
>
> 上書きを含むスケジュールを編集すると、変更内容が上書きに影響する可能性があります。上書きが期待どおりに設定されていることを確認するには、スケジュールを更新した後、シフト上書きを注意深く見直すことをお勧めします。

オンコールスケジュールのコピー

既存のオンコールスケジュールの設定を新しいスケジュールの出発点として使用するには、カレンダーのコピーを作成し、必要に応じて変更することができます。

オンコールスケジュールをコピーするには

1. Incident Manager コンソールを開きます。
2. 左のナビゲーションで [オンコールスケジュール] を選択します。
3. コピーするオンコールスケジュールの行にあるラジオボタンを選択します。
4. [Copy] (コピー) を選択します。
5. カレンダーおよびそのローテーションに必要な変更を加えます。ローテーションは必要に応じて変更、追加、または削除できます。

   > **Note**
   >
   > 既存のスケジュールをコピーする場合、ローテーションごとに新しい開始日を指定する必要があります。コピーしたスケジュールは、開始日が過去のローテーションをサポートしていません。

   ページ上のオプションの使用方法については、「Incident Manager でのオンコールスケジュールとローテーションの作成」を参照してください。

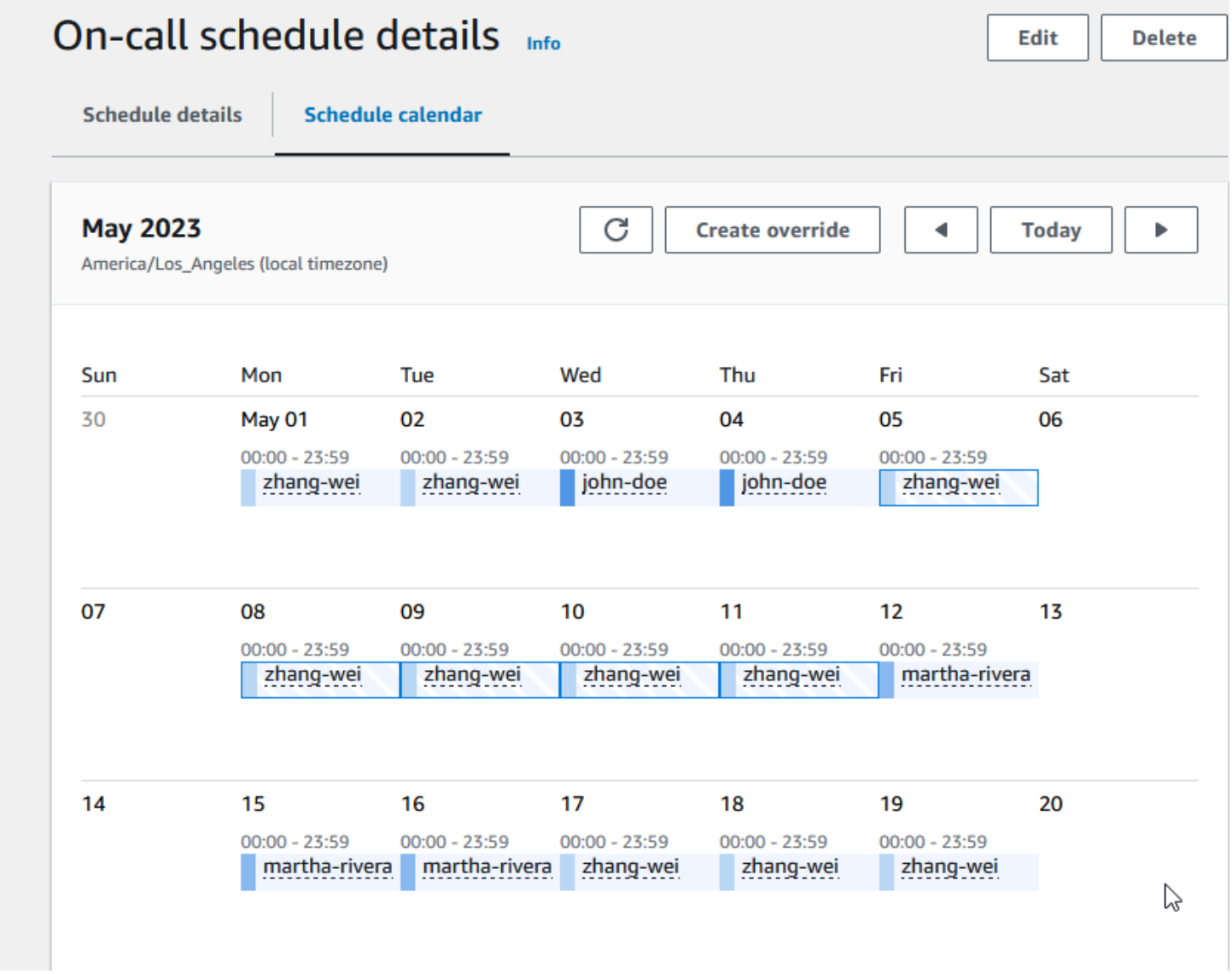
6. [Create copy] (コピーを作成) を選択します。

オンコールスケジュールローテーションに対する上書きの作成

既存のローテーションスケジュールに 1 回限りの変更を加える必要がある場合は、上書きを作成できます。上書きにより、連絡先のシフトのすべてまたは一部を別の連絡先に置き換えることができます。複数のシフトにまたがる上書きを作成することもできます。

連絡先は、ローテーションに既に割り当てられているもののみ上書きに割り当てることができます。

カレンダープレビューでは、上書きされたシフトは、単色の背景ではなく縞模様の背景で表示されます。以下の画像では、John Doe と Martha Rivera のシフトの一部を含む上書きで、5 月 5 日から 5 月 11 日にかけて Zhang Wei がオンコールであることがわかります。



オンコールスケジュールに対して上書きを作成するには

1. Incident Manager コンソールを開きます。
2. 左のナビゲーションで [オンコールスケジュール] を選択します。
3. オンコールスケジュールを表示する行で、以下のいずれかを実行します。
   - スケジュールエイリアスを選択し、次に [スケジュールカレンダー] タブを選択します。
   - [カレンダーを表示]

     を選択します。
4. 次のいずれかを実行します。
   - [上書きを作成] を選択します。
   - カレンダープレビューで連絡先の名前を選択し、[シフトを上書き] を選択します。
5. [シフト上書きの作成] ダイアログボックスで、以下の操作を実行します。

   > **Note**
   > 上書きの長さは少なくとも 30 分である必要があります。上書きは、6 か月以内に発生するシフトに対してのみ指定できます。

   a. [ローテーションを選択] では、上書きを作成するローテーションの名前を選択します。
   b. [開始日] には、上書きを開始する日付を選択または入力します。
   c. [開始時刻] には、上書きを開始する時刻を hh:mm フォーマットで入力します。
   d. [終了日] には、上書きが終了する日付を選択または入力します。
   e. [終了時刻] には、上書きが終了する時刻を hh:mm フォーマットで入力します。
   f. [上書き連絡先を選択] では、上書き期間中にオンコールのローテーション連絡先の名前を選択します。
6. [上書きを作成] を選択します。

上書きを作成すると、縞模様の背景で識別できます。上書きされたシフトの連絡先名を選択すると、そのシフトが上書きされたシフトであることが情報ボックスに表示されます。[上書きを削除] を選択して上書きを削除し、元のオンコール割り当てに復元することができます。

オンコールスケジュールを削除する

特定のオンコールスケジュールが不要になった場合は、Incident Manager から削除できます。

現在、オンコールスケジュールをエスカレーションチャネルとして使用しているエスカレーション計画または対応計画がある場合は、スケジュールを削除する前にそれらの計画からスケジュールを削除する必要があります。

オンコールスケジュールを削除するには

1. Incident Manager コンソールを開きます。
2. 左のナビゲーションで [オンコールスケジュール] を選択します。
3. 削除するオンコールスケジュールの行にあるラジオボタンを選択します。
4. [Delete] (削除) をクリックします。
5. [オンコールスケジュールを削除しますか?] ダイアログボックスで、テキストボックスに **`confirm`** を入力します。
6. [Delete] (削除) をクリックします。

Incident Manager でのエスカレーション計画の操作

AWS Systems Manager Incident Manager は、定義済みの連絡先やオンコールスケジュールへのエスカレーションパス (エスカレーションチャネル) を提供します。複数のエスカレーションチャネルを同時に 1 つのインシデントに取り込むことができます。エスカレーションチャネルに指定されている連絡先が応答しない場合、Incident Manager は次の連絡先にエスカレーションします。ユーザーがエンゲージメントを承認した後、計画のエスカレーションを停止するかどうかを選択することもできます。エスカレーション計画を対応計画に追加して、インシデントの開始時にエスカレーションが自動的に開始されるようにできます。アクティブなインシデントにエスカレーション計画を追加することもできます。

トピック

- ステージ
- エスカレーション計画を作成する

ステージ

エスカレーション計画では、各ステージが定義された分数を持続するステージを使用します。各ステージには次の情報があります。

- 期間 - 次のステージを開始するまで計画が待機する時間。エスカレーション計画の第 1 ステップは、エンゲージメントが開始されると開始されます。
- エスカレーションチャネル — エスカレーションチャネルとは、単一の連絡先、または定義済みのスケジュールに従って責任をローテーションする複数の連絡先で構成されるオンコールスケジュールです。エスカレーション計画では、定義されたエンゲージメント計画を使用して、各チャネルをエンゲージメントします。次のステージに進む前に、エスカレーション計画の進行を停止するように各エスカレーションチャネルを設定できます。各ステージには、複数のエスカレーションチャネルを含めることができます。

  個別の連絡先のセットアップについては、「Incident Manager での連絡先の操作」を参照してください。オンコールスケジュールの作成については、「Incident Manager でのオンコールスケジュールの操作」を参照してください。

エスカレーション計画を作成する

1. Incident Manager コンソール を開き、左のナビゲーションから エスカレーション計画 を選択します。
2. エスカレーション計画の作成を選択します。
3. [名前] にエスカレーション計画の一意の名前 (**`My Escalation Plan`**など) を入力します。
4. [エイリアス] には、計画の識別に役立つエイリアス (など**`my-escalation-plan`**) を入力します。
5. [ステージの期間] には、Incident Manager が次のステージに進むまでに待機する分数を入力します。
6. [エスカレーションチャネル] には、このステージ中にエンゲージメントする連絡先またはオンコールスケジュールを 1 つ以上選択します。
7. (オプション) 連絡先がエンゲージメントを承認したときにエスカレーション計画を停止させるには、[プランの進行停止を承認] を選択します。
8. このステージに別のチャネルを追加するには、[エスカレーションチャネルを追加してください] を選択します。
9. エスカレーション計画に別のステージを追加するには、[ステージを追加] を選択します。

10. このエスカレーション計画に必要なエスカレーションチャネルとステージの追加が完了するまで、手順 5～9 を繰り返します。
11. (オプション) [タグ] 領域で、1 つ以上のタグキーの名前と値のペアをエスカレーション計画に適用します。

    タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。例えば、エスカレーション計画にタグを付けて、この計画を使用するインシデントの種類、この計画に含まれるエスカレーションチャネルの種類、この計画がサポートするエスカレーション計画を識別できます。Incident Manager リソースへのタグ付けの詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。
12. エスカレーション計画の作成を選択します。

Incident Manager でのチャットチャネルの操作

AWS Systems Manager の一機能である Incident Manager により、インシデント応答者はインシデント中にチャットチャネルを通じて直接連絡を取ることができます。チャットチャネルは、AWS Chatbot でセットアップするチャットルームです。次に、このチャネルを Incident Manager の対応計画に接続します。

インシデント中に、応答者はチャットチャネルを使用してインシデントについて互いに連絡を取ります。また、Incident Manager は、インシデントに関する更新や通知をチャットチャネルに直接プッシュします。Incident Manager は、これらの通知をチャットルーム設定で指定した 1 つ以上の Amazon Simple Notification Service (Amazon SNS) トピックを使用して送信します。

AWS Chatbot および Incident Manager は、以下のアプリケーションのチャットチャネルをサポートしています。

- Slack
- Microsoft Teams
- Amazon Chime

インシデントで使用するチャットチャネルをセットアップするプロセスは、3 つの異なる Amazon Web Services サービスのタスクで構成されています。

タスク

- タスク 1: チャットチャネルの Amazon SNS トピックを作成または更新する

- タスク 2: AWS Chatbot でチャットチャネルを作成する
- タスク 3: Incident Manager の対応計画にチャットチャネルを追加する
- チャットチャネルを通じた対話

タスク 1: チャットチャネルの Amazon SNS トピックを作成または更新する

Amazon SNS は、パブリッシャーからサブスクライバー (生産者および消費者とも呼ばれます) へのメッセージ配信を提供するマネージドサービスです。発行者は、論理アクセスポイントおよび通信チャネルであるトピックにメッセージを送信することで、受信者と非同期的に通信します。Incident Manager は、ユーザーが対応計画に関連付けた 1 つ以上のトピックを使用して、インシデントに関する通知をインシデント応答者に送信します。

対応計画では、1 つ以上の Amazon SNS トピックをインシデント通知に含めることができます。ベストプラクティスとして、レプリケーションセットに追加した各 AWS リージョン に SNS トピックを作成する必要があります。

> **Tip**
>
> より線形なセットアップワークフローを実現するには、まず Amazon SNS トピックを Incident Manager で使用するように設定することをお勧めします。設定が完了したら、チャットチャネルを作成できます。

チャットチャネルの Amazon SNS トピックを作成または更新するには

1. 「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS トピックを作成」の手順を行います。

   > **Note**
   >
   > トピックを作成した後、トピックを編集してアクセスポリシーを更新します。

2. 作成したトピックを選択し、トピックの Amazon リソースネーム (ARN) を `arn:aws:sns:us-east-2:111122223333:My_SNS_topic` などの形式でメモするかコピーします。
3. [編集] を選択し、[アクセスポリシー] セクションを展開して、デフォルト以外の追加のアクセス許可を設定します。

4. 以下のステートメントをポリシーの [ステートメント] 配列に追加します。

```
{
    "Sid": "IncidentManagerSNSPublishingPermissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "sns-topic-arn",
    "Condition": {
        "StringEqualsIfExists": {
            "AWS:SourceAccount": "account-id"
        }
    }
}
```

*##########*を以下のように置き換えます。

- *sns-topic-arn* は、このリージョン用に作成したトピックの Amazon リソースネーム (ARN) で、形式は `arn:aws:sns:us-east-2:111122223333:My_SNS_topic` です。
- *account-id* は、ユーザーが作業している AWS アカウント の ID (111122223333 など) です。

5. [Save changes] (変更の保存) をクリックします。
6. レプリケーションセットに含まれる各リージョンでこの処理を繰り返します。

タスク 2: AWS Chatbot でチャットチャネルを作成する

チャットチャネルは、Slack、Microsoft Teams、または Amazon Chime で作成できます。対応計画ごとに必要なチャットチャネルは 1 つだけです。

チャットチャネルについては、最小特権のプリンシパルに従うことをお勧めします (タスクを完了するために必要以上のアクセス許可をユーザーに与えない)。また、AWS Chatbot チャットチャネルのメンバーシップも定期的に確認する必要があります。レビューは、適切な応答者および他のステークホルダーのみがチャットチャネルにアクセスできることを確認するのに役立ちます。

AWS Chatbot が有効な Slack チャネルおよび Microsoft Teams チャネルでは、インシデント応答者は Slack または Microsoft Teams アプリケーションから複数の Incident Manager CLI コマンドを直接実行できます。詳細については、「チャットチャネルを通じた対話」を参照してください。

> **Important**
>
> チャットチャネルに追加するユーザーは、エスカレーション計画または対応計画に記載されている連絡先と同じである必要があります。また、ステークホルダーおよびインシデントオブザーバーなどのユーザーをチャットチャネルに追加することもできます。

AWS Chatbot の一般情報については、「AWS Chatbot Administrator Guide」の「What is AWS Chatbot」を参照してください。

チャネルを作成するアプリケーションを以下から選択してください。

Slack

この手順のステップでは、すべてのチャネルユーザーが Incident Manager でチャットコマンドを使用できるようにするために、推奨されるアクセス許可設定を示します。サポートされているチャットコマンドを使用すると、インシデント応答者は Slack チャットチャネルから直接インシデントを更新して、対話できます。詳細については、チャットチャネルを通じた対話を参照してください。

Slack でチャットチャネルを作成するには

- 「AWS Chatbot Administrator Guide」の「Tutorial: Get started with Slack」の手順に従い、設定に以下を含めてください。
  - ステップ 10 の [ロール設定] で [チャネルロール] を選択します。
  - ステップ 10d の [ポリシーテンプレート] で、[Incident Manager のアクセス許可] を選択します。
  - ステップ 11 の [チャネルガードレールのポリシー] の、[ポリシー名] で [AWSIncidentManagerResolverAccess] を選択します。
  - ステップ 12 の [SNS トピック] セクションで、以下の操作を行います。
    - [リージョン 1] で、レプリケーションセットに含まれる AWS リージョン を選択します。
    - [トピック 1] で、そのリージョンで作成した SNS トピックを選択し、チャットチャネルへのインシデント通知の送信に使用します。
    - レプリケーションセット内のリージョンを追加するたびに、[別のリージョンを追加] を選択し、リージョンおよび SNS トピックを追加します。

Microsoft Teams

この手順のステップでは、すべてのチャネルユーザーが Incident Manager でチャットコマンドを使用できるようにするために、推奨されるアクセス許可設定を示します。サポートされているチャットコマンドを使用すると、インシデント応答者は Microsoft Teams チャットチャネルから直接インシデントを更新して、対話できます。詳細については、チャットチャネルを通じた対話を参照してください。

Microsoft Teams でチャットチャネルを作成するには

- 「AWS Chatbot Administrator Guide」の「Tutorial: Get started with Microsoft Teams」の手順に従い、設定に以下を含めてください。
  - ステップ 10 の [ロール設定] で [チャネルロール] を選択します。
  - ステップ 10d の [ポリシーテンプレート] で、[Incident Manager のアクセス許可] を選択します。
  - ステップ 11 の [チャネルガードレールのポリシー] の、[ポリシー名] で [AWSIncidentManagerResolverAccess] を選択します。
  - ステップ 12 の [SNS トピック] セクションで、以下の操作を行います。
    - [リージョン 1] で、レプリケーションセットに含まれる AWS リージョン を選択します。
    - [トピック 1] で、そのリージョンで作成した SNS トピックを選択し、チャットチャネルへのインシデント通知の送信に使用します。
    - レプリケーションセット内のリージョンを追加するたびに、[別のリージョンを追加] を選択し、リージョンおよび SNS トピックを追加します。

Amazon Chime

Amazon Chime でチャットチャネルを作成するには

- 「AWS Chatbot Administrator Guide」の「Tutorial: Get started with Amazon Chime」の手順に従い、設定に以下を含めてください。
  - ステップ 11 の [ポリシーテンプレート] で、[Incident Manager のアクセス許可] を選択します。
  - ステップ 12 の [SNS トピック] セクションで、Amazon Chime ウェブフックに通知を送信する SNS トピックを選択します。

- [リージョン 1] で、レプリケーションセットに含まれる AWS リージョン を選択します。
- [トピック 1] で、そのリージョンで作成した SNS トピックを選択し、チャットチャネルへのインシデント通知の送信に使用します。
- レプリケーションセット内のリージョンを追加するたびに、[別のリージョンを追加] を選択し、リージョンおよび SNS トピックを追加します。

> **Note**
>
> インシデント応答者が Slack や Microsoft Teams のチャットチャネルで使用できるチャットコマンドは、Amazon Chime ではサポートされていません。

タスク 3: Incident Manager の対応計画にチャットチャネルを追加する

対応計画を作成または更新するときに、応答者が連絡を取り、最新情報を受け取るためのチャットチャネルを追加できます。

「対応計画の作成」の手順に従うときは、セクション「(オプション) インシデント対応チャットチャネルの指定」で、この対応計画に関連するインシデントに使用するチャネルを選択してください。

チャットチャネルを通じた対話

Slack および Microsoft Teams のチャネルの場合、Incident Manager を使用すると、応答者は以下の `ssm-incidents` コマンドを使用してチャットチャネルから直接インシデントと対話できるようになります。

- start-incident
- list-response-plan
- get-response-plan
- create-timeline-event
- delete-timeline-event
- get-incident-record
- get-timeline-event
- list-incident-records

- list-timeline-events
- list-related-items
- update-related-items
- update-incident-record
- update-timeline-event

アクティブなインシデントのチャットチャネルでコマンドを実行するには、以下の形式を使用します。*cli-options* は、コマンドに含めるオプションに置き換えてください。

```
@aws ssm-incidents cli-options
```

例:

```
@aws ssm-incidents start-incident --response-plan-arn arn:aws:ssm-
incidents::111122223333:response-plan/test-response-plan-chat --region us-east-2
```

```
@aws ssm-incidents create-timeline-event --event-data "\"example timeline event"\" --
event-time 2023-03-31 T20:30:00.000  --event-type Custom Event --incident-record-arn
 arn:aws:ssm-incidents::111122223333:incident-record/MyResponsePlanChat/98c397e6-7c10-
aa10-9b86-f199aEXAMPLE
```

```
@aws ssm-incidents list-incident-records
```

Incident Manager での Systems Manager Automation ランブックの操作

AWS Systems Manager の機能である AWS Systems Manager Automation のランブックを使用して、AWS クラウド 環境内のアプリケーションとインフラストラクチャの一般的なタスクを自動化できます。

各ランブックはランブックワークフローを定義します。ランブックワークフローは、Systems Manager がマネージドノードまたは他の AWS リソースタイプに対して実行するアクションで構成されます。ランブックを使用すると、AWS リソースのメンテナンス、デプロイ、修復を自動化できます。

Incident Manager では、ランブックがインシデント対応および緩和を促進し、対応計画の一部として使用するランブックを指定します。

対応計画では、一般的に自動化されるタスク用に事前設定された数十のランブックから選択することも、カスタムランブックを作成することもできます。対応計画定義でランブックを指定すると、インシデントが発生するとシステムが自動的にランブックを起動できます。

> **Important**
>
> クロスリージョンフェイルオーバーによって作成されたインシデントは、対応計画で指定されているランブックを呼び出しません。

Systems Manager Automation、ランブック、および Incident Manager でのランブックの使用の詳細については、以下のトピックを参照してください。

- 対応計画にランブックを追加する方法については、「Incident Manager での対応計画の操作」を参照してください。
- ランブックについて詳しくは、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager Automation」および「AWS Systems Manager Automation runbook reference」を参照してください。
- ランブックの使用料金については、「Systems Manager の料金」を参照してください。
- Amazon CloudWatch アラームまたは Amazon EventBridge イベントによってインシデントが作成されたときに自動的にランブックを呼び出す方法については、「Tutorial: Using Systems Manager Automation runbooks with Incident Manager」を参照してください。

トピック

- ランブックワークフローの開始と実行に必要な IAM アクセス許可
- ランブックパラメータの使用
- ランブックを定義する
- Incident Manager ランブックテンプレート

ランブックワークフローの開始と実行に必要な IAM アクセス許可

Incident Manager には、インシデント対応の一環としてランブックを実行するアクセス許可が必要です。これらのアクセス許可を付与するには、AWS Identity and Access Management (IAM) ロール、ランブックサービスロール、およびオートメーション `AssumeRole` を使用します。

ランブックサービスロールは必須のサービスロールです。このロールは、Incident Manager に対して、ランブックのワークフローにアクセスして開始するために必要なアクセス許可を付与します。

オートメーション `AssumeRole` はランブック内で指定されている個々のコマンドを実行するのに必要なアクセス許可を付与します。

> **Note**
>
> `AssumeRole` が指定されていない場合、Systems Manager Automation は個々のコマンドにランブックサービスロールを使用しようとします。`AssumeRole` を指定しない場合は、ランブックサービスロールに必要なアクセス許可を追加する必要があります。追加しないと、ランブックはそれらのコマンドの実行に失敗します。
> ただし、セキュリティのベストプラクティスとして、別の `AssumeRole` の使用をお勧めします。別の `AssumeRole` を使用すると、各ロールに追加しなければならない必要なアクセス許可を制限できます。

オートメーション `AssumeRole` について詳しくは、「AWS Systems Manager ユーザーガイド」の「オートメーションのサービスロール (ロールを引き受ける) アクセスの設定」を参照してください。

どちらのタイプのロールも IAM コンソールで手動で作成できます。対応計画を作成または更新する場合、Incident Manager にどちらかのロールを作成させることもできます。

ランブックサービスロールのアクセス許可

ランブックサービスロールアクセス許可は、以下のようなポリシーによって提供されます。

最初のステートメントにより、Incident Manager は Systems Manager `StartAutomationExecution` オペレーションを開始できます。このオペレーションは、3 つの Amazon リソースネーム (ARN) 形式で表されるリソース上で実行されます。

2 番目のステートメントにより、ランブックが影響を受けたアカウントで実行されるときに、ランブックサービスロールが別のアカウントのロールを引き受けることができます。詳細については、

「AWS Systems Manager ユーザーガイド」の「複数の AWS リージョン とアカウントでのオートメーションの実行」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartAutomationExecution",
      "Resource": [
        "arn:aws:ssm:*:{{DocumentAccountId}}:automation-definition/{{DocumentName}}:*",
        "arn:aws:ssm:*:{{DocumentAccountId}}:document/{{DocumentName}}:*",
        "arn:aws:ssm:*::automation-definition/{{DocumentName}}:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-AutomationExecutionRole",
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

オートメーション AssumeRole アクセス許可

対応計画を作成または更新する場合、Incident Manager が作成する AssumeRole にアタッチする AWS マネージドポリシーは、複数の中から選択できます。これらのポリシーは、Incident Manager ランブックシナリオで使用されるさまざまな一般的なオペレーションを実行するアクセス許可を付与します。これらのマネージドポリシーを 1 つ以上選択して、AssumeRole ポリシーにアクセス許可を付与できます。 以下の表では、Incident Manager コンソールから AssumeRole を作成するときに選択できるポリシーについて説明します。

AWS マネージドポリシー名	ポリシーの説明
AmazonSSMAutomationRole	Systems Manager Automation サービスにランブックで定義されているアクティビティを実行

AWS マネージドポリシー名	ポリシーの説明
	するためのアクセス許可を付与します。このポリシーは、管理者および信頼されたパワーユーザーに割り当てます。
AWSIncidentManagerResolverAccess	ユーザーにインシデントを開始、表示、更新するアクセス許可を付与します。それらを使用して、インシデントダッシュボードで顧客のタイムラインイベントおよび関連アイテムを作成することもできます。

これらのマネージドポリシーを使用して、多くの一般的なインシデント対応シナリオにアクセス許可を付与できます。ただし、必要な特定のタスクに必須のアクセス許可は異なる場合があります。このような場合は、AssumeRole に追加のポリシーアクセス許可を付与する必要があります。詳細については、「AWS Systems Manager Automation runbook reference」を参照してください。

ランブックパラメータの使用

応答プランに Runbook を追加する場合、Runbook が実行時に使用するパラメータを指定できます。応答プランでは、静的な値と動的な値の両方を持つパラメータをサポートします。静的な値の場合、応答プランでパラメータを定義するときに値を入力します。動的な値の場合、システムはインシデントから情報を収集することによって正しいパラメータ値を決定します。Incident Manager は、次の動的なパラメータをサポートしています。

`Incident ARN`

Incident Manager がインシデントを作成すると、システムは対応するインシデントレコードの Amazon リソースネーム (ARN) をキャプチャし、それを Runbook にあるこのパラメータに入力します。

> **Note**
>
> この値は、タイプ `String` のパラメータにのみ割り当てることができます。他のタイプのパラメータに割り当てられた場合、Runbook は実行に失敗します。

`Involved resources`

Incident Manager がインシデントを作成すると、システムはインシデントに関連するリソースの ARN をキャプチャします。その後、これらのリソース ARN は、Runbook のこのパラメータに割り当てられます。

関連付けられたリソースについて

Incident Manager は、CloudWatch アラーム、EventBridge イベント、および手動で作成されたインシデントで指定された AWS リソースの ARN をランブックパラメータ値に入力できます。このセクションでは、Incident Manager がこのパラメータにデータを入力するときに ARN をキャプチャできるさまざまなタイプのリソースについて説明します。

CloudWatch アラーム

CloudWatch アラームアクションからインシデントが作成されると、Incident Manager は関連するメトリクスから以下のタイプのリソースを自動的に抽出します。その後、選択したパラメータに以下の関連リソースを入力します。

AWS のサービス	リソースタイプ
Amazon DynamoDB	グローバルセカンダリインデックス Streams テーブル
Amazon EC2	イメージ インスタンス
AWS Lambda	関数のエイリアス 関数のバージョン 関数
Amazon Relational Database Service (Amazon RDS)	クラスター データベースインスタンス

AWS のサービス	リソースタイプ
Amazon Simple Storage Service (Amazon S3)	バケット

EventBridge ルール

システムが EventBridge イベントからインシデントを作成すると、Incident Manager は選択したパラメータにイベントの `Resources` プロパティを入力します。詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge イベント」を参照してください。

手動で作成されたインシデント

StartIncident API アクションを使用してインシデントを作成すると、Incident Manager は API コールの情報を使用して選択したパラメータにデータを入力します。具体的には、`relatedItems` パラメータで渡されるタイプ `INVOLVED_RESOURCE` の項目を使用してパラメータにデータを入力します。

> **Note**
>
> `INVOLVED_RESOURCES` 値は、タイプ `StringList` のパラメータにのみ割り当てることができます。他のタイプのパラメータに割り当てられた場合、Runbook は実行に失敗します。

ランブックを定義する

ランブックを作成する際には、ここで説明するステップに従うか、「Systems Manager ユーザーガイド」の「Working with runbooks」セクションに記載されているより詳細なガイドに従ってください。複数アカウント、複数リージョンのランブックを作成する場合は、「Systems Manager ユーザーガイド」の「複数の AWS リージョン とアカウントでのオートメーションの実行」を参照してください。

ランブックを定義する

1. Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) 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. [Create automation (オートメーションを作成)] を選択します。

4. 一意で識別可能なランブック名を入力します。
5. ランブックの説明を入力します。
6. オートメーションドキュメントが引き受ける IAM ロールを指定します。これにより、ランブックがコマンドを自動的に実行できるようになります。詳細については、「オートメーションワークフローにサービスロールのアクセスを設定する」を参照してください。
7. (オプション) ランブックが起動時に使用する入力パラメータを追加します。ランブックを起動するときには、動的パラメータまたは静的パラメータを使用できます。動的パラメータはランブックが起動されるインシデントの値を使用します。静的パラメータは指定した値を使用します。
8. (オプション) ターゲット タイプを追加します。
9. (オプション) タグを追加します。
10. ランブックが実行時に行うステップを記入します。各ステップには以下が必要です。
    - 名前。
    - ステップの目的の説明。
    - ステップ中に実行するアクション。ランブックでは、手動のステップを説明するのに 一時停止 というアクションタイプを使用します。
    - (オプション) コマンドプロパティ。
11. 必要なランブックステップをすべて追加したら、オートメーションの作成を選択します。

クロスアカウント機能を有効にするには、インシデント中にランブックを使用するすべてのアプリケーションアカウントと、管理アカウントのランブックを共有します。

ランブックを共有する

1. Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) 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. ドキュメントリストで共有するドキュメントを選択し、[詳細を表示] を選択します。[Permissions] タブで自分がドキュメントの所有者であることを確認します。ドキュメントの所有者のみがドキュメントを共有できます。
4. [Edit] を選択します。
5. コマンドをパブリックに共有するには、[Public] を選択し、[Save] を選択します。コマンドをプライベートに共有するには、[Private (プライベート)] を選択し、AWS アカウント ID を入力します。次に、[Add permission (アクセス権限の追加)] を選択し、[Save (保存)] を選択します。

Incident Manager ランブックテンプレート

Incident Manager には、チームが Systems Manager オートメーションでランブックの作成を開始できるように、以下のランブックテンプレートが用意されています。このテンプレートをそのまま使用するか、編集して、アプリケーションおよびリソースに固有の詳細を含めることができます。

Incident Manager ランブックテンプレートを検索する

1. Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) 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. [ドキュメント] 領域で検索フィールドに **AWSIncidents-** を入力すると、Incident Manager のすべてのランブックが表示されます。

> **Tip**
>
> [ドキュメント名のプレフィックス] フィルターオプションを使用するのではなく、フリーテキストで **AWSIncidents-** を入力してください。

テンプレートの使用

1. Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) 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. ドキュメントリストから更新するテンプレートを選択します。
4. [コンテンツ] タブを選択し、ドキュメントのコンテンツをコピーします。
5. ナビゲーションペインで、[ドキュメント] を選択します。
6. [Create automation (オートメーションを作成)] を選択します。
7. 一意で識別可能な名前を入力します。
8. [エディタ] タブを選択します。
9. [Edit] (編集) を選択します。
10. [ドキュメントエディタ] 領域にコピーした詳細を貼り付けるか入力します。
11. [Create automation (オートメーションを作成)] を選択します。

AWSIncidents-CriticalIncidentRunbookTemplate

AWSIncidents-CriticalIncidentRunbookTemplate は、Incident Manager インシデントライフサイクルを手動ステップで提供するテンプレートです。これらのステップは、ほとんどのアプリケーションで使用できる一般的な手順ですが、応答者がインシデント解決に着手するのに十分な詳細が記載されています。

Incident Manager での対応計画の操作

対応計画を使用して、ユーザーに影響を与えるインシデントへの対応方法を計画します。対応計画はテンプレートとして機能するもので、エンゲージする担当者、イベントの予想される重大度、開始する自動ランブック、モニタリングするメトリクスに関する情報が含まれます。

ベストプラクティス

事前にインシデントの計画を立てておくと、チームへのインシデントの影響を軽減できます。チームは、対応計画を作成する際に以下のベストプラクティスを考慮する必要があります。

- エンゲージメントの合理化 - インシデントに最も適したチームを特定します。エンゲージの範囲が広すぎたり、間違ったチームにエンゲージさせたりすると、混乱を招き、インシデント発生時に応答者の時間を無駄にする可能性があります。
- 確実なエスカレーション — 対応計画に取り組む場合は、連絡先やオンコールスケジュールではなく、エンゲージメント計画を選択することをお勧めします。エンゲージメント計画には、インシデント発生時にエンゲージする個々の連絡先またはオンコールスケジュール (複数の交代連絡先を含む) を指定する必要があります。エンゲージメント計画に指定されている応答者に連絡が取れないことがあるため、そのようなシナリオをカバーするために対応計画にバックアップ応答者を設定する必要があります。バックアップの連絡先を指定すると、主要連絡先と副連絡先が不在だったり、カバレッジにその他の予定外のギャップが生じた場合でも、Incident Manager はインシデントについて連絡先に通知します。
- ランブック - 繰り返し可能でわかりやすいステップを提供するランブックを使用して、インシデント中に応答者が経験するストレスを軽減します。
- コラボレーション - チャットチャネルを使用して、インシデント中のコミュニケーションを合理化します。チャットチャネルは、応答者が最新の情報を維持するのに役立ちます。応答者はこれらのチャネルを通じて他の応答者と情報を共有することもできます。

対応計画の作成

以下の手順に従って対応計画を作成し、インシデント対応を自動化します。

対応計画を作成するには

1. Incident Manager コンソールを開き、左のナビゲーションペインで、[対応プラン] を選択します。
2. 対応計画の作成を選択します。
3. [名前] に、対応計画の Amazon リソースネーム (ARN) に使用する、一意で識別可能な対応計画名を入力します。
4. (オプション) [表示名] に、インシデントを作成するときに対応計画を識別するのに役立つ、わかりやすい名前を入力します。
5. 続けて、インシデントレコードのデフォルト値を指定します。

インシデントデフォルト値の指定

インシデントをより効果的に管理するために、デフォルト値を指定できます。Incident Manager は、これらの値を対応計画に関連するすべてのインシデントに適用します。

インシデントのデフォルト値を指定するには

1. [タイトル] に、Incident Manager のホームページで識別するのに役立つように、このインシデントのタイトルを入力します。
2. [影響] では、この対応計画から作成されるインシデントの潜在的な範囲を示す影響レベル ([重大] や [低] など) を選択します。Incident Manager での影響評価の詳細については、「トリアージ」を参照してください。
3. (オプション) [概要] に、この対応計画から作成されたインシデントのタイプの簡潔な概要を入力します。
4. (オプション) [重複排除文字列] は、重複排除文字列を入力します。Incident Manager は、この文字列を使用して、同じ根本原因が同じアカウントに複数のインシデントを作成しないようにします。

   重複排除文字列は、システムがインシデントの重複をチェックするために使用する用語またはフレーズです。重複排除文字列を指定すると、Incident Manager はインシデントを作成するときに `dedupeString` フィールドに同じ文字列が含まれる未解決のインシデントを検索します。重複

が検出されると、Incident Manager は新しいインシデントを既存のインシデントに重複排除します。

> **Note**
>
> デフォルトでは、Incident Manager は同じ Amazon CloudWatch アラームまたは Amazon EventBridge イベントによって作成された複数のインシデントを自動的に重複排除します。これらのリソースタイプの重複を避けるために、独自の重複排除文字列を入力する必要はありません。

5. (オプション) [インシデントタグ] の下に、この対応計画から作成されたインシデントに割り当てるタグキーと値を追加します。

   対応計画内にインシデントタグを設定するには、インシデントレコードリソースに対する `TagResource` アクセス許可が必要です。

6. 続いて、解決者どうしがインシデントについてやり取りするための[オプションのチャットチャネルを指定](#)します。

(オプション) インシデント対応チャットチャネルの指定

対応計画にチャットチャネルを含めると、応答者はこのチャネルを通じてインシデントの最新情報を受け取ります。応答者は、チャットコマンドを使用して、チャットチャネルから直接インシデントを操作できます。

AWS Chatbot を使用すると、Slack または Amazon Chime にチャネルを作成し、対応計画で使用することができます。AWS Chatbot でチャットチャネルを作成する方法については、「[AWS Chatbot 管理者ガイド](#)」を参照してください。

> **Important**
>
> Incident Manager には、チャットチャネルの Amazon Simple Notification Service (Amazon SNS) トピックに公開するための許可が必要です。この SNS トピックに公開する許可がない場合、対応計画に追加することはできません。Incident Manager は、SNS トピックにテスト通知を発行して、許可を検証します。

チャットチャネルの詳細については、「[Incident Manager でのチャットチャネルの操作](#)」を参照してください。

インシデント対応チャットチャネルを指定するには

1. [チャットチャネル] で、インシデント発生時に応答者が通信できる AWS Chatbot チャットチャネルを選択します。

   > **Tip**
   >
   > AWS Chatbot に新しいチャットチャネルを作成するには、[新しい Chatbot クライアントの設定] を選択します。

2. [チャットチャネルの SNS トピック] で、インシデント中に公開する追加の SNS トピックを選択します。複数の AWS リージョン に SNS トピックを追加すると、インシデント時にリージョンがダウンしている場合の冗長性が向上します。
3. 続いて、インシデント発生時にエンゲージする連絡先、オンコールスケジュール、エスカレーション計画を選択します。

(オプション) インシデント対応にエンゲージするリソースの選択

インシデントが発生したときに、最も適切な応答者を特定することが重要です。ベストプラクティスとして、以下を実行することをお勧めします。

1. エスカレーション計画のエスカレーションチャネルとして、連絡先とオンコールスケジュールを追加します。
2. 対応計画のエンゲージメントとして、エスカレーション計画を選択します。

連絡先とエスカレーション計画の詳細については、「Incident Manager での連絡先の操作」と「Incident Manager でのエスカレーション計画の操作」を参照してください。

インシデント対応にエンゲージするリソースを選択するには

1. [エンゲージメント] では、エスカレーション計画、オンコールスケジュール、個別の連絡先をいくつでも選択できます。
2. 続いて、オプションで、インシデント軽減の一環として実行するランブックを指定します。

(オプション) インシデント軽減のためのランブックの指定

AWS Systems Manager の機能である AWS Systems Manager Automation のランブックを使用して、AWS クラウド 環境内のアプリケーションとインフラストラクチャの一般的なタスクを自動化できます。

各ランブックでは、ランブックワークフローを定義します。ランブックワークフローには、マネージドノードまたはその他の AWS リソースタイプで Systems Manager が実行するアクションが含まれています。Incident Manager では、ランブックはインシデント対応とインシデントの軽減に役立ちます。

対応計画でのランブックの使用の詳細については、「Incident Manager での Systems Manager Automation ランブックの操作」を参照してください。

インシデント軽減のためのランブックを指定するには:

1. [ランブック] で、以下のいずれかを実行します。

   - [テンプレートからランブックのクローンを作成] を選択し、デフォルトの Incident Manager ランブックのコピーを作成します。[名前] に、新しいランブックのわかりやすい名前を入力します。
   - [既存のランブックを選択] を選択します。[所有者]、[ランブック]、使用する [バージョン] を選択します。

   > **Tip**
   >
   > ランブックを一から作成するには、[新しいランブックを設定] を選択します。ランブックの作成の詳細については、「Incident Manager での Systems Manager Automation ランブックの操作」を参照してください。

2. [パラメータ] 領域で、選択したランブックに必要なパラメータを指定します。

   使用可能なパラメータは、ランブックに指定されているパラメータです。ランブックに応じて、別のランブックとは異なるパラメータが必要になることがあります。パラメータには必須のものとオプションのものがあります。

   多くの場合、Amazon EC2 インスタンス ID のリストなど、パラメータの静的な値は、手動で入力することを選択できます。インシデントによって動的に生成されたパラメータ値を Incident Manager に入力させることもできます。

3. (オプション) [AutomationAssumeRole] に、使用する AWS Identity and Access Management (IAM) ロールを指定します。このロールには、ランブック内に指定されている個々のコマンドの実行に必要なアクセス許可が必要です。

   > **Note**
   >
   > `AssumeRole` が指定されていない場合、Incident Manager はランブックサービスロールを使用して、ランブック内で指定されている個々のコマンドを実行しようとします。

   次から選択します。

   - [ARN 値を入力] — AssumeRole の Amazon リソースネーム (ARN) を`arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name`* 形式で手動で入力します。例えば、**`arn:aws:iam::123456789012:role/MyAssumeRole`** です。
   - [既存のサービスロールを使用] — アカウント内の既存のロールのリストから、必要なアクセス許可を持つロールを選択します。
   - [新しいサービスロールを作成] — AWS マネージドポリシーから選択してAssumeRole にアタッチします。このオプションを選択した後、[AWS マネージドポリシー] で、リストから 1 つ以上のポリシーを選択します。

     新しいロールに提示されたデフォルト名を使用することも、選択した名前を入力することもできます。

     > **Note**
     >
     > この新しいランブックサービスロールは、選択した特定のランブックに関連付けられます。別のランブックでは使用できません。これは、ポリシーのランブックセクションが他のランブックをサポートしないためです。

4. [ランブックサービスロール] に、ランブック自体のワークフローへのアクセスと開始に必要なアクセス許可を提供するために使用する IAM ロールを指定します。

   少なくとも、このロールは、特定のランブックの `ssm:StartAutomationExecution` アクションを許可する必要があります。ランブックがアカウント間で動作するためには、Incident Manager でのクロスリージョンおよびクロスアカウントのインシデント管理 中に作成した `AWS-SystemsManager-AutomationExecutionRole` ロールに対する `sts:AssumeRole` アクションも許可する必要があります。

次から選択します。

- [新しいサービスロールを作成] — Incident Manager は、ランブックワークフローを開始するために最低限必要なアクセス許可を含むランブックサービスロールを自動的に作成します。

  [ロール名] には、提示されたデフォルト名を使用することも、選択した名前を入力することもできます。この名前には、提示された名前を使用するか、ランブックの名前を残しておくことをお勧めします。これは、新しい AssumeRole には、選択した特定のランブックに関連付けられており、他のランブックに必要なアクセス許可が含まれていない可能性があるためです。

- [既存のサービスロールを使用] — ユーザーまたは Incident Manager が以前に作成した IAM ロールは、必要なアクセス許可を付与します。

  [ロール名] で、使用する既存のロールの名前を選択します。

5. [追加のオプション] を展開し、次のいずれかを選択してランブックワークフローを実行する AWS アカウント を指定します。

   - [対応プラン所有者のアカウント] — ランブックワークフローを作成した AWS アカウント でランブックワークフローを開始します。
   - [影響を受けたアカウント] — インシデントを開始または報告したアカウントでランブックワークフローを開始します。

     [影響を受けたアカウント] は、Incident Manager をクロスアカウントシナリオで使用していて、ランブックが影響を受けたアカウントのリソースにアクセスしてそれらを修正する必要がある場合に選択します。

6. 続いて、オプションで PagerDuty サービスを対応計画に統合します。

(オプション) PagerDuty サービスの対応計画への統合

PagerDuty サービスを対応計画に統合するには

Incident Manager を PagerDuty と統合すると、Incident Manager がインシデントを作成するたびに、PagerDuty は対応するインシデントを作成します。PagerDuty のインシデントは、Incident Manager に含まれるものに加えて、そこで定義したページングワークフローとエスカレーションポリシーを使用します。PagerDuty は、Incident Manager からのタイムラインイベントをインシデントに関するメモとしてアタッチします。

1. [サードパーティ統合] を展開し、[PagerDuty 統合を有効にする] チェックボックスをオンにします。
2. [シークレットを選択] で、PagerDuty アカウントにアクセスするための認証情報を保存する AWS Secrets Manager のシークレットを選択します。

   PagerDuty 認証情報を Secrets Manager のシークレットに保存する方法については、「PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存する」を参照してください。
3. [PagerDuty サービス] で、PagerDuty アカウントから PagerDuty インシデントを作成したいサービスを選択します。
4. 続いて、オプションでタグを追加して対応計画を作成します。

タグを追加して対応計画を作成する

タグを追加して対応計画を作成するには

1. (オプション) [タグ] 領域で、1 つ以上のタグキーの名前と値のペアを対応計画に適用します。

   タグは、リソースに割り当てるオプションのメタデータです。タグを使用して、目的、所有者、環境などのさまざまな方法でリソースを分類できます。例えば、軽減対象となるインシデントの種類、含まれるエスカレーションチャネルの種類、関連するエスカレーション計画を識別するために、対応計画にタグを付けることができます。Incident Manager リソースへのタグ付けの詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。
2. 対応計画の作成を選択します。

Incident Manager での検出結果の使用

Incident Manager では、検出結果とは、インシデント発生前後に発生し、インシデントに関連する可能性のある 1 つ以上のリソースが関与している AWS CodeDeploy デプロイまたは AWS CloudFormation スタックの更新に関する情報です。各検出結果は、インシデントの潜在的な原因として調査できます。これらの潜在的な原因に関する情報は、インシデントのインシデント詳細ページに追加されます。こうしたデプロイや変更に関する情報がすぐに手元にあれば、対応者はこの情報を手動で検索する必要がありません。そのため潜在的な原因の評価に必要な時間が短縮され、インシデントからの平均回復時間 (MTTR) を短縮できます。

現在 Incident Manager は、AWS CodeDeploy と AWS CloudFormation の 2 つの AWS のサービスからの検出結果の収集をサポートしています。

検出結果はオプトイン機能です。この機能は、Incident Manager に初めてオンボーディングするときに 準備ウィザードで有効化することも、後で設定ページで有効化することもできます。

検出結果機能を有効にすると、Incident Manager がユーザーに代わってサービスロールを作成します。このサービスロールには、CodeDeploy と CloudFormation から検出結果を取得するために必要な権限が含まれています。

クロスアカウントシナリオで検出結果を使用するには、管理アカウントでこの機能を有効にします。その後、AWS Resource Access Manager (AWS RAM) 組織の各アプリケーションアカウントが、対応するサービスロールを作成する必要があります。

検出結果機能を使用する際に役立つ以下のトピックを参照してください。

トピック

- 検出結果を使用するためのサービスロールの有効化と作成
- クロスアカウント検出結果サポートのための許可の設定

検出結果を使用するためのサービスロールの有効化と作成

検出結果機能を有効にすると、Incident Manager は `IncidentManagerIncidentAccessServiceRole` という名前のサービスロールをユーザーに代わって作成します。このサービスロールは、インシデントが作成されたころに発生した CodeDeploy デプロイと CloudFormation スタックの更新に関する情報を収集するために Incident Manager が必要とする権限を提供します。

> **Note**
>
> Incident Manager を組織で使用している場合、このサービスロールは管理アカウントに作成されます。組織内の他のアカウントで検出結果を使用するには、各アプリケーションアカウントにこのサービスロールを作成する必要があります。CloudFormation テンプレートを使用してアプリケーションアカウントにこのロールを作成する方法については、「クロスアカウントインシデント管理のセットアップと設定」のステップ 4 を参照してください。

このサービスロールは AWS マネージドポリシーに関連付けられています。このポリシーのアクセス許可の詳細については、「AWS マネージドポリシー：AWSIncidentManagerIncidentAccessServiceRolePolicy」を参照してください。

Incident Manager のオンボーディングプロセス中に検出結果を有効にする方法については、「Incident Manager の使用開始」を参照してください。

オンボーディングプロセス完了後に検出結果を有効にする方法については、「検出結果機能の管理」を参照してください。

クロスアカウント検出結果サポートのための許可の設定

AWS RAM に設定されている組織の複数のアカウントで検出結果機能を使用するには、各アプリケーションアカウントが、自身に代わって管理アカウントのサービスロールを引き受ける許可を Incident Manager に設定する必要があります。

これらの許可は、AWS が提供する AWS CloudFormation テンプレートをデプロイすることでアプリケーションアカウント内で設定できます。これにより、`IncidentManagerIncidentAccessServiceRole` ロールが作成されます。

このテンプレートをダウンロードしてアプリケーションアカウントにデプロイする方法については、「Incident Manager でのクロスリージョンおよびクロスアカウントのインシデント管理」のステップ 4 を参照してください。

Incident Manager でのインシデントの作成

AWS Systems Manager の機能である Incident Manager は、インシデントの管理とインシデントへの迅速な対応に役立ちます。CloudWatch アラームと EventBridge イベントに基づいて自動的にインシデントを作成するように Amazon CloudWatch と Amazon EventBridge を設定できます。インシデントは、インシデントリストページで手動で作成することも、AWS CLI または AWS SDK から StartIncident API アクションを使用して作成することもできます。Incident Manager は、同じ CloudWatch アラームまたは EventBridge イベントから作成されたインシデントを同じインシデントに重複排除します。

CloudWatch アラームまたは EventBridge イベントによって自動的に作成されたインシデントの場合、Incident Manager はイベントルールまたはアラームと同じ AWS リージョン にインシデントを作成しようとします。Incident Manager が AWS リージョン で利用できない場合、CloudWatch または EventBridge は、レプリケーションセットで指定されている使用可能なリージョンのいずれかにインシデントを自動的に作成します。詳細については、「Incident Manager でのクロスリージョンおよびクロスアカウントのインシデント管理」を参照してください。

システムによってインシデントが作成されると、Incident Manager はインシデントに関係する AWS リソースに関する情報を自動的に収集し、その情報を [関連項目] タブに追加します。対応計画にランブックを指定している場合、システムによってインシデントが作成されると、Incident Manager はインシデントに関係する AWS リソースに関する情報をランブックに送信できます。その後システムは、ランブックを開始して問題の修正を試みるときに、それらのリソースをターゲットにすることができます。

システムはインシデントを作成すると、Systems Manager のコンポーネントである OpsCenter にも親運用作業項目 (OpsItem) を作成し、関連項目としてこの項目をインシデントにリンクします。この OpsItem を使用して、関連する作業と将来のインシデント分析を追跡できます。OpsCenter の使用には料金がかかります。OpsCenter の料金の詳細については、Systems Manager の料金を参照してください。

> **Important**
>
> 次の重要な詳細に留意してください。
>
> - Incident Manager が使用できない状況では、レプリケーションセットに少なくとも 2 つのリージョンを指定している場合にのみ、システムはフェイルオーバーして他の AWS リージョン リージョンにインシデントを作成できます。レプリケーションセットの設定については、「Incident Manager の使用開始」を参照してください。

- クロスリージョンフェイルオーバーによって作成されたインシデントは、対応計画で指定されているランブックを呼び出しません。

CloudWatch アラームでインシデントを自動的に作成する

CloudWatch は CloudWatch メトリクスを使用して、環境内の変更について警告し、インシデントの開始アクションを自動的に実行します。CloudWatch は、Systems Manager と Incident Manager と連携して、アラームがアラーム状態になったときに対応計画テンプレートからインシデントを作成します。これには、次の前提条件が必要です。

- Incident Manager が設定され、レプリケーションセットが作成されました。この手順では、アカウントに Incident Manager サービスリンクロールを作成し、必要な許可を提供します。
- Incident Manager の対応計画を設定しました。Incident Manager の対応計画を設定する方法については、このガイドの「インシデントの準備」の Incident Manager での対応計画の操作 を参照してください。
- アプリケーションをモニタリングする CloudWatch メトリクスを設定しました。モニタリングのベストプラクティスについては、このガイドの「インシデントの準備」の モニタリング を参照してください。

インシデント開始 アクションでアラームを作成するには

1. CloudWatch にアラームを作成します。詳細については、『Amazon CloudWatch 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。
2. アラームが実行するアクションを選択する場合は、Systems Manager アクションの追加を選択します。
3. インシデントの作成 を選択し、このインシデントの 対応計画 を選択します。
4. 選択したアラームタイプガイドの残りのステップを完了します。

> **Tip**
>
> また、既存のアラームにインシデント作成アクションを追加することもできます。

EventBridge イベントでインシデントを自動的に作成する

EventBridge ルールはイベントパターンを監視します。イベントが定義されたパターンと一致する場合、Incident Manager は、選択した対応計画を使用してインシデントを作成します。

SaaS パートナーイベントを使用したインシデントの作成

EventBridgeは、サービスとしてのソフトウェア (SaaS) パートナーのアプリケーションやサービスからイベントを受け取れるように設定でき、サードパーティの統合が可能です。サードパーティパートナーからイベントを受け取れるように EventBridge を設定した後は、パートナーイベントに一致するルールを作成してインシデントを作成できます。サードパーティ統合のリストは、「SaaS パートナーからイベントを受け取る」を参照してください。

SaaS 統合からイベントを受け取れるように EventBridge を設定します。

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで、[Partner event sources (パートナーイベントソース)] を選択します。
3. 検索バーを使用して希望するパートナーを検索し、そのパートナーの [Set up (設定)] を選択します。
4. [Copy (コピー)] を選択して、アカウント ID をクリップボードにコピーします。

> **Note**
>
> Salesforce と統合するには、Amazon AppFlow ユーザーガイドに記載されている手順を使用します。

5. パートナーのウェブサイトにアクセスし、手順に従ってパートナーイベントソースを作成します。これには、アカウント ID を使用します。作成したイベントソースは、アカウントのみで使用できます。
6. Eventbridge コンソールに戻り、ナビゲーションペインで [Partner event sources] (パートナーイベントソース) を選択します。
7. パートナーイベントソースの横にあるボタンを選択し、[Associate with event bus (イベントバスと関連付ける)] を選択します。

SaaS パートナーからのイベントでトリガーするルールを作成するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。

2. ナビゲーションペインで [Rules] (ルール) を選択します。
3. [Create rule] (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] で、このパートナーに対応するイベントバスを選択します。
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) をクリックします。
8. [Event source] (イベントソース) で、[AWS events or EventBridge partner events] (イベントまたは EventBridge パートナーイベント) 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. [イベントソース] で、[EventBridge パートナー] を選択します。
11. [パートナー] で、パートナーの名前を選択します。
12. Event type (イベントタイプ)で、All Events (すべてのイベント)を選択するか、このルールに使用するイベントのタイプを選択します。[All Events (すべてのイベント)] を選択した場合、このパートナーイベントソースによって出力されたすべてのイベントがルールに一致します。

    イベントパターンをカスタマイズする場合は、[Edit (編集)] を選択して変更を加えてから、[Save (保存)] を選択します。
13. [Next] (次へ) をクリックします。
14. [ターゲットを選択] で、[Incident Manager の対応プラン] を選択し、次に [対応プラン] を選択します。

    > **Note**
    >
    > 対応計画を選択すると、所有し、アカウントで共有しているすべての対応計画が [対応プラン] ドロップダウンリストに表示されます。
15. EventBridge は、イベントの実行に必要な IAM ロールを作成できます。

    - 自動的に IAM ロールを作成するには、[この特定のリソースに対して新しいロールを作成する] を選択します。
    - 以前に作成した IAM ロールを使用するには、[Use existing role] (既存のロールの使用) を選択します。

16. [Next] (次へ) をクリックします。
17. (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 EventBridge ユーザーガイド」の「Amazon EventBridge のタグ」を参照してください。
18. [Next] (次へ) をクリックします。
19. ルールを確認したら、[ルールを作成] を選択します。

AWS サービスイベントを使用したインシデントの作成

EventBridge は、「サポートされている AWS サービスからのイベント」に記載されている AWS サービスからもイベントを受け取ります。SaaS パートナーのルールを設定する方法と同様に、AWS サービスに対してもルールを設定できます。

AWS サービスのイベントをトリガーとするルールの作成

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで [Rules] (ルール) を選択します。
3. [Create rule] (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) をクリックします。
8. [Event source] (イベントソース) で、[AWS events or EventBridge partner events] (イベントまたは EventBridge パートナーイベント) 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. サービス名で、インシデントをモニタリングするサービスを選択します。
12. Event type (イベントタイプ)で、All Events (すべてのイベント)を選択するか、このルールに使用するイベントのタイプを選択します。[All Events (すべてのイベント)] を選択した場合、このパートナーイベントソースによって出力されたすべてのイベントがルールに一致します。

    イベントパターンをカスタマイズする場合は、[Edit (編集)] を選択して変更を加えてから、[Save (保存)] を選択します。

13. [Next] (次へ) をクリックします。
14. [ターゲットを選択] で、[Incident Manager の対応プラン] を選択し、次に [対応プラン] を選択します。

> **Note**
>
> 対応計画を選択すると、所有し、アカウントで共有しているすべての対応計画が [対応プラン] ドロップダウンリストに表示されます。

15. EventBridge は、イベントの実行に必要な IAM ロールを作成できます。
    - 自動的に IAM ロールを作成するには、[この特定のリソースに対して新しいロールを作成する] を選択します。
    - 以前に作成した IAM ロールを使用するには、[Use existing role] (既存のロールの使用) を選択します。
16. [Next] (次へ) をクリックします。
17. (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 EventBridge ユーザーガイド」の「Amazon EventBridge のタグ」を参照してください。
18. [Next] (次へ) をクリックします。
19. ルールを確認したら、[ルールを作成] を選択します。

インシデントを手動で作成する

応答者は、事前定義された対応計画を使用し、Incident Manager コンソールを使用してインシデントを手動で追跡できます。次の手順に従ってインシデントを作成します。

1. Incident Manager コンソールを開きます。
2. [インシデントの開始] を選択します。
3. 対応計画では、リストから対応計画を選択します。
4. (オプション) 定義された対応計画で提供されるタイトルを上書きするには、インシデントタイトルを入力します。
5. (オプション) 定義された対応計画で提供される影響を上書きするには、インシデントの 影響 を入力します。

Incident Manager でのインシデントの追跡

AWS Systems Manager Incident Manager は、インシデントが検出された瞬間から解決、インシデント後分析までインシデントを追跡します。すべてのインシデントは、Incident Manager コンソールのインシデントリストページで確認でき、インシデントの詳細に直接リンクされています。

トピック

- インシデントリスト
- インシデントの詳細

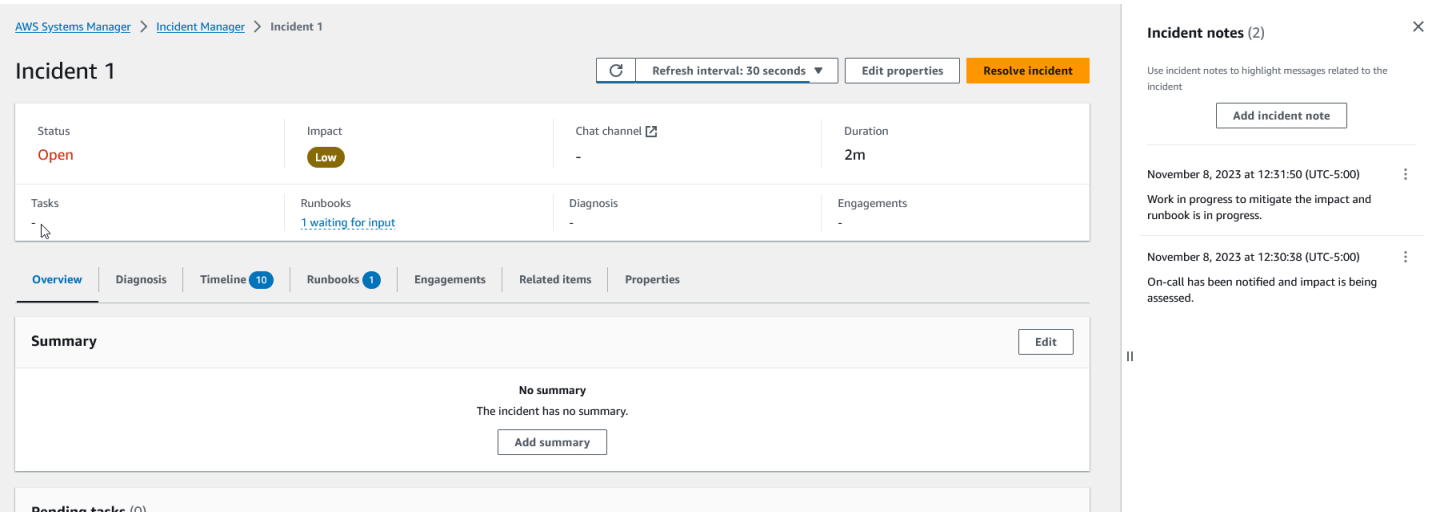
インシデントリスト

インシデントリストページには、オープン状態のインシデント、解決済みのインシデント、分析の 3 つのセクションがあります。このページから新しいインシデントを手動で追跡し、分析を作成できます。インシデントを手動で追跡する方法については、このガイドの インシデントの作成 セクションの インシデントを手動で作成する を参照してください。インシデント後分析の詳細については、このガイドの「Incident Manager でのインシデント後分析の実行」セクションを参照してください。

インシデントの詳細では、そのインシデントのタイトル、影響、期間、チャットチャネルが表示されたタイル内にオープン状態のインシデントが表示されます。インシデントを解決すると、インシデントは 解決済みのインシデント リストに移動します。分析は 2 番目のタブにあります。

インシデントの詳細

インシデントの詳細ページは、インシデントの管理に使用できる詳細なインサイトとツールを提供します。このページから、ランブックを起動してインシデントを軽減したり、インシデントのメモを追加したり、他の解決者をエンゲージしたり、タイムライン、メトリクス、プロパティ、関連リソースなどのインシデントの詳細を表示したりできます。インシデントの詳細ページには、トップバナー、インシデントのメモ、および追加情報やリソースが含まれる 7 つのタブがあります。デフォルトでは、トップバナーと [インシデントのメモ] セクションがすべての [インシデントの詳細] ページに表示されます。



このトピックでは、インシデントの詳細ページの要素と、このページから実行できるアクションについて説明します。

トップバナー

各インシデントの詳細ページのトップバナーには、次の情報が含まれています。

- ステータス — インシデントの現在のステータスは、未解決または解決済みになります。
- 影響 — インシデントが環境に及ぼす影響。高、中、または低になります。インシデントの影響を変更するには、[プロパティの編集] を選択します。
- チャットチャネル — インシデントの最新情報や通知を確認できるチャットチャネルにアクセスするためのリンク。
- 期間 — 応答者がこのインシデントを解決するまでに経過した時間。
- ランブック — このインシデントに関連するランブックのステータス。ステータスは、入力待ち、成功、不成功のいずれかになります。ランブックのステータスが入力待ちの場合、ランブックを選択してアクションの詳細を表示できます。[失敗] を選択すると、タイムアウト、失敗、またはキャンセル済みのランブックを表示できます。
- エンゲージメント — エンゲージメントの総数と各エンゲージメントのステータス。エンゲージメントを作成すると、そのステータスはエンゲージ済みになります。エンゲージメントを承認すると、ステータスがエンゲージ済みから承認済みに変わります。Incident Manager は、第三者のエンゲージメントの承認をサポートしていません。このようなエンゲージメントは、エンゲージ済みステータスのままになります。

バナーの右上にある [編集] を選択すると、インシデントのタイトル、影響、チャットチャネルを編集できます。

インシデントのメモ

画面の右側には、インシデントのメモが表示されます。メモを使用すると、インシデントに取り組んでいる他のユーザーと共同作業したり、やり取りしたりすることができます。適用した緩和、特定した潜在的な根本原因、またはインシデントの現在のステータスについて説明できます。ベストプラクティスとして、インシデントのメモセクションを使用して、ステータスの最新情報や、自分または他のユーザーがインシデントに対して取った措置を投稿します。他の解決者とリアルタイムでコミュニケーションを取る必要がある場合は、Incident Manager で使用可能なチャットチャネルを使用します。

メモを追加するには、[インシデントのメモを追加] ボタンを選択し、メモを入力します。メモには、インシデントのステータスに関する最新情報や、他のユーザーに可視性を提供するその他の関連情報を含めることができます。必要に応じて、インシデントのメモは編集または削除することもできます。

> **Note**
>
> `ssm-incidents:UpdateTimelineEvent` および `ssm-incidents:DeleteTimelineEvent` アクションを実行する IAM 権限を持つすべてのユーザーが、メモを編集および削除できます。ただし、インシデントを別のアカウントと共有する場合、リソースポリシーに `ssm-incidents:DeleteTimelineEvent` アクションは含まれません。これにより、インシデントを共有しているユーザーはメモを削除できなくなります。Incident Manager のイベントからのメモの監査証跡は AWS CloudTrail コンソールで表示できます。

タブ

インシデントの詳細ページには 7 つのタブがあり、応答者がインシデント中に情報を簡単に検索・表示できます。タブには、タブ名にカウンターが表示され、タブの更新回数が表示されます。各タブの内容と実行可能なアクションについては、このまま読み進めてください。

概要

概要 タブは、応答者のランディングページです。これには、インシデントのサマリー、最近のタイムラインイベントのリスト、現在のランブックステップが含まれます。

応答者は、インシデントのサマリーを使用して、どのアクションが行われたか、変更の結果、考えられる次のステップ、インシデントの影響に関する情報などを把握できます。サマリーを更新するには、サマリー セクションの右上にある 編集 を選択します。

> **Important**
>
> 複数の応答者がサマリーフィールドを同時に編集している場合、編集内容を送信した応答者が他のすべての入力を上書きします。

[最近のタイムラインのイベント] セクションには、Incident Manager によって入力された最近の 5 つのイベントのタイムラインが含まれています。このセクションを使用すると、インシデントのステータスと最近発生した内容を理解できます。完全なタイムラインを表示するには、タイムライン タブに進みます。

また、概要ページには、現在のランブックステップも表示されます。このステップは、AWS 環境で実行される自動ステップの場合も、応答者のための一連の手動の指示の場合もあります。これまでのステップや今後のステップを含む完全なランブックを表示するには、[ランブック] タブに進みます。

診断

[診断] タブには、メトリクスや (有効になっている場合) 検出結果に関する情報など、AWS でホストされているアプリケーションやシステムに関する重要な情報が含まれています。

メトリクスの使用

Incident Manager は、Amazon CloudWatch を使用して、このタブにあるメトリクスとアラームグラフを作成します。アラームやメトリクスを定義するためのインシデント管理のベストプラクティスについては、このユーザーガイドの インシデント計画 セクションの モニタリング を参照してください。

メトリクスを追加するには

- このタブの右上にある [追加] を選択します。
  - 既存の CloudWatch ダッシュボードからメトリクスを追加するには、[既存の CloudWatch ダッシュボードから] を選択します。
    a. ダッシュボードを選択します。これにより、選択されたダッシュボードの一部であるすべてのメトリクスとアラームが追加されます。

b. (オプション) ダッシュボードからメトリクスを選択して特定のメトリクスを表示できます。

- CloudWatch から を選択し、メトリクスソースを貼り付けることで、単一のメトリクスを追加します。メトリクスソースをコピーするには、次の手順に従います。

  a. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。

  b. ナビゲーションペインで [Metrics] (メトリクス) を選択します。

  c. [すべてのメトリクス] タブで、検索フィールドに検索語 (メトリクス名、リソース名など) を入力し、Enter キーを選択します。

     例えば、`CPUUtilization` メトリクスを検索した場合、そのメトリクスに関連する名前空間とディメンションが見つかります。

  d. 検索結果から結果を 1 つを選択すると、メトリクスが表示されます。

  e. ソース タブを選択し、ソースをコピーします。

メトリクスのアラームグラフは、関連する対応計画を通じてインシデントの詳細に追加するか、メトリクスの追加時に [既存の CloudWatch ダッシュボードから] を選択することでのみ追加できます。

メトリクスを削除するには、[削除] を選択し、提供された [メトリクス] ドロップダウンから削除したいメトリクスを選択します。

AWS CodeDeployおよび AWS CloudFormation からの検出結果の表示

検出結果を有効にし、必要なアクセス許可をすべて設定すると、特定のインシデントに関連する可能性のあるすべての検査結果がインシデントにアタッチされます。応答者は、これらの検出結果に関する情報をインシデント詳細ページで確認できます。

CodeDeploy および CloudFormation からの検出結果を表示するには

1. Incident Manager コンソールを開きます。
2. 調査するインシデントの名前を選択します。
3. [診断] タブの [検出結果] 領域で、報告されたすべての検出結果の開始時刻とインシデントの開始時刻を比較します。
4. 検出結果の詳細を表示するには、[リファレンス] 列で、CodeDeploy または CloudFormation の検出結果へのリンクを選択します。

タイムライン

タイムライン タブを使用して、インシデント中に発生したイベントを追跡します。Incident Manager は、インシデント中の重要な発生を特定するタイムラインイベントを自動的に入力します。応答者は、手動で検出した事象に基づいて、カスタムイベントを追加できます。インシデント後分析中に、[タイムライン] タブは、今後のインシデントをより適切に準備して対応する方法に関する貴重なインサイトを提供します。インシデント後分析の詳細については、「Incident Manager でのインシデント後分析の実行」を参照してください。

カスタムタイムラインイベントを追加するには、追加を選択します。カレンダーを使用して日付を選択し、時間を入力します。表示されるすべての時間はローカルタイムゾーンです。タイムラインに表示されるイベントの簡単な説明を入力します。

既存のカスタムイベントを編集するには、タイムライン上のイベントを選択し、編集を選択します。カスタム イベントの時刻、日付、説明を変更できます。カスタムイベントのみを編集できます。

ランブック

インシデント詳細ページの [ランブック] タブでは、応答者がランブックの手順を確認したり、新しいランブックを開始したりできます。

新しいランブック開始するには、[ランブック] セクションの [ランブックを開始] を選択します。検索フィールドを使用して、開始したいランブックを見つけます。ランブックを開始するときに必要なパラメータと使用するランブックのバージョンを入力します。インシデント中に [ランブック] タブから開始されたランブックは、現在サインインしているアカウントのアクセス許可を使用します。

Systems Manager でランブックの定義に移動するには、[ランブック] の下でランブックのタイトルを選択します。Systems Manager でランブックの実行中のインスタンスに移動するには、[実行の詳細] の下で実行の詳細を選択します。これらのページには、ランブックを起動するために使用されるテンプレートと、オートメーションドキュメントの現在実行中のインスタンスの具体的な詳細が表示されます。

[ランブックのステップ] セクションには、選択されたランブックが自動的に実行する、または応答者が手動で実行するステップのリストが表示されます。ステップが現在のステップになると展開され、ステップを完了するために必要な情報またはステップの実行内容の詳細が表示されます。自動ランブックステップは、オートメーションの完了後に解決されます。手動ステップでは、応答者はステップの下部にある [次のステップ] を選択する必要があります。ステップが完了すると、ステップ出力がドロップダウンとして表示されます。

ランブックの実行をキャンセルするには、[ランブックをキャンセル] を選択します。これによりランブックは実行を停止し、ランブック内のそれ以降のステップは完了しません。

エンゲージメント

インシデントの詳細のエンゲージメントタブでは、応答者やチームのエンゲージメントを確認できます。このタブから、エスカレーション計画の一部としてエンゲージした人、応答した人、およびこれからエンゲージされる応答者を確認できます。応答者は、このタブから他の連絡先に直接エンゲージできます。連絡先やエスカレーション計画の作成については、このガイドの Incident Manager での連絡先の操作 と Incident Manager でのエスカレーション計画の操作 セクションを参照してください。

インシデントの開始時に自動的にエンゲージメントを開始するように、連絡先とエスカレーションプランを含む対応計画を設定できます。対応計画の設定の詳細については、このガイドの「Incident Manager での対応計画の操作」セクションを参照してください。

各連絡先に関する情報は、表の中にあります。この表には、次の情報が含まれます。

- 名前 — 連絡先への連絡方法やエンゲージメント計画が表示される連絡先の詳細ページへのリンク。
- エスカレーション計画 — 連絡先をエンゲージしたエスカレーション計画へのリンク。
- 連絡先ソース — この連絡先をエンゲージしたサービス (AWS Systems Manager や PagerDuty など) を特定します。
- エンゲージ済み — 計画が連絡先をエンゲージした時期、またはエスカレーションプランの一環として連絡先をエンゲージさせる時期を表示します。
- 承認 — 連絡先がエンゲージメントを承認したかどうかが表示されます。

エンゲージメントを承認するには、応答者は次のいずれかを実行します。

- 電話 — プロンプトが表示されたら **1** を入力します。
- SMS – 提供されたコードでメッセージに返信するか、インシデントの [エンゲージメント] タブで提供されたコードを入力します。
- E メール – インシデントのエンゲージメントタブで指定されたコードを入力します。

関連項目

[関連項目] タブは、インシデント軽減に関連するリソースを収集するために使用されます。これらのリソースには、ARN、外部リソースへのリンク、または Amazon S3 バケットにアップロードされたファイルなどがあります。表には、説明的なタイトルと、ARN、リンク、またはバケットの詳細が表示されます。S3 バケットを使用する前に、「Amazon S3 ユーザーガイド」の「Amazon S3 のセキュリティのベストプラクティス」を確認してください。

Amazon S3 バケットにファイルをアップロードするときに、そのバケットではバージョニングが有効化または停止されています。バケットでバージョニングが有効の場合、既存のファイルと同じ名前でアップロードされたファイルは、ファイルの新しいバージョンとして追加されます。バージョニングが停止されている場合、既存のファイルと同じ名前でアップロードされたファイルは、既存のファイルを上書きします。バージョニングの詳細については、「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。

ファイル関連の項目を削除すると、ファイルはインシデントからは削除されますが、Amazon S3 バケットからは削除されません。Amazon S3 バケットからオブジェクトを削除する方法の詳細については、「Amazon S3 ユーザーガイド」の「Amazon S3 オブジェクトの削除」を参照してください。

プロパティ

[プロパティ] タブには、インシデントの詳細が表示されます。

[インシデントプロパティ] セクションでは、以下を確認できます。

- ステータス — インシデントの、現在のステータスを示します。インシデントは未解決または解決済みになります。
- 開始時刻 — Incident Manager でインシデントが作成された時刻。
- 解決時刻 — Incident Manager でインシデントが解決された時刻。
- Amazon リソースネーム (ARN) – インシデントの ARN。チャットや AWS Command Line Interface (AWS CLI) コマンドでインシデントを参照するときは、ARN を使用します。
- 対応プラン — 選択したインシデントの対応計画を特定します。対応計画を選択すると、対応計画の詳細ページが開きます。
- 親 OpsItem — インシデントの親として作成された OpsItem を特定します。親 OpsItem は、複数の関連するインシデントとフォローアップアクション項目を持つことができます。親 OpsItem を選択すると、OpsCenter の OpsItems 詳細ページが開きます。

- 分析 — このインシデントから作成された分析を特定します。解決済みのインシデントから分析を作成し、インシデント対応プロセスを改善します。分析を選択すると、分析の詳細ページが開きます。
- 所有者 — インシデントが作成されたアカウント。

[タグ] セクションでは、インシデントレコードに関連するタグキーと値を表示および編集できます。Incident Manager のタグの詳細については、「Incident Manager でのリソースのタグ付け」を参照してください。

Incident Manager でのインシデント後分析の実行

インシデント後分析により、検出までの時間や緩和など、インシデントへの対応を改善するための改善点を特定する手順が示されます。分析は、インシデントの原因を理解するのに役立ちます。Incident Manager は、インシデント対応を改善するための推奨 アクション項目 を作成します。

インシデント後分析の利点

- インシデント対応の改善
- 問題の根本原因への理解
- 配信性能なアクション項目で根本原因に対処することができる
- インシデントの影響の分析
- 組織内で学習内容をキャプチャして共有する

分析してはいけないもの

分析に罪はなく、人を名指しで呼ぶこともありません。

「何が発見されたかにかかわらず、私たちは、当時の知識、スキル、能力、利用可能なリソース、状況に応じて、全員ができる限りの仕事をしたと理解し、それを心から信じています。」 - Norm Kerth『Project Retrospectives: A Handbook for Team Review』

分析の詳細

分析の詳細ページでは、情報の収集、改善の評価、およびアクション項目の作成について説明します。分析の詳細ページは、インシデントの詳細と似ていますが、履歴メトリクス、編集可能なタイムライン、今後のインシデントを改善するための質問など、いくつかの重要な 違い があります。

概要

概要はインシデントのサマリーです。このサマリーには、背景、何が起こったのか、発生した理由、緩和方法、期間、およびインシデントが再び発生しないようにするための主要なアクション項目が含まれます。概要は高レベルです。詳細は、分析の 質問 タブで確認できます。

メトリクス

[メトリクス] タブを使用して、インシデント期間中のアプリケーション内の主要なメトリクスを視覚化します。同じグラフに 1 つ以上のメトリクスが表示されたメトリクスグラフをここに追加できま

す。インシデント中に使用されるメトリクスは、このタブに自動的に入力されます。インシデント中の主要なタイムポイントの説明、タイトル、注釈を追加することをお勧めします。

メトリクスグラフの分析時に考慮できる重要な時点:

- デプロイの変更
- 設定変更
- インシデント開始時刻
- アラーム時刻
- エンゲージメント時刻
- 緩和の開始時刻
- インシデント解決時刻

制限事項

- CloudWatch アラームとメトリクス式は、インシデントからインポートされません。
- Incident Manager がサポートしていないリージョンにあるメトリクスは、インシデントからインポートされません。
- アプリケーションアカウントのメトリクスは、分析を作成する前に `CloudWatch-CrossAccountSharingRole` の設定が必要です。ロールの詳細については、CloudWatch ユーザーガイドの「Cross-Account Cross-Region CloudWatch コンソール」を参照してください。

タイムライン

インシデントの理解を深めながら、タイムライン上の重要な時点を説明してください。インシデントのタイムラインは、このタブに自動的に入力されます。分析に関係のないタイムポイントを削除できます。また、時点を追加· 編集して、インシデントとその影響をより正確に記述することもできます。

[タイムライン] タブでは、 質問 タブで見つけたインシデント対応に関する質問に答えます。

Questions

Incident Manager の質問を使用して、アプリケーション内のインシデントの解決までの時間を短縮し、インシデントの発生を減らします。質問に答えながら、メトリクス と タイムライン タブを更新して、精度を確認します。これらの質問は、インシデント対応の主な側面に焦点を当てています。

- 検出 — 検出までの時間を改善できますか。インシデントを早く検出するメトリクスとアラームの更新はありますか。
- 診断 — 診断までの時間を改善できますか。対応計画またはエスカレーション計画の更新があり、正しい応答者をより早くエンゲージすることはありますか。
- 緩和 — 緩和までの時間を改善できますか。追加または改善できるランブックステップはありますか。
- 予防 — 今後のインシデントの発生を防ぐことはできますか。インシデントの根本原因を発見するために、Amazon は問題調査で 5-Whys アプローチを使用しています。

アクション

Incident Manager は、質問の完了時にレビューするための推奨アクション項目を作成します。このタブでは、これらのアクションを受け入れて完了するか、これらのアクションを却下するかを選択できます。却下されたアクション項目を確認するには、却下されたアクション項目を選択します。アクション項目は、OpsCenter の分析とインシデントにリンクされている OpsItem の一種です。

チェックリスト

分析を閉じる前に、チェックリストを使用して、応答者が実行すべきアクションを確認します。応答者がチェックリスト内のアクションを完了すると、アクションの横にあるアイコンが楕円からチェックマークに変わり、アクションが完了したことを示します。チェックリスト項目が完了していない場合、Incident Manager は応答者が分析を完了せずに閉じることを希望していることを確認するメッセージを表示します。

分析テンプレート

分析テンプレートは、インシデントの根本原因を深く掘り下げた一連の質問を提供します。これらの質問に対する回答を使用して、アプリケーションのパフォーマンスとインシデント対応を改善できます。

AWS スタンダードテンプレート

Incident Manager は、AWS インシデント対応や問題分析のベストプラクティスに基づいた、`AWSIncidents-PostIncidentAnalysisTemplate` というタイトルの標準的な質問のテンプレートを提供します。

分析テンプレートを作成する

デフォルトの AWSIncidents-PostIncidentAnalysisTemplate テンプレートを使用し、ユースケースに適した質問やセクションを追加することをお勧めします。デフォルトのテンプレートに基づいて分析テンプレートを作成します。このテンプレートを出発点として使用し、管理アカウントで分析テンプレートを作成します。その後、Incident Manager を有効にした各リージョンに分析テンプレートを複製できます。

分析テンプレートを作成する

1. GetDocument アクションを呼び出し、その Name パラメータを使用して AWSIncidents-PostIncidentAnalysisTemplate をダウンロードします。GetDocument 構文の詳細については、Systems Manager API リファレンスを参照してください。
2. 対応のコンテンツには、分析用の JSON 構築ブロックが含まれています。質問構築ブロックを使用して、分析に追加の質問を挿入します。Incident questions セクションで質問またはセクションを追加することをお勧めします。
3. 新しいテンプレートを作成するには、前のステップで更新された JSON を使用して CreateDocument オペレーションを行います。以下を含める必要があります。ここで、*Analysis_Template_Name* はテンプレートの名前です。

   - DocumentFormat: "JSON"
   - DocumentType: "ProblemAnalysisTemplate"
   - Name: "*Analysis_Template_Name*"

分析の作成

1. 分析を作成するには、解決済みのインシデントの「インシデントの詳細」ページから 分析の作成 を選択します。
2. この分析を作成する分析テンプレートを選択し、分析の説明的な名前を入力します。
3. [Create] (作成) を選択します。

フォーマット済みインシデント分析の印刷

印刷用にフォーマットされた完全または不完全な分析のコピーを生成できます。このコピーは PDF として保存することもできます。分析は一度に 1 つずつ印刷できます。現在、複数の分析のバッチ印刷はサポートされていません。

フォーマット済み分析を印刷するには

1. Incident Manager コンソールを開きます。
2. [分析] タブを選択します。
3. 印刷する分析のタイトルを選択します。
4. 分析詳細ページの右上の [印刷] を選択します。
5. [インシデント分析の印刷] ダイアログボックスで、印刷バージョンに含めない分析のセクションをクリアします。デフォルトでは、すべてのセクションが選択されています。
6. [印刷] を選択すると、デバイスのローカル印刷コントロールが開きます。
7. 印刷先または印刷形式を選択します。ローカルプリンタまたはネットワークプリンタを選択するか、分析を PDF に保存できます。必要に応じて残りの印刷オプションを変更し、[印刷] を選択します。

> **Note**
>
> ローカル印刷コントロールとは、Web ブラウザおよびデバイスが提供するユーザーインターフェイスを指します。
> 印刷先とは、デバイス用に設定され、デバイスからアクセスできる送信先です。

Incident Manager チュートリアル

これらの AWS Systems Manager Incident Manager チュートリアルは、より堅牢なインシデント管理システムを構築するのに役立ちます。これらのチュートリアルでは、インシデントまたはサポートインシデント対応中に発生する一般的なアクティビティについて説明します。

トピック

- Incident Manager での Systems Manager Automation ランブックの使用
- Incident Manager でのセキュリティインシデントの管理

Incident Manager での Systems Manager Automation ランブックの使用

Automation AWS Systems Managerランブックを使用すると、 AWS サービスの一般的なメンテナンス、デプロイ、修復タスクを簡素化できます。このチュートリアルでは、Incident Manager のインシデント対応を自動化するためのカスタムランブックを作成します。このチュートリアルのシナリオでは、Amazon EC2 メトリクスに割り当てられた Amazon CloudWatch アラームを使用します。インスタンスがアラームをトリガーする状態になると、Incident Manager は以下のタスクを自動的に実行します。

1. Incident Manager でインシデントを作成します。
2. 問題の修正を試みるランブックを開始します。
3. ランブックの結果を Incident Manager のインシデント詳細ページに発行します。

このチュートリアルで説明するプロセスは、Amazon EventBridge イベントやその他のタイプの AWS リソースでも使用できます。アラームおよびイベントへの修復対応を自動化することで、インシデントが組織およびそのリソースに与える影響を軽減できます。

このチュートリアルでは、Incident Manager 対応計画の Amazon EC2 インスタンスに割り当てられた CloudWatch アラームを編集する方法について説明します。アラーム、インスタンス、または対応計画が設定されていない場合は、開始する前にそれらのリソースを設定することをお勧めします。詳細については、次のトピックを参照してください。

- 「Amazon ユーザーガイド」の「Amazon CloudWatch アラームの使用 CloudWatch 」
- Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスAmazon EC2」

- Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスAmazon EC2」
- Incident Manager での対応計画の操作

> **Important**
>
> AWS リソースを作成し、ランブックの自動化ステップを使用することで、コストが発生します。詳細については、「AWS 料金表」を参照してください。

トピック

- タスク 1: ランブックを作成する
- タスク 2: IAM ロールの作成
- タスク 3: ランブックを対応計画に接続する
- タスク 4: 対応計画に CloudWatch アラームを割り当てる
- タスク 5: 結果の検証

タスク 1: ランブックを作成する

Systems Manager コンソールでランブックを作成するには、以下の手順を使用します。Incident Manager のインシデントから呼び出されると、ランブックは Amazon EC2 インスタンスを再起動し、ランブックの実行に関する情報でインシデントを更新します。開始する前に、ランブックを作成するアクセス許可があることを確認します。詳細については、「AWS Systems Manager ユーザーガイド」の「オートメーションの設定」を参照してください。

> **Important**
>
> このチュートリアルのランブックの作成に関する以下の重要な詳細情報を確認してください。
>
> - ランブックは、 CloudWatch アラームソースから作成されたインシデントを対象としています。このランブックを他のタイプのインシデント (手動で作成したインシデントなど) に使用すると、ランブックの最初のステップのタイムラインイベントが見つからず、システムからエラーが返されます。
> - ランブックでは、 CloudWatch アラームに というディメンションが含まれている必要がありますInstanceId。Amazon EC2 インスタンスメトリクスのアラームにはこのディメンションがあります。このランブックを他のメトリクス (または などの他のインシデント

ソース EventBridge) で使用する場合は、シナリオでキャプチャされたデータと一致するようにJsonDecode2ステップを変更する必要があります。

- ランブックは Amazon EC2 インスタンスを再起動することで、アラームをトリガーした問題の修正を試みます。実際のインシデントでは、インスタンスを再起動したくない場合があります。システムに実行させたい具体的な修正アクションでランブックを更新してください。

ランブックの作成に関する詳細は、「AWS Systems Manager ユーザーガイド」の「Working with runbooks」を参照してください。

ランブックを作成するには

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. [オートメーション] を選択します。
4. [名前] に、ランブックのわかりやすい名前 (**IncidentResponseRunbook** など) を入力します。
5. [Editor (エディタ)] タブを選択し、次に [Edit (編集)] を選択します。
6. エディタに、以下の内容を貼り付けます。

```
description: This runbook attempts to restart an Amazon EC2 instance that caused an
 incident.
schemaVersion: '0.3'
parameters:
  IncidentRecordArn:
    type: String
    description: The incident
mainSteps:
  - name: ListTimelineEvents
    action: 'aws:executeAwsApi'
    outputs:
      - Selector: '$.eventSummaries[0].eventId'
        Name: eventId
        Type: String
    inputs:
      Service: ssm-incidents
      Api: ListTimelineEvents
```

```
      incidentRecordArn: '{{IncidentRecordArn}}'
      filters:
        - key: eventType
          condition:
            equals:
              stringValues:
                - SSM Incident Trigger
    description: This step retrieves the ID of the first timeline event with the
CloudWatch alarm details.
  - name: GetTimelineEvent
    action: 'aws:executeAwsApi'
    inputs:
      Service: ssm-incidents
      Api: GetTimelineEvent
      incidentRecordArn: '{{IncidentRecordArn}}'
      eventId: '{{ListTimelineEvents.eventId}}'
    outputs:
      - Name: eventData
        Selector: $.event.eventData
        Type: String
    description: This step retrieves the timeline event itself.
  - name: JsonDecode
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["eventData"])
          return data
      InputPayload:
        eventData: '{{GetTimelineEvent.eventData}}'
    outputs:
      - Name: rawData
        Selector: $.Payload.rawData
        Type: String
    description: This step parses the timeline event data.
  - name: JsonDecode2
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
```

```
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["rawData"])
          return data
      InputPayload:
        rawData: '{{JsonDecode.rawData}}'
    outputs:
      - Name: InstanceId
        Selector:
'$.Payload.detail.configuration.metrics[0].metricStat.metric.dimensions.InstanceId'
        Type: String
    description: This step parses the CloudWatch event data.
  - name: RestartInstance
    action: 'aws:executeAutomation'
    inputs:
      DocumentName: AWS-RestartEC2Instance
      DocumentVersion: $DEFAULT
      RuntimeParameters:
        InstanceId: '{{JsonDecode2.InstanceId}}'
    description: This step restarts the Amazon EC2 instance
```

7. [Create automation (オートメーションを作成)] を選択します。

タスク 2: IAM ロールの作成

次のチュートリアルを使用して、対応計画で指定されたランブックを開始するアクセス許可を Incident Manager に付与する AWS Identity and Access Management (IAM) ロールを作成します。このチュートリアルのランブックは、Amazon EC2 インスタンスを再起動します。この IAM ロールは次のタスクで、ランブックを対応計画に接続するときに指定します。

対応計画からランブックを開始する IAM ロールを作成する

1. https://console.aws.amazon.com/iam/IAMコンソールを開きます。
2. ナビゲーションペインで ロール を選択してから、ロールを作成する を選択します。
3. [信頼されたエンティティタイプ] で、[AWS サービス] が選択されていることを確認します。
4. [ユースケース] の [その他の AWS サービスのユースケース] フィールドに **Incident Manager** を入力します。
5. [Incident Manager] を選択し、[次へ] を選択します。

6. [アクセス許可の追加] ページで、[ポリシーの作成] を選択します。アクセス許可エディタが新しいブラウザウィンドウまたはタブで開きます。
7. エディタで、[JSON] タブを選択します。
8. 以下のアクセス許可ポリシーをコピーして、JSON エディタに貼り付けます。*account_ID* を自分の AWS アカウント ID に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:account_ID:automation-definition/
IncidentResponseRunbook:*",
                "arn:aws:ssm:*::automation-definition/AWS-RestartEC2Instance:*"
            ],
            "Action": "ssm:StartAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Action": "ssm:GetAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm-incidents:*:*:*",
            "Action": "ssm-incidents:*"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances"
            ]
```

```
        }
    ]
}
```

9. [Next: Tags] (次へ: タグ) を選択します。
10. (オプション) 必要に応じて、タグをポリシーに追加します。
11. [次へ: レビュー] を選択します。
12. [名前] フィールドに、このロールがチュートリアルで使用されるものであることを識別するのに役立つ名前を入力します。
13. (オプション) [説明] フィールドに説明を入力します。
14. [ポリシーの作成] を選択します。
15. 作成しているロールのブラウザウィンドウまたはタブに戻ります。[アクセス許可の追加] ページが表示されます。
16. 更新ボタン ([ポリシーの作成] ボタンの横にあります) を選択し、作成したアクセス許可ポリシーの名前をフィルターボックスに入力します。
17. 作成したアクセス許可ポリシーを選択し、[次へ] を選択します。
18. [名前、レビュー、および作成] ページの [ロール名] に、このロールがチュートリアルで使用されるものであることを識別するのに役立つ名前を入力します。
19. (オプション) [説明] フィールドに説明を入力します。
20. ロールの詳細を確認し、必要に応じてタグを追加し、[ロールの作成] を選択します。

タスク 3: ランブックを対応計画に接続する

ランブックを Incident Manager の対応計画に接続することで、一貫性があり、反復可能で、タイムリーな緩和プロセスを確保できます。このランブックは、リゾルバーが次の一連のアクションを決定するための出発点としても役立ちます。

ランブックを対応計画に割り当てるには

1. Incident Manager コンソールを開きます。
2. [対応計画] を選択します。
3. [対応計画] では、既存の対応計画を選択し、[編集] を選択します。既存の対応計画がない場合は、[対応計画の作成] を選択して新しい対応計画を作成します。

   以下のフィールドに値を入力します。

a. [ランブック] セクションで [既存のランブックを選択] を選択します。
b. [所有者] に [自分が所有] が選択されていることを確認します。
c. [ランブック] では、タスク 1: ランブックを作成する で作成したランブックを選択します。
d. [バージョン] では、[実行時のデフォルト] を選択します。
e. 入力セクションの IncidentRecordArn パラメータで、インシデント ARN を選択します。
f. [実行アクセス許可] セクションで、タスク 2: IAM ロールの作成 で作成した IAM ロールを選択します。

4. 変更を保存します。

タスク 4: 対応計画に CloudWatch アラームを割り当てる

次の手順を使用して、Amazon EC2 インスタンスの CloudWatch アラームを対応計画に割り当てます。

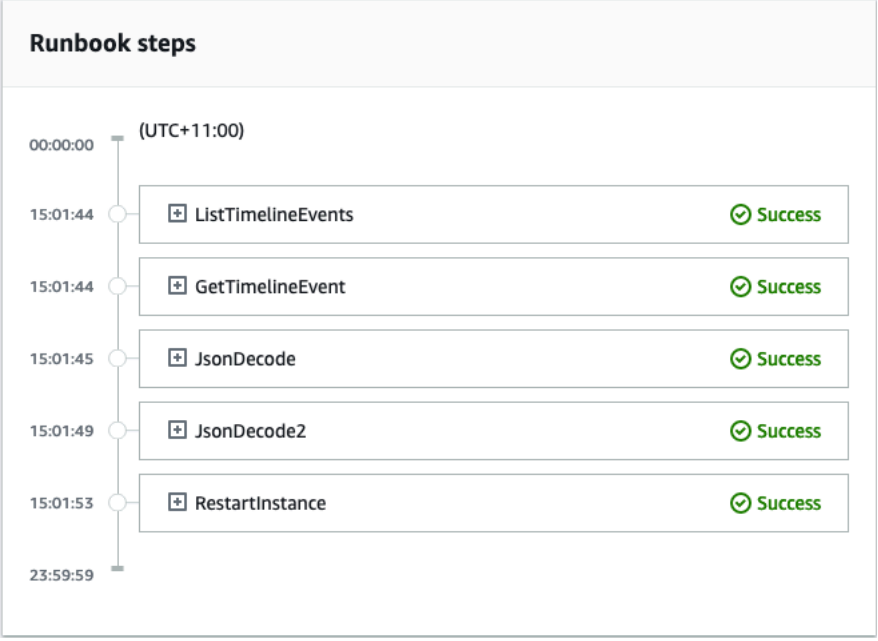
対応計画に CloudWatch アラームを割り当てるには

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の [アラーム] で、[すべてのアラーム] を選択します。
3. 対応計画に接続する Amazon EC2 インスタンスのアラームを選択します。
4. [Actions] (アクション) を選択して、[Edit] (編集) を選択します。メトリクスに `InstanceId` というディメンションがあることを確認します。
5. [次へ] をクリックします。
6. [アクションの設定ウィザード] で、[Systems Manager アクションを追加] を選択します。
7. [インシデントの作成] を選択します。
8. タスク 3: ランブックを対応計画に接続する で作成した対応計画を選択します。
9. [Update alarm] (アラームの更新) を選択します。

タスク 5: 結果の検証

CloudWatch アラームがインシデントを作成し、対応計画で指定されたランブックを処理することを確認するには、アラームをトリガーする必要があります。アラームをトリガーしてランブックの処理が終了したら、以下の手順を使用してランブックの結果を確認できます。アラームをトリガーする方法については、「AWS CLI Command Reference」の「set-alarm-state」を参照してください。

1. Incident Manager コンソールを開きます。
2. CloudWatch アラームによって作成されたインシデントを選択します。
3. [ランブック] タブを選択します。
4. Amazon EC2 インスタンスで実行されたアクションは、[ランブックのステップ] セクションで確認できます。以下の画像は、このチュートリアルで作成したランブックで実行されたステップの例です。各ステップはタイムスタンプおよびステータスメッセージと共に一覧表示されます。



CloudWatch アラームのすべての詳細を表示するには、JsonDecode2 ステップを展開し、出力を展開します。

> **Important**
>
> このチュートリアルで実装したリソースの変更のうち、残さないものはすべてクリーンアップする必要があります。これには、リソースプランやインシデントなどの Incident Manager リソースの変更、 CloudWatch アラームの変更、このチュートリアル用に作成した IAM ロールが含まれます。

Incident Manager でのセキュリティインシデントの管理

AWS Security Hub、Amazon EventBridge、Incident Manager を一緒に使用して、 AWS ホストアプリケーションのセキュリティインシデントを特定および管理できます。このチュートリアルで

は、Security Hub が自動的に送信した検出結果に基づいてインシデントを作成する EventBridge ルールを設定する手順を説明します。

> **Note**
>
> このチュートリアルでは、 EventBridge Security Hub を使用します。これらのサービスの使用によりコストが発生する場合があります。

前提条件

- Security Hub を設定します。詳細については、「AWS Security Hubの設定」を参照してください。
- Security Hub で調査結果を作成または更新します。詳細については、AWS Security Hubの調査結果を参照してください。
- Incident Manager がセキュリティインシデントを作成するときに、テンプレートとして使用する対応計画を設定します。詳細については、「Incident Manager でのインシデントへの準備」を参照してください。

このチュートリアルでは、事前定義されたパターンを使用して EventBridge ルールを作成します。カスタムパターンを使用してルールを作成するには、ユーザーガイドの「カスタムパターンを使用してルールを作成する AWS Security Hub 」を参照してください。

EventBridge ルールを作成する

1. https://console.aws.amazon.com/events/ で Amazon EventBridge コンソールを開きます。
2. ナビゲーションペインで Rules] (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 [Name (名前)] と [Description (説明)] に入力します。

   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. 次へ をクリックします。
8. イベントソース で、AWS イベント または EventBridgeパートナーイベント 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、[Security Hub] を選択します。
12. [Event type] (イベントタイプ)で、[Security Hub Findings - Imported] (Security Hub 調査結果 - インポート) を選択します。
13. デフォルトでは、 はフィルター値なしでイベントパターン EventBridge を設定します。各属性では、いずれかの **###** オプションが選択されます。これらのフィルターを更新して、環境に最も影響を与えるセキュリティ調査結果に基づいてインシデントを作成します。
14. [次へ] をクリックします。
15. ターゲットタイプ] では、AWS サービス] を選択します。
16. [ターゲットの選択] では、[Incident Manager 対応計画] を選択します。
17. 対応計画では、作成したインシデントのテンプレートとして使用する対応計画を選択します。
18. EventBridge は、ルールの実行に必要な IAM ロールを作成できます。
    - 自動的に IAM ロールを作成するには、[特定のリソースに対して新しいロールを作成する] を選択します。
    - アカウントに既に存在する IAM ロールを使用するには、「既存のロールの使用」を選択します。
19. (オプション) ルールに 1 つ以上のタグを入力します。
20. 次へ をクリックします。
21. ルールの詳細を確認し、ルールの作成 を選択します。

この EventBridge ルールを作成したので、定義した属性値と一致するセキュリティ検出結果は Incident Manager でインシデントを作成します。これらのインシデントから、インシデント後分析をトリアージ、管理、モニタリング、作成できます。

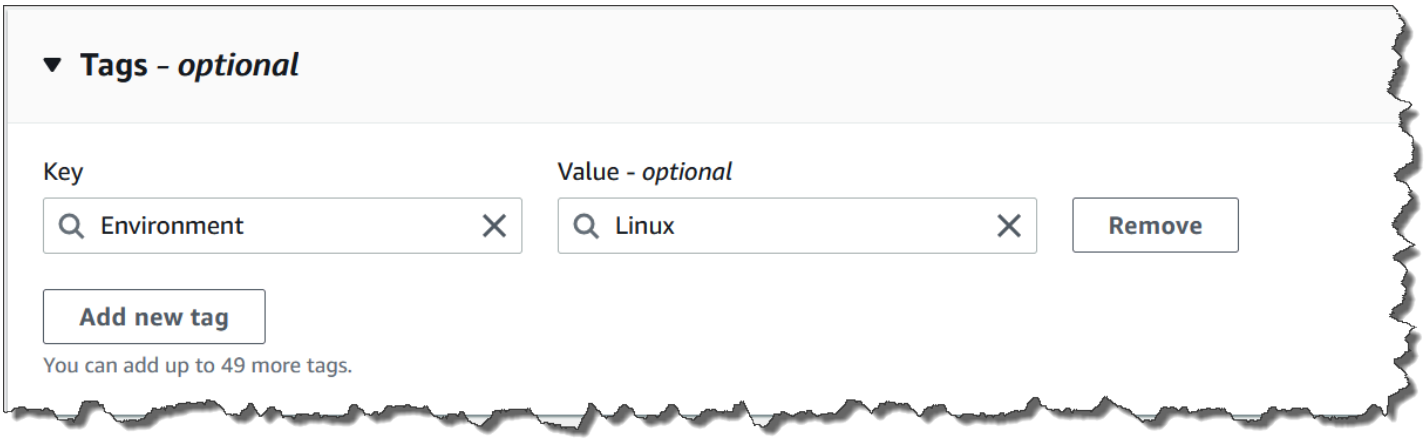
Incident Manager でのリソースのタグ付け

タグは、レプリケーションセットで指定された AWS リージョン 内の Incident Manager リソースに割り当てることができるオプションのメタデータです。対応計画、インシデントレコード、連絡先にタグを割り当てることができます。オンコールスケジュールおよびローテーションにタグを追加することもできます。また、レプリケーションセット自体にタグを追加することもできます。タグを使用すると、さまざまな方法でこれらのリソースを分類し、アクセスを制御できます。タグはそれぞれ、1 つのキーとオプションの 1 つの値で設定されており、どちらもお客様側が定義します。各 Incident Manager リソースタイプのニーズを満たす一連のタグキーを考案することをお勧めします。一貫性のある一連のタグキーを使用することで、これらのリソースの管理およびリソースへのアクセスの管理が容易になります。タグに基づいてリソースを検索およびフィルタリングできます。タグを使用したリソースへのアクセス制御の詳細については、「IAM ユーザーガイド」の「タグを使用した AWS リソースへのアクセスの制御」を参照してください。

対応計画を作成するときに、[インシデントのデフォルト] セクションでタグを指定できます。これらのタグは、対応計画を使用してインシデントが作成されるときにインシデントレコードに適用されます。

> **Note**
>
> タグには意味論的な意味がありません。タグは単なる文字列として解釈されます。

Incident Manager コンソールを使用して、タグを追加または削除できます。以下のスクリーンショットは、新しい対応計画を作成するときのタグセクションを示しています。



タグをプログラムで操作するには、以下の API アクションを使用します。

- TagResource
- UntagResource
- ListTagsForResource

> **Important**
>
> 対応計画、インシデントレコード、連絡先、オンコールスケジュールとローテーション、およびレプリケーションセットに適用されるタグは、リソース所有者アカウントからのみ表示および変更できます。

のセキュリティ AWS Systems Manager Incident Manager

のクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — AWS は、 AWS のサービス で実行されるインフラストラクチャを保護する責任を担います AWS クラウド。また、 は、安全に使用できるサービス AWS も提供します。コンプライアンスAWS プログラム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者は定期的にセキュリティの有効性をテストおよび検証。に適用されるコンプライアンスプログラムの詳細については AWS Systems Manager Incident Manager、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Incident Manager の使用時に責任共有モデルがどのように適用されるかを理解するために役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Incident Manager を設定する方法を示します。また、Incident Manager リソースのモニタリングや保護 AWS のサービス に役立つ他の の使用方法についても説明します。

トピック

- Incident Manager でのデータ保護
- の Identity and Access Management AWS Systems Manager Incident Manager
- Incident Manager での共有連絡先と対応計画の操作
- のコンプライアンス検証 AWS Systems Manager Incident Manager
- の耐障害性 AWS Systems Manager Incident Manager
- のインフラストラクチャセキュリティ AWS Systems Manager Incident Manager
- AWS Systems Manager Incident Manager およびインターフェイス VPC エンドポイントの操作 (AWS PrivateLink)
- Incident Manager での設定と脆弱性の分析

- におけるセキュリティのベストプラクティス AWS Systems Manager Incident Manager

Incident Manager でのデータ保護

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Systems Manager Incident Manager。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。
- を使用して 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、または SDK を使用して Incident Manager 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。

デフォルトでは、Incident Manager は SSL/TLS を使用して、転送中のデータを暗号化します。

データ暗号化

Incident Manager は AWS Key Management Service 、 (AWS KMS) キーを使用して Incident Manager リソースを暗号化します。の詳細については AWS KMS、「 AWS KMS デベロッパーガイド」を参照してください。 AWS KMS は、安全で可用性の高いハードウェアとソフトウェアを組み合わせて、クラウド向けに拡張されたキー管理システムを提供します。Incident Manager は、指定したキーを使用してデータを暗号化し、 AWS 所有キーを使用してメタデータを暗号化します。Incident Manager を使用するには、暗号化の設定を含むレプリケーションセットを設定する必要があります。Incident Manager を使用するには、データ暗号化が必要です。

AWS 所有キーを使用してレプリケーションセットを暗号化することも、 で作成した独自のカスタマーマネージドキーを使用してレプリケーションセット内のリージョンを AWS KMS 暗号化することもできます。Incident Manager は、 内で作成されたデータを暗号化するための対称暗号化 AWS KMS キーのみをサポートします AWS KMS。Incident Manager は、インポートされた AWS KMS キーマテリアル、カスタムキーストア、ハッシュベースのメッセージ認証コード (HMAC)、またはその他のタイプのキーを持つキーをサポートしていません。カスタマーマネージドキーを使用する場合は、AWS KMS コンソール または AWS KMS APIを使用してカスタマーマネージドキーを一元的に作成し、Incident Manager がカスタマーマネージドキーを使用する方法を制御するキーポリシーを定義します。Incident Manager での暗号化にカスタマーマネージドキーを使用する場合、 AWS KMS カスタマーマネージドキーは リソースと同じリージョンに存在する必要があります。Incident Manager でのデータ暗号化の設定の詳細については、「準備ウィザード」をご参照ください。

AWS KMS カスタマーマネージドキーの使用には追加料金がかかります。詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS の概念 - KMS キー」および「AWS KMS pricing」を参照してください。

> **Important**
>
> カスタマーマネージドキー (CMK) を使用してレプリケーションセットおよび Incident Manager データを暗号化し、後でそのレプリケーションセットを削除する場合は、CMK を無効化または削除する前に、必ずレプリケーションセットを削除してください。

Incident Manager がカスタマーマネージドキーを使用してデータを暗号化できるようにするには、カスタマーマネージドキーのキーポリシーに次のポリシーステートメントを追加する必要があります。アカウントでのキーポリシーのセットアップおよび変更の詳細については、「AWS Key

Management Service デベロッパーガイド」の「Using key policies in AWS KMS」を参照してください。このポリシーで、次の許可が付与されます。

- Incident Manager がアカウント内の Incident Manager の CMK を検索するための読み取り専用オペレーションの実行を許可します。
- Incident Manager が CMK を使用して許可を作成し、キーを記述することを許可します。ただし、Incident Manager の使用を許可されているアカウントのプリンシパルを代表して行動する場合に限ります。ポリシー ステートメントで指定されたプリンシパルが、KMS キーの使用と Incident Manager の使用を許可されていない場合、Incident Manager サービスからの呼び出しであっても、呼び出しは失敗します。

```
    {
    "Sid": "Allow CreateGrant through AWS Systems Manager Incident Manager",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:user/ssm-lead"
    },
    "Action": [
      "kms:CreateGrant",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "ssm-incidents.amazonaws.com",
          "ssm-contacts.amazonaws.com"
        ]
      }
    }
  }
```

`Principal` の値を、レプリケーションセットを作成した IAM プリンシパルに置き換えます。

Incident Manager は、暗号化オペレーションのために へのすべてのリクエストで暗号化コンテキストを使用します。 AWS KMS この暗号化コンテキストを使用して、Incident Manager が KMS キーを使用する CloudTrail ログイベントを識別できます。Incident Manager では、次の暗号化コンテキストが使用されます。

- `contactArn=`*`ARN of the contact or escalation plan`*

の Identity and Access Management AWS Systems Manager Incident Manager

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 Incident Manager 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。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
- が IAM と AWS Systems Manager Incident Manager 連携する方法
- AWS Systems Manager Incident Managerのアイデンティティベースのポリシーの例
- のリソースベースのポリシーの例 AWS Systems Manager Incident Manager
- Incident Manager におけるサービス間の混乱した代理の防止
- Incident Manager のサービスリンクロールの使用
- AWS の マネージドポリシー AWS Systems Manager Incident Manager
- AWS Systems Manager Incident Manager ID 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、Incident Manager で行う作業によって異なります。

サービスユーザー – ジョブを実行するために Incident Manager サービスを使用する場合は、管理者から必要なアクセス許可と認証情報が与えられます。さらに多くの Incident Manager 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。Incident Manager の機能にアクセスできない場合は、「AWS Systems Manager Incident Manager ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Incident Manager リソースを担当している場合は、通常、Incident Manager へのフルアクセスがあります。サービスユーザーがアクセスする必要がある Incident Manager の機

能およびリソースを決定するのは、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。お客様の会社で Incident Manager で IAM を利用する方法の詳細については、「が IAM と AWS Systems Manager Incident Manager 連携する方法」を参照してください。

IAM 管理者 – 管理者は、Incident Manager 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。IAM で使用できる Incident Manager 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、「AWS Systems Manager Incident Managerのアイデンティティベースのポリシーの例」を参照してください。

アイデンティティを使用した認証

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、フェデレーティッド 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、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント 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 AWS のサービス およびリソースへの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、Identity Center ディレクトリのユーザー、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「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の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リソースアクセス」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、サービスリンクロールの許可を表示できますが、編集することはできません。
- 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、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、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。

が IAM と AWS Systems Manager Incident Manager 連携する方法

IAM を使用して Incident Manager へのアクセスを管理する前に、Incident Manager で使用できる IAM の機能について説明します。

で使用できる IAM の機能 AWS Systems Manager Incident Manager

IAM 機能	Incident Manager サポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	はい
ポリシーアクション	Yes
ポリシーリソース	Yes
ポリシー条件キー	いいえ

IAM 機能	Incident Manager サポート
ACL	No
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	Yes
プリンシパル権限	Yes
サービスロール	あり
サービスリンクロール	はい

Incident Manager 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AWS 「IAM と連携する のサービス」を参照してください。

Incident Manager は、 AWS RAMで共有されているリソースへのアクセスを拒否するポリシーをサポートしていません。

Incident Manager 用 ID ベースのポリシー

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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。

Incident Manager 用 ID ベースのポリシーの例

Incident Manager でのアイデンティティベースのポリシーの例は、「AWS Systems Manager Incident Managerのアイデンティティベースのポリシーの例」でご確認ください。

Incident Manager 内のリソースベースのポリシー

リソースベースのポリシーのサポート	はい

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。

Incident Manager サービスは、対応計画または連絡先にアタッチされている AWS RAM コンソールまたは PutResourcePolicy アクションを使用して、 と呼ばれる 2 種類のリソースベースのポリシーのみをサポートします。このポリシーは、対応計画、連絡先、エスカレーション計画、およびインシデントに対してアクションを実行できるプリンシパルを定義します。Incident Manager は、リソースベースのポリシーを使用して、アカウント間でリソースを共有します。

Incident Manager は、 AWS RAMで共有されているリソースへのアクセスを拒否するポリシーをサポートしていません。

リソースベースのポリシーを対応計画または連絡先にアタッチする方法については、Incident Manager でのクロスリージョンおよびクロスアカウントのインシデント管理を参照してください。

Incident Manager のリソースベースのポリシーの例

Incident Manager のリソースベースのポリシー例を表示するには、「のリソースベースのポリシーの例 AWS Systems Manager Incident Manager」を参照してください。

Incident Manager のポリシーアクション

ポリシーアクションに対するサポート	はい

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。

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。

Incident Manager 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「AWS Systems Manager Incident Managerによって定義されるアクション」を参照してください。

Incident Manager のポリシーアクションでは、アクションの前に次のプレフィックスを使用します。

```
ssm-incidents
ssm-contacts
```

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": [
      "ssm-incidents:GetResponsePlan",
      "ssm-contacts:GetContact"
         ]
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、Get という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "ssm-incidents:Get*"
```

Incident Manager でのアイデンティティベースのポリシーの例は、「AWS Systems Manager Incident Managerのアイデンティティベースのポリシーの例」でご確認ください。

Incident Manager は、ssm インシデントと ssm 連絡先という 2 つの異なる名前空間でアクションを使用します。Incident Manager のポリシーを作成するときは、アクションに名前空間を正しく使用してください。SSM インシデントは、対応計画およびインシデント関連のアクションに使用されます。SSM 連絡先は、連絡先と連絡先のエンゲージメントに関連するアクションに使用されます。例:

- `ssm-contacts:GetContact`
- `ssm-incidents:GetResponsePlan`

Incident Manager のポリシーリソース

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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": "*"
```

Incident Manager でのリソースタイプとその ARN のリストを確認するには、「サービス認証リファレンス」の「AWS Systems Manager Incident Managerによって定義されたリソースタイプ」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、「AWS Systems Manager Incident Managerで定義されるアクション」を参照してください。

Incident Manager でのアイデンティティベースのポリシーの例は、「AWS Systems Manager Incident Managerのアイデンティティベースのポリシーの例」でご確認ください。

Incident Manager リソースは、インシデントの作成、チャットチャネルでのコラボレーション、インシデントの解決、レスポンダーのエンゲージメントに使用されます。ユーザーが応答計画へのアクセス権を持っている場合、その対応計画から作成されたすべてのインシデントへのアクセス権があります。ユーザーが連絡先またはエスカレーションプランへのアクセス権を持っている場合、エスカレーションプランの連絡先にエンゲージできます。

Incident Manager のポリシー条件キー

サービス固有のポリシー条件キーのサポート	いいえ

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 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。

Incident Manager のアクセスコントロールリスト (ACL)

ACL のサポート	No

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。

Incident Manager での属性ベースのアクセスコントロール (ABAC)

ABAC (ポリシー内のタグ) のサポート	いいえ

属性ベースのアクセス制御 (ABAC) は、属性に基づいて権限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はいです。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 を設定する手順を示したチュートリアルを表示するには、IAM ユーザーガイドの 属性ベースの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。

Incident Manager での一時的な認証情報の使用

一時的な認証情報のサポート	はい

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。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。

Incident Manager のクロスサービスプリンシパル許可

フォワードアクセスセッション (FAS) をサポート	はい

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。

Incident Manager 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**
>
> サービスロールの許可を変更すると、Incident Manager の機能が破損する可能性があります。Incident Manager が指示する場合以外は、サービスロールを編集しないでください。

Incident Manager での IAM ロールの選択

Incident Manager で対応計画リソースを作成する場合、ユーザーに代わって Systems Manager の自動化ドキュメントを Incident Manager で実行できるようにするロールを選択する必要があります。サービスロールあるいはサービスにリンクされたロールを以前に作成している場合、Incident Manager は選択できるロールのリストを示します。オートメーションドキュメントインスタンスの実行へのアクセスを許可するロールを選択することが重要です。詳細については、「Incident Manager での Systems Manager Automation ランブックの操作」を参照してください。インシデント中に使用する AWS Chatbot チャットチャネルを作成するときは、チャットから直接コマンドを使用できるようにするサービスロールを選択できます。インシデントコラボレーション用のチャットチャネルの作成の詳細については、「Incident Manager でのチャットチャネルの操作」をご参照ください。の IAM ポリシーの詳細については AWS Chatbot、「 AWS Chatbot 管理者ガイド」の「 を使用してコマンドを実行するためのアクセス許可の管理 AWS Chatbot」を参照してください。

Incident Manager のサービスリンクロール

サービスリンクロールのサポート	はい

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、サービスリンクロールの許可を表示できますが、編集することはできません。

Incident Manager 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、「Incident Manager のサービスリンクロールの使用」を参照してください。

AWS Systems Manager Incident Managerのアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールには、Incident Manager リソースを作成または変更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。

Incident Manager が定義するアクションおよびリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認証リファレンス」の「AWS Systems Manager Incident Managerのアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- Incident Manager コンソールの使用
- 自分の権限の表示をユーザーに許可する
- 応答計画へのアクセス

ポリシーのベストプラクティス

アイデンティティベースのポリシーは、アカウント内で誰かが Incident Manager のリソースを作成、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「AWS ジョブ機能の管理ポリシー」を参照してください。

- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、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 を介し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。

Incident Manager コンソールの使用

AWS Systems Manager Incident Manager 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、 AWS アカウントの Incident Manager リソースの詳細をリストおよび表示できます。最小限必要な許可よりも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 Incident Manager コンソールを使用してインシデントを解決できるようにするには、Incident Manager `IncidentManagerResolverAccess` AWS 管理ポリシーもエンティティにアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

```
IncidentManagerResolverAccess
```

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": "*"
        }
    ]
}
```

応答計画へのアクセス

この例では、Amazon Web Services アカウントの IAM ユーザーに、Incident Manager の対応計画の 1 つである「exampleplan」へのアクセス権を付与します。また、ユーザーが対応計画を追加、更新、および削除できるようにします。

このポリシーは、ssm-incidents:ListResponsePlans、ssm-incidents:GetResponsePlan、ssm-incidents:UpdateResponsePlan、ssm-incident:ListResponsePlan アクセス許可をユーザーに付与します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListResponsePlans",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:ListResponsePlans"
         ],
         "Resource":"arn:aws:ssm-incidents:::*"
      },
      {
         "Sid":"ViewSpecificResponsePlanInfo",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:GetResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan"
      },
      {
         "Sid":"ManageResponsePlan",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:UpdateResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan/*"
      }
```

```
    ]
}
```

のリソースベースのポリシーの例 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager は、Incident Manager の対応計画と連絡先のリソースベースのアクセス許可ポリシーをサポートします。

Incident Manager は、 を使用して共有されたリソースへのアクセスを拒否するリソースベースのポリシーをサポートしていません AWS RAM。

対応計画または連絡先を作成する方法については、「Incident Manager での対応計画の操作」と「Incident Manager での連絡先の操作」を参照してください。

組織別の Incident Manager の対応計画アクセスの制限

次の例では、組織 ID: o-abc123def45 の組織内のユーザーに、対応計画 myplanで作成されたインシデントに対応する許可を付与しています。

Condition ブロックは、 StringEquals 条件と、 AWS Organizations 特定のaws:PrincipalOrgID条件キーである 条件キーを使用します。これらの条件キーの詳細については、「ポリシーでの条件の指定」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationAccess",
      "Effect": "Allow",
      "Principal": “*”,
      "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"o-abc123def45"}
      },
      "Action": [
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:StartIncident",
        "ssm-incidents:UpdateIncidentRecord",
```

```
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:UpdateRelatedItems",
        "ssm-incidents:ListRelatedItems"
      ],
      "Resource": [
        "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
        "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
      ]
    }
  ]
}
```

Incident Manager の連絡先にプリンシパルへのアクセスを提供する

次の例では、ARN `arn:aws:iam::999988887777:root` を持つプリンシパルに、連絡先 `mycontact`に対するエンゲージメントの作成を許可しています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
            },
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact"
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
        }
    ]
}
```

Incident Manager におけるサービス間の混乱した代理の防止

不分別な代理処理問題とは、アクションを実行する権限のないエンティティが、権限のあるエンティティにアクションを実行するように 呼び出し をすることで発生する情報セキュリティ上の問題です。これにより、悪意のあるアクターが本来であれば実行またはアクセスの権限がないコマンドを実行したり、リソースを変更することが可能になります。

では AWS、サービス間のなりすましは、混乱した代理シナリオにつながる可能性があります。クロスサービスでのなりすましとは、あるサービス (呼び出し側のサービス) が別のサービス (呼び出しされた側のサービス) を呼び出すことです。悪意のあるアクターは、呼び出し元のサービスを使用して、通常持っていない許可を使用して、別のサービスのリソースを変更できます。

AWS は、 アカウントのリソースへのマネージドアクセスをサービスプリンシパルに提供し、リソースのセキュリティを保護します。リソースポリシーには、aws:SourceArn および aws:SourceAccount のグローバル条件コンテキストキーを使用することをお勧めします。これらのキーは、 がそのリソースに別のサービスに AWS Systems Manager Incident Manager 付与するアクセス許可を制限します。両方のグローバル条件コンテキストキーを同じポリシーステートメントで使用する場合、aws:SourceAccount 値と aws:SourceArn 値で参照されるアカウントは、同じアカウント ID を使用する必要があります。

aws:SourceArn 値は、影響を受けるインシデントレコードの ARN である必要があります。リソースの完全な ARN がわからない場合や、複数のリソースを指定している場合は、ARN の未知部分に * ワイルドカードで aws:SourceArn グローバルコンテキスト条件キーを使用します。たとえば、aws:SourceArn を arn:aws:ssm-incidents::*111122223333*:*に設定できます。

以下の信頼ポリシーの例では、aws:SourceArn 条件キーを使用して、インシデントレコードの ARN に基づいてサービスロールへのアクセスを制限しています。このロールを使用できるのは、対応計画 myresponseplan から作成されたインシデントレコードのみです。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/
myresponseplan/*"
      }
```

```
    }
  }
}
```

Incident Manager のサービスリンクロールの使用

AWS Systems Manager Incident Manager は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスリンクロールは、Incident Manager に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、Incident Manager によって事前定義されており、サービスがユーザーに代わって他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスリンクロールを使用することで、必要なアクセス権限を手動で追加する必要がなくなるため、Incident Manager の設定が簡単になります。Incident Manager は、サービスリンクロールのアクセス許可を定義します。特に定義されている場合を除き、Incident Manager のみがそのロールを引き受けることができます。定義したアクセス許可には、信頼ポリシーと許可ポリシーが含まれます。この許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールは、まずその関連リソースを削除しなければ削除できません。これにより、リソースに対するアクセス許可が誤って削除されることがなくなり、Incident Manager のリソースは保護されます。

サービスリンクロールをサポートするその他のサービスについては、「IAM と連携するAWS サービス」を参照し、サービスリンクロール 列が はい になっているサービスを探してください。サービスにリンクされた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。

Incident Manager でのサービスにリンクされたロールのアクセス許可

Incident Manager は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleforIncidentManager。これにより、Incident Manager はユーザーに代わって Incident Manager のインシデントレコードと関連リソースを管理できます。

AWSServiceRoleforIncidentManager サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `ssm-incidents.amazonaws.com`

ロールのアクセス許可ポリシー `AWSIncidentManagerServiceRolePolicy` は、指定したリソースに対して以下のアクションを完了することを Incident Manager に許可します。

- アクション: アクションに関連するすべてのリソース上のssm-incidents:ListIncidentRecords。
- アクション: アクションに関連するすべてのリソース上のssm-incidents:CreateTimelineEvent。
- アクション: アクションに関連するすべてのリソース上のssm:CreateOpsItem。
- アクション: all resources related to the action. 上でssm:AssociateOpsItemRelatedItem
- アクション: アクションに関連するすべてのリソース上のssm-contacts:StartEngagement。
- アクション: cloudwatch:PutMetricData AWS/IncidentManager名前空間内の CloudWatch メトリクス

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

Incident Manager のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。 AWS Management Console、、 AWS CLIまたは AWS API でレプリケーションセットを作成すると、Incident Manager によってサービスにリンクされたロールが作成されます。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。レプリケーションセットを作成すると、Incident Manager がサービスリンクロールを再作成します。

Incident Manager のサービスにリンクロールを編集する

Incident Manager では、 AWSServiceRoleforIncidentManager 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。

Incident Manager のサービスリンクロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、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ま

たはメンテナンスされることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

サービスリンクロールを削除するには、最初にレプリケーションセットを削除する必要があります。レプリケーションセットを削除すると、対応計画、連絡先、エスカレーションプランなど、Incident Manager で作成および保存されているすべてのデータが削除されます。また、以前に作成したインシデントもすべて失われます。削除された対応計画を指すアラームと EventBridge ルールは、アラームまたはルールの一致時にインシデントを作成しなくなります。レプリケーションセットを削除するには、セット内のすべてのリージョンを削除する必要があります。

> **Note**
>
> リソースを削除する際に、Incident Manager のサービスでそのロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

で使用されるレプリケーションセット内のリージョンを削除するには AWSServiceRoleforIncidentManager

1. Incident Manager コンソール を開き、左のナビゲーションから [設定] を選択します。
2. [レプリケーションセット] のリージョンを選択します。
3. [削除] を選択します。
4. リージョンの削除を確認するには、リージョン名を入力して [削除] を選択します。
5. レプリケーションセット内のすべてのリージョンを削除するまで、この手順を繰り返します。最後のリージョンを削除すると、コンソールは、そのリージョンとともにレプリケーションセットを削除することを通知します。

サービスにリンクされたロールを IAM で手動削除するには

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

Incident Manager サービスリンクロールをサポートするリージョン

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

AWS の マネージドポリシー AWS Systems Manager Incident Manager

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、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ように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 は、新しい AWS のサービス が起動されたとき、または既存のサービスで新しい API AWS オペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

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 マネージドポリシー： AWSIncidentManagerIncidentAccessServiceRolePolicy

IAM エンティティに `AWSIncidentManagerIncidentAccessServiceRolePolicy` をアタッチできます。Incident Manager は、ユーザーに代わって Incident Manager がアクションを実行することを許可する Incident Manager ロールにもこのポリシーをアタッチします。

このポリシーは、Incident Manager が他の特定の のリソースを読み取って、それらのサービスのインシデントに関連する結果を識別 AWS のサービス 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。

- `cloudformation` — プリンシパルが AWS CloudFormation スタックを記述できるようにします。これは、Incident Manager がインシデントに関連する CloudFormation イベントとリソースを識別するために必要です。
- `codedeploy` — プリンシパルが AWS CodeDeploy デプロイを読み取ることを許可します。これは、Incident Manager がインシデントに関連する CodeDeploy デプロイとターゲットを識別するために必要です。
- `autoscaling` — プリンシパルが Amazon Elastic Compute Cloud (EC2) インスタンスが Auto Scaling グループの一部であるかどうかを判断できるようにします。これは、Incident Manager が Auto Scaling グループの一部である EC2 インスタンスの検出結果を提供できるようにするために必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IncidentAccessPermissions",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResources",
                "codedeploy:BatchGetDeployments",
                "codedeploy:ListDeployments",
                "codedeploy:ListDeploymentTargets",
                "autoscaling:DescribeAutoScalingInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSIncidentManagerIncidentAccessServiceRolePolicy」を参照してください。

AWS マネージドポリシー: **AWSIncidentManagerServiceRolePolicy**

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

このポリシーは、インシデントの一覧表示、タイムラインイベントの作成、 の作成 OpsItems、関連項目の への関連付け OpsItems、エンゲージメントの開始、インシデントに関連するメトリクスの発行 CloudWatchを行うアクセス許可を Incident Manager に付与します。

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。

- ssm-incidents - プリンシパルがインシデントを一覧表示し、タイムラインイベントを作成できるようにします。これは、インシデントダッシュボードでインシデント中にレスポンダーがコラボレーションできるようにするために必要です。
- ssm – プリンシパルが関連項目を作成して OpsItems 関連付けることを許可します。これは、インシデントの開始 OpsItem 時に親を作成するために必要です。
- ssm-contacts — プリンシパルがエンゲージメントを開始できるようにします。これは、Incident Manager がインシデント中に連絡先をエンゲージするために必要です。
- cloudwatch – プリンシパルが CloudWatch メトリクスを発行できるようにします。これは、Incident Manager がインシデントに関連するメトリクスを発行するために必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UpdateIncidentRecordPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:CreateTimelineEvent"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "RelatedOpsItemPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem",
                "ssm:AssociateOpsItemRelatedItem"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentEngagementPermissions",
            "Effect": "Allow",
            "Action": "ssm-contacts:StartEngagement",
            "Resource": "*"
        },
        {
            "Sid": "PutCloudWatchMetricPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IncidentManager"
                }
            }
        }
    ]
}
```

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSIncidentManagerServiceRolePolicy」を参照してください。

AWS マネージドポリシー: **AWSIncidentManagerResolverAccess**

AWSIncidentManagerResolverAccess を IAM エンティティにアタッチすることで、IAM エンティティがインシデントを開始、表示、更新できるようになります。これにより、インシデントダッシュボードで顧客のタイムラインイベントと関連アイテムを作成することもできます。このポリシーを AWS Chatbot サービスロールにアタッチすることも、インシデントコラボレーションに使用されるチャットチャネルに関連付けられたカスタマー管理ロールに直接アタッチすることもできます。

AWS Chatbotの IAM ポリシーの詳細については、「AWS Chatbot 管理者ガイド」の「AWS Chatbot を使用してコマンドを実行するための許可の管理」を参照してください。

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。

- ssm-incidents - インシデントの開始、対応計画の一覧表示、インシデントの一覧表示、インシデントの更新、タイムラインイベントの一覧表示、カスタムタイムラインイベントの作成、カスタムタイムラインイベントの更新、カスタムタイムラインイベントの削除、関連アイテムの一覧表示、関連アイテムの作成および関連アイテムの更新を実行できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StartIncidentPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ResponsePlanReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:GetResponsePlan"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentRecordResolverPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:ListTimelineEvents",
```

```
                "ssm-incidents:CreateTimelineEvent",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:DeleteTimelineEvent",
                "ssm-incidents:ListRelatedItems",
                "ssm-incidents:UpdateRelatedItems"
            ],
            "Resource": "*"
        }
    ]
}
```

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSIncidentManagerResolverAccess」を参照してください。

Incident Manager の AWS マネージドポリシーの更新

Incident Manager の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更を自動通知するには、Incident Manager ドキュメント履歴ページの RSS フィードに登録してください。

変更	説明	日付
AWSIncidentManagerIncidentAccessServiceRolePolicy – ポリシーの更新	Incident Manager はAWSIncidentManagerIncidentAccessServiceRolePolicy 、検出結果機能をサポートする新しいアクセス許可を に追加しました。これにより、EC2 インスタンスが Auto Scaling グループの一部であるかどうかを確認できます。	2024 年 2 月 20 日
AWSIncidentManagerIncidentAccessServ	Incident Manager は、インシデントの管理 AWS のサービ	2023 年 11 月 17 日

変更	説明	日付
iceRolePolicy - 新しいポリシー	ス の一環として他の を呼び出すアクセス許可を Incident Manager に付与する新しいポリシーを追加しました。	
AWSIncidentManagerServiceRolePolicy – ポリシーの更新	Incident Manager は、Incident Manager がアカウントにメトリクスを発行できるようにする新しいアクセス許可を追加しました。	2022 年 12 月 16 日
AWSIncidentManagerResolverAccess - 新しいポリシー	Incident Manager は、インシデントの開始、対応計画の一覧表示、インシデントの一覧表示、インシデントの更新、タイムラインイベントの一覧表示、カスタムタイムラインイベントの作成、カスタムタイムラインイベントの更新、カスタムタイムラインイベントの削除、関連アイテムの一覧表示、関連アイテムの作成、および関連アイテムの更新を可能にする新しいポリシーを追加しました。	2021 年 4 月 26 日

変更	説明	日付
AWSIncidentManagerServiceRolePolicy - 新しいポリシー	Incident Manager は、インシデントの一覧表示、タイムラインイベントの作成、 の作成、 への関連アイテムの OpsItems関連付け OpsItems、およびインシデントに関連するエンゲージメントの開始を行うためのアクセス許可を Incident Manager に付与する新しいポリシーを追加しました。	2021 年 4 月 26 日
Incident Manager が変更の追跡を開始	Incident Manager 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 4 月 26 日

AWS Systems Manager Incident Manager ID とアクセスのトラブルシューティング

次の情報は、Incident Manager と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

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

Incident Manager でアクションを実行する権限がない

「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ssm-incidents:*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: ssm-incidents:GetWidget on resource: my-example-widget
```

この場合、ssm-incidents:*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 Incident Manager にロールを渡せるようにする必要があります。

一部の AWS のサービス では、新しいサービスロール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。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Incident Manager でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。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 Amazon Web Services アカウント以外のユーザーに Incident Manager CodeCommit リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセス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:

- これらの機能を Incident Manager でサポートされるかどうかを確認するには、が IAM と AWS Systems Manager Incident Manager 連携する方法 を参照してください。
- 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認証されたユーザーへのアクセスの提供 (ID フェデレーション) 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。

Incident Manager での共有連絡先と対応計画の操作

問い合わせ共有では、問い合わせ所有者として、連絡先情報、エスカレーション計画、エンゲージメントを他の AWS アカウント または AWS 組織内で共有できます。連絡先とエスカレーション計画を一元的に作成および管理し、インシデント中にほかのユーザーが正しい連絡先をエンゲージできるようにすることができます。

対応計画の共有では、対応計画の所有者として、対応計画と関連するインシデントを他の AWS アカウント または AWS 組織内で共有できます。対応計画を一元的に作成および管理することで、コンシューマーアカウントのレスポンダーがインシデント発生時に対応できるようになります。

連絡先または対応計画の所有者は、連絡先と応答計画を以下と共有できます。

- の組織 AWS アカウント 内外に固有 AWS Organizations
- の組織内の組織単位 AWS Organizations
- の組織全体 AWS Organizations

内容

- 連絡先と対応計画を共有するための前提条件
- 関連サービス
- 連絡先または対応計画を共有する
- 共有連絡先または対応計画の共有を停止する
- 共有連絡先または対応計画を特定する
- 連絡先と対応計画の共有許可
- 請求と使用量測定
- インスタンス制限

連絡先と対応計画を共有するための前提条件

AWS Organizationsの組織または組織単位で連絡先または対応計画を共有する

- のリソースを所有している必要があります AWS アカウント。既に共有している連絡先または対応計画を共有することはできません。
- との共有を有効にする必要があります AWS Organizations。詳細については、AWS RAM ユーザーガイドの「Enable Sharing with AWS Organizations」を参照してください。

関連サービス

問い合わせと対応計画の共有は AWS Resource Access Manager () と統合されますAWS RAM。では AWS RAM、 AWS リソースを AWS アカウント または を通じて共有できます AWS Organizations。リソース共有を作成することで、自身が所有するリソースを共有できます。リソース共有は、共有するリソースと、それらを共有するコンシューマーを指定します。コンシューマーは、個々の AWS アカウント、組織単位、または 内の組織全体にすることができます AWS Organizations。

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

連絡先または対応計画を共有する

対応計画を共有すると、コンシューマーは、その応答計画を使用して作成された過去、現在、および将来のすべてのインシデントにアクセスできます。

連絡先を共有すると、コンシューマーは、インシデント中に発生する連絡先情報、エンゲージメント計画、エスカレーション計画、およびエンゲージメントにアクセスできます。消費者は、インシデント中に連絡先またはエスカレーション計画に参加することもできます。

自分が の組織に属 AWS Organizations していて、組織内での共有が有効になっている場合、組織内のコンシューマーには共有連絡先または対応計画へのアクセス許可が自動的に付与されます。これに該当しない場合、コンシューマーはリソースへの参加の招待を受け取り、その招待を受け入れた後で、共有された連絡先または対応計画に対するアクセス許可が付与されます。

AWS RAM コンソールまたは を使用して、所有している連絡先または対応計画を共有できます AWS CLI。

AWS RAM コンソールを使用して、所有している連絡先または対応計画を共有するには

「AWS RAM ユーザーガイド 」の「リソース共有の作成」を参照してください。

を使用して、所有している連絡先または対応計画を共有するには AWS CLI

create-resource-share コマンドを使用します。

共有連絡先または対応計画の共有を停止する

リソース所有者がコンシューマーとの連絡先または対応計画の共有を停止すると、連絡先、対応計画、エスカレーション計画、エンゲージメント、およびインシデントがコンシューマーのコンソールに表示されなくなります。

> **Note**
>
> コンシューマーがコンソールで連絡先、対応計画、エスカレーション計画、エンゲージメント、またはインシデントを表示している場合、ページを更新するか、ページから移動するまで、更新されずに表示され続けます。

自身が所有している連絡先または対応計画の共有を停止するには、リソースの共有から削除する必要があります。これを行うには、 AWS RAM コンソールまたは を使用します AWS CLI。

AWS RAM コンソールを使用して、自身が所有する共有連絡先または対応計画の共有を停止する

「AWS RAM ユーザーガイド」の「リソース共有の更新」を参照してください。

AWS CLIで所有している共有連絡先または対応計画の共有を停止する

disassociate-resource-share コマンドを使用します。

共有連絡先または対応計画を特定する

所有者とコンシューマーは、Incident Manager コンソールおよび AWS CLIを使用して、共有連絡先と対応計画を特定できます。

Incident Manager コンソールを使用して共有連絡先または対応計画を特定する

> **Note**
>
> 連絡先、対応計画、エスカレーション計画、エンゲージメント、およびインシデントは、通常、Incident Manager コンソールで共有リソースとして特定できません。Amazon リソースネーム (ARN) が表示されている場所では、ARN に所有者のアカウント ID が表示されます。

を使用して共有連絡先または対応計画を特定するには AWS CLI

ListResponseプランまたはListContactsコマンドを使用します。このコマンドは、自身が所有している連絡先と対応計画、共有連絡先と応答計画を返します。ARN は、問い合わせまたは対応計画の所有者の AWS アカウント ID を示します。

連絡先と対応計画の共有許可

所有者のアクセス許可

所有者は、連絡先と対応計画の更新、表示、共有、共有停止、使用ができます。連絡先と対応計画には、関連するエンゲージメントとインシデントが含まれます。

コンシューマーのアクセス許可

コンシューマーは、対応計画と連絡先のみを使用および表示できます。連絡先と対応計画には、関連するエンゲージメントとインシデントが含まれます。

請求と使用量測定

リソースの所有者は、リソースの料金を請求されます。コンシューマーは、共有リソースの料金を請求されません。リソースの共有に関連する追加コストは発生しません。

インスタンス制限

リソースを共有しても、所有者またはコンシューマーのアカウントのリソースの制限には影響しません。リソースの制限の計算には、所有者のアカウントのみが使用されます。

のコンプライアンス検証 AWS Systems Manager Incident Manager

サードパーティーの監査者は、複数の コンプライアンスプログラム AWS Systems Manager Incident Manager の一環として のセキュリティと AWS コンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

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。 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 AWS のサービス 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。

の耐障害性 AWS Systems Manager Incident Manager

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョンとアベイラビリティーゾーンの詳細については、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。

Incident Manager はグローバルリージョナルサービスであり、現在、アベイラビリティーゾーンをサポートしていません。

Incident Manager には、 AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズをサポートするのに役立つ機能がいくつか用意されています。準備ウィザード中

は、レプリケーションセットのセットアップを求められます。このリージョナルレプリケーションセットは、複数のリージョンからデータとリソースにアクセスできるようにし、クラウドネットワーク全体のインシデント管理をより容易にします。また、このレプリケーションにより、リージョンのいずれかがダウンした場合でも、データの安全性とアクセス性が確保されます。

Incident Manager レプリケーションセットの使用の詳細については、「Incident Manager レプリケーションセットの使用」を参照してください。

のインフラストラクチャセキュリティ AWS Systems Manager Incident Manager

マネージドサービスである AWS Systems Manager Incident Manager は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS 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、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開した API コールを使用して、ネットワーク経由で Incident Manager にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token 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 Systems Manager Incident Manager およびインターフェイス VPC エンドポイントの操作 (AWS PrivateLink)

インターフェイス VPC エンドポイント を作成 AWS Systems Manager Incident Manager することで、VPC と の間にプライベート接続を確立できます。インターフェイスエンドポイントは を使用します AWS PrivateLinkを使用すると AWS PrivateLink、インターネットゲートウェイ、NAT デバ

イス、VPN 接続、または AWS Direct Connect 接続なしで Incident Manager API オペレーションにプライベートにアクセスできます。VPC 内のインスタンスは、パブリック IP アドレスがなくても Incident Manager API と通信できます。VPC と Incident Manager の間のトラフィックは、Amazon ネットワーク内にとどまります。

各インターフェースエンドポイントは、サブネット内の 1 つ以上の Elastic Network Interface によって表されます。

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイス VPC エンドポイント (AWS PrivateLink) 」を参照してください。

Incident Manager VPC エンドポイントに関する考慮事項

Incident Manager のインターフェイス VPC エンドポイントを設定する前に、「Amazon VPC ユーザーガイド」の「Interface endpoint properties and limitations」および「AWS PrivateLink のクォータ」を確認してください。

Incident Manager は、VPC からのすべての API アクションの呼び出しをサポートしています。Incident Manager のすべてを使用するには、`ssm-incidents` および `ssm-contacts` それぞれに 1 つの VPC エンドポイントを作成する必要があります。

Incident Manager 用のインターフェイス VPC エンドポイントの作成

Incident Manager 用の VPC エンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface (AWS CLI) で作成できます。詳細については、 Amazon VPC ユーザーガイド のインターフェイスエンドポイントの作成を参照してください。

Incident Manager 用の VPC エンドポイントは、以下のサービス名を使用して作成します。

- `com.amazonaws.region.ssm-incidents`
- `com.amazonaws.region.ssm-contacts`

エンドポイントのプライベート DNS を使用すると、リージョンのデフォルト DNS 名を使用して、Incident Manager に API リクエストを実行できます。例えば、`ssm-incidents.us-east-1.amazonaws.com` または `ssm-contacts.us-east-1.amazonaws.com` という名前を使用できます。

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントを介したサービスへのアクセス」を参照してください。

Incident Manager 用の VPC エンドポイントの作成

Incident Manager へのアクセスをコントロールする VPC エンドポイントには、エンドポイントポリシーをアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。
- これらのアクションを実行できるリソース。

詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントでサービスへのアクセスを制御する」を参照してください。

例: Incident Manager アクション用の VPC エンドポイントポリシー

以下は、Incident Manager 用のエンドポイントポリシーの例です。このポリシーは、エンドポイントにアタッチされると、すべてのリソースのすべてのプリンシパルに対して、リストされている Incident Manager アクションへのアクセスを許可します。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "ssm-contacts:ListContacts",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:StartIncident"
         ],
         "Resource":"*"
      }
   ]
}
```

Incident Manager での設定と脆弱性の分析

設定と IT コントロールは、 AWS とお客様の間の責任共有です。詳細については、 AWS 「 責任共有モデル」を参照してください。

におけるセキュリティのベストプラクティス AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager には、独自のセキュリティポリシーを開発および実装する際に考慮すべき多くのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを提供するものではありません。これらのベストプラクティスはお客様の環境に必ずしも適切または十分でない可能性があるため、処方箋ではなく、あくまで有用な検討事項とお考えください。

トピック

- Incident Manager の予防的セキュリティのベストプラクティス
- Incident Manager の検出に関するセキュリティのベストプラクティス

Incident Manager の予防的セキュリティのベストプラクティス

最小特権アクセスの実装

アクセス許可を付与する場合、どのユーザーにどの Incident Manager リソースに対するアクセス許可を付与するかは、お客様が決定します。つまり、該当リソースに対して許可する特定のアクションを有効にするということです。このため、タスクを実行するために必要な許可のみを付与します。最小限の特権アクセスの実装は、セキュリティリスクはもちろん、エラーや悪意ある行動によってもたらされる可能性のある影響を減らす上での基本となります。

以下のツールは、最小限の特権アクセスを実装するために使用できます。

- IAM エンティティのポリシーとアクセス許可の境界を使用した AWS リソースへのアクセスの制御
- サービスコントロールポリシー

連絡先の作成と管理

連絡先をアクティベーションするとき、Incident Manager はデバイスに連絡してアクティベーションを確認します。デバイスをアクティベーションする前に、デバイス情報が正しいことを確認してください。これにより、アクティベーション中に Incident Manager が間違ったデバイスまたは人に接触する可能性が軽減されます。

連絡先とエスカレーション計画を定期的に確認して、インシデント中に連絡が必要な連絡先のみに連絡していることを確認します。連絡先を定期的に確認して、古い情報または誤った情報を削除しま

す。インシデントの発生時に連絡先に通知する必要がない場合は、関連するエスカレーション計画から削除するか、Incident Manager から削除します。

チャットチャネルを非公開にする

インシデントチャットチャネルをプライベートにすると、最小特権アクセスを実装できます。対応計画テンプレートごとに、スコープダウンユーザー・リストを持つ別のチャットチャネルを使用することを検討してください。これにより、機密情報を含む可能性のあるチャットチャネルに、適切な応答者のみを引き込むことができます。

AWS Chatbot が有効な Slack チャネルは、 の設定に使用される IAM ロールのアクセス許可を継承します AWS Chatbot。これにより、 AWS Chatbot 有効な Slack チャネルの応答者は、Incident Manager APIs やメトリクスグラフの取得など、許可リストに登録されたアクションを呼び出すことができます。

AWS ツールを最新の状態に保つ

AWS は、 AWS オペレーションで使用できるツールとプラグインの更新バージョンを定期的にリリースします。これらのリソースを最新の状態に保つことで、アカウントのユーザーとインスタンスが、これらのツールの最新の機能やセキュリティ機能にアクセスできます。

- AWS CLI – AWS Command Line Interface （ AWS CLI) は、コマンドラインシェルのコマンドを使用して AWS サービスとやり取りできるオープンソースツールです。 AWS CLIを更新するには、 AWS CLIのインストールに使用したコマンドと同じコマンドを実行します。オペレーティングシステムに適したコマンドを実行するために、少なくとも 2 週間に 1 回ローカルマシンでスケジュールされたタスクを作成することをお勧めします。インストールコマンドの詳細については、AWS 「 コマンドラインインターフェイスユーザーガイド」のAWS 「 コマンドラインインターフェイスのインストール」を参照してください。
- AWS Tools for Windows PowerShell – Tools for Windows PowerShell は、 AWS SDK for .NET によって公開される機能に基づいて構築された PowerShell モジュールのセットです。Tools for Windows PowerShell を使用すると、 PowerShell コマンドラインから AWS リソースに対するオペレーションをスクリプト化できます。Tools for Windows の更新バージョン PowerShell がリリースされたら、ローカルで実行しているバージョンを定期的に更新する必要があります。詳細については、「Windows AWS Tools for Windows PowerShell での の更新」または「Linux または macOS AWS Tools for Windows PowerShell での の更新」を参照してください。

関連情報

Systems Manager のセキュリティのベストプラクティス

Incident Manager の検出に関するセキュリティのベストプラクティス

Incident Manager のすべてのリソースの特定と監査

IT アセットの特定はガバナンスとセキュリティの重要な側面です。セキュリティ体制を評価し、潜在的な弱点に対処するには、すべての Systems Manager リソースを特定します。Incident Manager リソースのResource Groupsを作成します。詳細については、「AWS Resource Groups ユーザーガイド」の「 リソースグループとは」を参照してください。

を使用する AWS CloudTrail

AWS CloudTrail は、Incident Manager 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します。で収集された情報を使用して AWS CloudTrail、Incident Manager に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「AWS CloudTrail を使用した Incident Manager API コールのログ記録」を参照してください。

AWS セキュリティアドバイザリのモニタリング

Trusted Advisor に投稿されている のセキュリティアドバイザリを定期的にチェックします AWS アカウント。これは、describe-trusted-advisor-checks を使用してプログラムにより行うことができます。

さらに、各 に登録されている主要な E メールアドレスを積極的にモニタリングします AWS アカウント。 AWS は、この E メールアドレスを使用して、ユーザーに影響を与える可能性のある新たなセキュリティ問題について連絡します。

AWS 広範な影響を伴う運用上の問題は、AWS Service Health Dashboard に投稿されます。運用上の問題も、 AWS Health Dashboardを通じて個々のアカウントに投稿されます。詳細については、「AWS Health ドキュメント」を参照してください。

関連情報

アマゾン ウェブ サービス: セキュリティプロセスの概要 (ホワイトペーパー)

開始方法: リソースを設定する AWS 際のセキュリティのベストプラクティスに従う (AWS セキュリティブログ)

IAM ベストプラクティス

のセキュリティのベストプラクティス AWS CloudTrail

Incident Manager でのログ記録とモニタリング

AWS Systems Manager Incident Manager は、モニタリングおよびログ記録機能を提供する以下のサービスと統合されます。

CloudWatch メトリクス

CloudWatch メトリクスを使用して、AWS Systems Manager Incident Manager のオペレーションのデータポイントに関する統計を、メトリクスと呼ばれる順序付けられた一連の時系列データとして取得できます。これらのメトリクスを使用して、システムが正常に実行されていることを確認できます。詳細については、「Incident Manager の Amazon CloudWatch メトリクス」を参照してください。

CloudTrail ログ

AWS CloudTrail を使用して、AWS API に対して実行された呼び出しに関する詳細情報をキャプチャします。これらの呼び出しは Amazon Simple Storage Service にログファイルとして保存できます。これらの CloudTrail ログを使用して、行われた呼び出し、呼び出し元のソース IP アドレス、呼び出し元、呼び出し時間などの情報を判断できます。CloudTrail ログには、Incident Manager の API アクションの呼び出しに関する情報が含まれています。詳細については、「AWS CloudTrail を使用した Incident Manager API コールのログ記録」を参照してください。

Trusted Advisor

AWS Trusted Advisor は、AWS リソースのパフォーマンス、信頼性、セキュリティ、費用効率を向上するためのモニタリングに役立ちます。すべてのユーザーは、4 つの Trusted Advisor; チェックを利用できます。ビジネスまたはエンタープライズサポートプランのユーザーは、50 以上のチェックを利用できます。Incident Manager の場合、Trusted Advisor は、レプリケーションセットの設定がリージョンごとのフェイルオーバーおよびレスポンスをサポートするために複数の AWS リージョン を使用していることを確認します。詳細については、「AWS Support ユーザーガイド」の 「AWS Trusted Advisor」を参照してください。

Incident Manager の Amazon CloudWatch メトリクス

Incident Manager は、Amazon CloudWatch でモニタリングできる集計メトリクスを提供します。これらのメトリックスを使用して、インシデントと対応計画のトレンドを特定できます。

これらのメトリクスには、以下が含まれます。

- 一定期間に作成されたインシデント数

- これらのインシデントへの対応と解決の所要時間
- 解決されたインシデント数

Incident Manager のメトリクスをモニタリングすることで、オペレーションの健全性に対する理解を深め、インシデント対応のオペレーショナルエクスペリエンスを高めるための有意義な行動を取ることができます。Incident Manager のメトリクスは、すべての Incident Manager のリージョンで利用できます。メトリクスは、Incident Manager へのオンボーディング時に、レプリケーションセットで指定したすべてのリージョンの Amazon CloudWatch で表示できます。インシデントに対するアクションが実行されたリージョンで公開されたメトリクスを表示できます。これらのメトリクスに対する追加料金はありません。

CloudWatch コンソールでは、これらのメトリックを表示するダッシュボードを作成し、次の目的で使用できます。

- 既存のインシデントの負荷を測定および確認する
- インシデントの負荷が増えているのか、減少しているのか、変わらないのかを追跡する
- Incident Manager をより効果的に使用して、インシデントの頻度、期間、影響を軽減する

このページでは、CloudWatch コンソールで使用できる Incident Manager のメトリクスについて説明します。

> **Important**
>
> カスタマー生成イベントの場合、`TriggerDetails` のソース値に ASCII 以外の文字を使用して名前が付けられていると、イベントのメトリクスは、ASCII 以外のテキストをサポートしていない Amazon CloudWatch メトリクスでは報告されません。`source` は、SDK や AWS CLI を使用するなどして、プログラムでのみ提供できます。

Incident Manager は、次のメトリクスを CloudWatch に送信します。

メトリクス	説明
`NumberOfCreateIncidents`	作成されたインシデント数。 有効なディメンション: [](空のディメンション)、[ResponsePlan]、[Impact]、[Source]、

メトリクス	説明
	[ResponsePlan , Impact]、[ResponsePlan , Source] 単位: 個
NumberOfResolveIncidents	解決されたインシデント数。 有効なディメンション: [](空のディメンション)、[ResponsePlan]、[Impact]、[Source]、[ResponsePlan , Impact]、[ResponsePlan , Source] 単位: 個
TimeToFirstAcknowledgement	インシデント作成時刻とインシデントに対する最初の承諾が行われた時刻との時間差。 有効なディメンション: [](空のディメンション)、[ResponsePlan]、[Impact]、[Source]、[ResponsePlan , Impact]、[ResponsePlan , Source] 単位: 秒
TimeToResolveIncident	インシデントが作成された時点と解決された時点の時間差。 有効なディメンション:](空のディメンション)、[ResponsePlan]、[Impact]、[Source]、[ResponsePlan , Impact]、[ResponsePlan , Source] 単位: 秒

CloudWatch コンソールでの Incident Manager のメトリクスの表示

CloudWatch コンソールで Incident Manager のメトリクスを表示するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで [Metrics] (メトリクス) を選択します。
3. `IncidentManager` 名前空間を選択します。
4. [メトリクス] タブで、ディメンションを選択し、メトリクスを選択します。

CloudWatch メトリクスの使用の詳細については、Amazon CloudWatch ユーザーガイドの以下のトピックを参照してください。

- メトリクス
- Amazon CloudWatch メトリクスを使用する

メトリクスのディメンション

Incident Manager のメトリクスは、`IncidentManager` 名前空間を使用し、以下のディメンションのメトリクスを提供します。

ディメンション	説明
`By Response Plan`	対応計画ごとに集計メトリクスを表示します。
`By Impact Level`	重大度レベルごとに集計メトリクスを表示します。
`By Source`	手動、CloudWatch アラーム、または EventBridge イベントで作成されたインシデントのメトリクスを表示します。
`Across All Incidents`	現在の AWS リージョン内のすべてのインシデントの集計メトリクスを表示します。
`Response Plan name and Source`	対応計画とソースの組み合わせごとの集計メトリクスを表示します。

ディメンション	説明
`Response Plan Name and Impact Level`	対応計画と重大度レベルの組み合わせごとの集計メトリクスを表示します。

AWS CloudTrail を使用した Incident Manager API コールのログ記録

AWS Systems Manager Incident Manager は、Incident Manager でユーザー、ロール、または AWS サービスが行っ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、Incident Manager のすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、Incident Manager コンソールからの呼び出しと Incident Manager API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Incident Manager のイベントを含む Amazon S3 バケットへの CloudTrail イベントの継続的な 配信を有効にすることができます。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、Incident Manager に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

CloudTrail での Incident Manager 情報

CloudTrail は、アカウント作成時に AWS アカウント で有効になります。Incident Manager でアクティビティが発生すると、そのアクティビティは [イベント履歴] 内の他の AWS のサービスのイベントと共に CloudTrail イベントに記録されます。最近のイベントは、AWS アカウント で表示、検索、ダウンロードできます。詳細については、 CloudTrail イベント履歴でのイベントの表示を参照してください。

AWS アカウント のイベント (Incident Manager のイベントなど) を継続的に記録するには、証跡を作成します。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 AWS リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、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。

- 「追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

CloudTrail は、Incident Manager のすべてのアクションをログに記録し、Incident Manager は、すべてのアクションを AWS Systems Manager Incident ManagerAPI リファレンスに記録します。例えば、`CreateResponsePlan`、`ActivateDevice`、`StartIncident` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

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

Incident Manager のログファイルエントリについて

「トレイル」は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できます。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。

次の例は、`StartIncident` アクションを示す CloudTrail ログエントリです。

```
 {
"eventVersion": "1.08",
"userIdentity": {
    "type": "IAMUser",
    "principalId": "1234567890abcdef0",
```

```
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2021-04-22T23:20:10Z",
    "eventSource": "gamma-ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/
ssmincidents.start-incident",
    "requestParameters": {
        "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-
test-response-plan-non-dedupe-v1",
        "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
    "responseElements": {
        "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/
security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```

次の例は、DeleteContactChannelアクションを示す CloudTrail ログエントリです。

```
    {
    "eventVersion":"1.08",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"1234567890abcdef0",
        "arn":"arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId":"abcdef01234567890",
        "accessKeyId":"021345abcdef6789",
        "userName":"nikki_wolf"
    },
    "eventTime":"2021-04-08T02:27:21Z",
```

```
    "eventSource":"ssm-contacts.amazonaws.com",
    "eventName":"DeleteContactChannel",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
    "requestParameters":{
        "contactChannelId":"arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
    },
    "responseElements":null,
    "requestID":"abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID":"12345678-1234-1234-abcd-abcdef1234567",
    "readOnly":true,
    "eventType":"AwsApiCall",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"12345678901234567"
}
```

「Product and service integrations with Incident Manager」

の一機能である Incident Manager は AWS Systems Manager、以下の 製品、サービス、ツールと統合されています。

との統合 AWS のサービス

Incident Manager は、次の表で説明されている AWS のサービス および ツールと統合されています。

AWS CDK	AWS CDK は、コードを使用してクラウドインフラストラクチャを定義し、プロビジョニング AWS CloudFormation に を使用するための開発フレームワークです。は、 TypeScript、JavaScript、、Python、C#/ などJava、複数のプログラミング言語 AWS CDK をサポートしています。Net。 Incident Manager AWS CDK で を使用する方法については、 AWS CDK API リファレンスの以下のセクションを参照してください。 • @aws-cdk/aws-ssmincidents モジュール • @aws-cdk/aws-ssmcontacts モジュール
AWS Chatbot	AWS Chatbot により、 DevOps とソフトウェア開発チームはメッセージングプログラムのチャットルームを使用して、 内の運用イベントをモニタリングして対応できます AWS クラウド。 Incident Manager AWS Chatbot で を使用すると、応答者がインシデントのモニタリングと対応に使用できるチャットチャネルを作成できます。 AWS Chatbot はSlackチャットルーム、Microsoft Teamsチャネル、Amazon

	Chime チャットルームをチャットチャネルとしてサポートしています。 チャットチャネルの作成の一環として、Amazon Simple Notification Service (Amazon SNS) にトピックも作成します。Amazon SNS は、パブリッシャーからサブスクライバーへのメッセージ配信を提供するマネージド型サービスです。インシデント対応計画では、作成したチャットチャネルを計画に関連付けるときに、そのチャットチャネルに関連付けた 1 つ以上のトピックも選択します。これらの SNS トピックは、インシデントに関する通知をインシデント応答者に送信するために使用されます。 詳細については、「Incident Manager でのチャットチャネルの操作」を参照してください。
AWS CloudFormation	AWS CloudFormation は、アプリケーションに必要なすべてのリソースを含むテンプレートを作成し、リソースを設定してプロビジョニングするために使用できるサービスです。このサービスによってすべての依存関係も設定されるため、リソースの管理よりもアプリケーションに集中することができます。 Incident Manager AWS CloudFormation で を使用する方法については、AWS CloudFormation 「 ユーザーガイド」の以下のトピックを参照してください。 • 「Incident Manager resource type reference」 • 「Contacts resource type reference resource type reference」

Amazon CloudWatch	CloudWatch は、 AWS リソースと AWS で実行しているアプリケーションをリアルタイムでモニタリングします。 CloudWatch を使用してメトリクスを収集および追跡できます。メトリクスとは、リソースやアプリケーションに関して測定できる変数です。 Incident Manager. CloudWatch works でインシデントを作成する CloudWatch アラームを Systems Manager および Incident Manager で設定して、アラームがアラーム状態になったときに対応計画テンプレートからインシデントを作成できます。 詳細については、「CloudWatch アラームでインシデントを自動的に作成する」を参照してください。
Amazon Chime	Amazon Chime は、会議、チャット、ビジネス通話機能を兼ね備えたオンラインワークプレイスです。Amazon Chime を使用すると、組織の内外を問わず、会議とチャットを行ったり、仕事の電話をかけたりできます。 AWS Chatbot に Amazon Chime 用のチャットチャネルを作成し、そのチャネルを対応計画に追加することで、Amazon Chime ルームを Incident Manager オペレーションに統合できます。 詳細については、「Incident Manager でのチャットチャネルの操作」を参照してください。

Amazon EventBridge	EventBridge は、イベントを使用してアプリケーションコンポーネントを接続するサーバーレスサービスです。これにより、スケーラブルなイベント駆動型アプリケーションを簡単に構築できます。 定義したパターンにイベントが一致したときに、 AWS リソース内のイベントパターンを監視し、Incident Manager でインシデントを作成するように EventBridge ルールを設定できます。ルールでは、数十の AWS のサービス およびサードパーティのアプリケーションやサービスのイベントパターンをモニタリングできます。 詳細については、「EventBridge イベントでインシデントを自動的に作成する」を参照してください。
AWS Secrets Manager	Secrets Manager を使用することで、データベース認証情報、アプリケーション認証情報、OAuth トークン、API キー、およびその他のシークレットをライフサイクルを通じて管理、取得、ローテーションすることができます。 Incident Manager を PagerDuty サービスと統合するときは、 PagerDuty 認証情報を含むシークレットを Secrets Manager に作成します。 詳細については、「 PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存する」を参照してください。

AWS Systems Manager	Systems Manager は、アプリケーションインフラストラクチャとクラウド環境向けの安全な end-to-end 管理ソリューションを表示および制御するために使用できるオペレーションハブです。以下の Systems Manager の機能は Incident Manager と直接統合します。 • オートメーション – オートメーションランブックは、 AWS リソースで Systems Manager が実行するアクションを定義します。Incident Manager では、ランブックはインシデントを解決するために使用する一連の自動および手動の手順を定義します。 Incident Manager で使用するためのオートメーションランブックの作成については、「Incident Manager での Systems Manager Automation ランブックの操作」を参照してください。 • OpsCenter - オペレーションエンジニアや IT プロフェッショナルが と呼ばれる AWS リソースOpsItemsに関連する運用作業項目を管理できる中心的な場所 OpsCenter を提供します。インシデント後分析から直接 を作成して OpsItems、関連する作業をフォローアップできます。 詳細については、「Incident Manager でのインシデント後分析の実行」を参照してください。

AWS Trusted Advisor	Trusted Advisor は、Basic または Developer サポートプランを持つ AWS お客様が利用できるツールです。 Trusted Advisor は、お客様の AWS 環境を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会があれば、レコメンデーションを作成します。 Incident Manager の場合、レプリケーションセットの設定でリージョン Trusted Advisor フェイルオーバーとレスポンス AWS リージョン をサポートするために複数の が使用されていることを確認します。

その他の製品やサービスとの統合

Incident Manager は、次の表で説明するサードパーティのサービスと統合するか、または併用することができます。

Jira Cloud	を使用すると AWS Service Management Connector、Incident Manager をサードパーティーのクラウドベースのワークフロープラットフォームである Jira Cloud (Atlassian) と統合できます。 Jira Cloud との統合を設定した後、Incident Manager で新しいインシデントを作成すると、統合によって Jira Cloud にもインシデントが作成されます。Incident Manager でインシデントを更新すると、これらの更新は Jira Cloud 内の対応するインシデントにも反映されます。Incident Manager または Jira Cloud のいずれかでインシデントを解決すると、設定に基づいて両方のサービスのインシデントが統合によって解決されます。

	詳細については、「 AWS Service Management Connector 管理者ガイド」の「Integrating AWS Systems Manager Incident Manager (Jira Cloud)」を参照してください。
Jira Service Management	を使用すると AWS Service Management Connector、Incident Manager をサードパーティーのクラウドベースのワークフロープラットフォームである Jira Service Management と統合できます。 Jira Service Management の統合を設定した後、Incident Manager で新しいインシデントを作成すると、統合によって Jira Service Management にもインシデントが作成されます。Incident Manager でインシデントを更新すると、これらの更新は Jira Service Management の対応するインシデントにも反映されます。Incident Manager または Jira Service Management のいずれかでインシデントを解決すると、設定に基づいて両方のサービスのインシデントが統合によって解決されます。 詳細については、「AWS Service Management Connector 管理者ガイド」の「Configuring Jira Service Management」を参照してください。

Microsoft Teams	Microsoft Teams は、チームメッセージング、音声/ビデオ会議、ファイル共有のためのクラウドベースのコラボレーションツールを提供します。 AWS Chatbot に Microsoft Team 用のチャットチャネルを作成し、そのチャネルを対応計画に追加することで、Microsoft Teams チャネルを Incident Manager のオペレーションに統合できます。 詳細については、「Incident Manager でのチャットチャネルの操作」を参照してください。

PagerDuty	PagerDuty は、ページングワークフローとエスカレーションポリシーをサポートするインシデント対応ツールです。 Incident Manager を と統合すると PagerDuty 、対応計画に PagerDuty サービスを追加できます。その後、Incident Manager で のインシデントが作成される PagerDuty たびに、対応するインシデントが に作成されます。のインシデントは、Incident Manager のものに加えて、そこで定義したページングワークフローとエスカレーションポリシー PagerDuty を使用します。PagerDuty は、Incident Manager からのタイムラインイベントをインシデントに関するメモとしてアタッチします。 Incident Manager を と統合するには PagerDuty 、まず PagerDuty 認証情報を含むシークレットを に AWS Secrets Manager 作成する必要があります。 PagerDuty REST API キーの追加、および のシークレットに必要なその他の詳細については AWS Secrets Manager、「」を参照してください PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存する。 Incident Manager の対応計画に PagerDuty アカウントから PagerDuty サービスを追加する方法については、トピック「」の「対応計画に PagerDuty サービスを統合する」の手順を参照してください対応計画の作成。

ServiceNow	を使用すると AWS Service Management Connector、Incident Manager をサードパーティーのクラウドベースのワークフロープラットフォームServiceNowである と統合できます。 との統合を設定した後 ServiceNow、Incident Manager で新しいインシデントを作成すると、統合によって ServiceNow にもインシデントが作成されます。Incident Manager でインシデントを更新すると、 の対応するインシデントにこれらの更新が加えられます ServiceNow。Incident Manager または のいずれかでインシデントを解決する場合 ServiceNow、統合は設定した設定に基づいて両方のサービスのインシデントを解決します。 詳細については、「 AWS Service Management Connector 管理者ガイドAWS Systems Manager Incident Manager 」の「 の統合 ServiceNow」を参照してください。
Slack	Slack は、チームメッセージング、音声/ビデオ会議、ファイル共有のためのクラウドベースのコラボレーションツールを提供します。 AWS Chatbot に Slack 用のチャットチャネルを作成し、そのチャネルを対応計画に追加することで、Slack チャネルを Incident Manager のオペレーションに統合できます。 詳細については、「Incident Manager でのチャットチャネルの操作」を参照してください。

Terraform	HashiCorp Terraform は、さまざまなクラウドサービスを管理するためのコマンドラインインターフェイス (CLI) ワークフローを提供するオープンソースの Infrastructure as Code (IaC) ソフトウェアツールです。Incident Manager では、Terraform を使用して以下の要素を管理またはプロビジョニングできます。 SSM Incident Manager 連絡先リソース • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssm Contacts_rotation SSM Contacts データソース • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssm Contacts_rotation SSM Incident Manager リソース • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan SSM Incident Manager データソース • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存する

対応計画 PagerDuty で との統合を有効にすると、Incident Manager は次の方法で と連携 PagerDuty します。

- Incident Manager は、Incident Manager で新しいインシデントを作成する PagerDuty と、対応するインシデントを に作成します。
- で作成したページングワークフローとエスカレーションポリシー PagerDuty は、 PagerDuty 環境で使用されます。ただし、Incident Manager は PagerDuty 設定をインポートしません。
- Incident Manager は、タイムラインイベントを、最大 2,000 件のメモまで PagerDuty、 のインシデントに対するメモとして発行します。
- Incident Manager で関連する PagerDuty インシデントを解決するときに、インシデントを自動的に解決するように選択できます。

Incident Manager を と統合するには PagerDuty、まず PagerDuty 認証情報 AWS Secrets Manager を含むシークレットを で作成する必要があります。これにより、Incident Manager はサービスと通信できます PagerDuty。その後、Incident Manager で作成した対応計画に PagerDuty サービスを含めることができます。

Secrets Manager で作成するこのシークレットには、適切な JSON 形式で以下が含まれている必要があります。

- PagerDuty アカウントの API キー。汎用アクセス REST API キーまたはユーザートークン REST API キーのいずれかを使用できます。
- PagerDuty サブドメインからの有効なユーザーの E メールアドレス。
- サブドメインをデプロイした PagerDuty サービスリージョン。

> **Note**
>
> PagerDuty サブドメイン内のすべてのサービスは、同じサービスリージョンにデプロイされます。

前提条件

Secrets Manager でシークレットを作成する前に、次の要件を満たしていることを確認してください。

KMS キー

作成したシークレットは、 AWS Key Management Service () で作成したカスタマーマネージドキーで暗号化する必要がありますAWS KMS。このキーは、 PagerDuty 認証情報を保存するシークレットを作成するときに指定します。

> **Important**
>
> Secrets Manager には、 を使用してシークレットを暗号化するオプションがありますが AWS マネージドキー、この暗号化モードはサポートされていません。

カスタマーマネージドキーは次の要件を満たしている必要があります。

- [キーのタイプ]: [対称] を選択します。
- [キーの使用法]: [暗号化および復号化] を選択します。
- リージョン: 対応計画を複数の にレプリケートする場合は AWS リージョン、必ずマルチリージョンキー を選択してください。

キーポリシー

対応計画を設定するユーザーには、キーのリソースベースのポリシーの `kms:GenerateDataKey` および `kms:Decrypt` に対するアクセス許可が必要です。`ssm-incidents.amazonaws.com` サービスプリンシパルには、キーのリソースベースポリシーの `kms:GenerateDataKey` および `kms:Decrypt` に対するアクセス許可が必要です。

次のポリシーは、これらのアクセス許可を示しています。各###############を独自の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow creator of response plan to use the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM_ARN_of_principal_creating_response_plan"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow Incident Manager to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm-incidents.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

新しいカスタマーマネージドキーの作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「Creating symmetric encryption KMS keys」を参照してください。 AWS KMS キーの詳細については、「 のAWS KMS 概念」を参照してください。

既存のカスタマーマネージドキーが上記の要件をすべて満たしている場合は、ポリシーを編集してこれらのアクセス許可を追加できます。カスタマーマネージドキーのポリシーの更新については、「AWS Key Management Service デベロッパーガイド」の「キーポリシーの変更」を参照してください。

> **Tip**
>
> 条件キーを指定してアクセスをさらに制限できます。例えば、次のポリシーでは、米国東部 (オハイオ) リージョン (us-east-2) でのみ Secrets Manager からのアクセスを許可します。

```
{
    "Sid": "Enable IM Permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
        }
    }
}
```

`GetSecretValue` アクセス許可

対応計画を作成する IAM アイデンティティ (ユーザー、ロール、またはグループ) には IAM アクセス許可 `secretsmanager:GetSecretValue` が必要です。

PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存するには

1. ユーザーガイドの「AWS Secrets Manager シークレットを作成する」のステップ 3a のステップに従います。 AWS Secrets Manager
2. ステップ 3bの [キーと値のペア] で、次の操作を行います。
   - [プレーンテキスト] タブを選択します。
   - ボックスのデフォルトの内容を以下の JSON 構造に置き換えます。

```
{
    "pagerDutyToken": "pagerduty-token",
    "pagerDutyServiceRegion": "pagerduty-region",
    "pagerDutyFromEmail": "pagerduty-email"
```

```
}
```

- 貼り付けた JSON サンプルで、*########*の値を次のように置き換えます。
  - *pagerduty-token* : PagerDuty アカウントの一般アクセス REST API キーまたはユーザートークン REST API キーの値。

    関連情報については、 PagerDuty ナレッジベース の「 API アクセスキー」を参照してください。
  - *pagerduty-region*: PagerDuty サブドメインをホストする PagerDuty データセンターのサービスリージョン。

    関連情報については、ナレッジPagerDuty ベース の「サービスリージョン」を参照してください。
  - *pagerduty-email*: PagerDuty サブドメインに属するユーザーの有効な E メールアドレス。

    関連情報については、 PagerDuty ナレッジベース の「ユーザーの管理」を参照してください。

  次の例は、必要な PagerDuty認証情報を含む完成した JSON シークレットを示しています。

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. ステップ 3c の [暗号化キー] で、前の「前提条件」セクションに記載されている要件を満たす、作成したカスタマーマネージドキーを選択します。
4. ステップ 4c の [リソースのアクセス許可] で、次の操作を行います。
   - [リソースのアクセス許可] を展開します。
   - [アクセス許可の編集] を選択します。
   - ポリシーボックスのデフォルトの内容を以下の JSON 構造に置き換えます。

```
{
    "Effect": "Allow",
```

```
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

- [保存] を選択します。

5. 対応計画を複数の AWS リージョン に複製した場合は、ステップ 4d の [シークレットをレプリケート] で次の操作を行います。
   - [シークレットをレプリケート] を展開します。
   - AWS リージョン で、対応計画を複製したリージョンを選択します。
   - [暗号化キー] には、「前提条件」セクションの下に記載されている要件を満たす、このリージョンで作成した、またはこのリージョンに複製したカスタマーマネージドキーを選択します。
   - 追加の ごとに AWS リージョン、リージョンの追加を選択し、リージョン名とカスタマーマネージドキーを選択します。
6. 「 ユーザーガイド」の「 AWS Secrets Manager シークレットを作成するAWS Secrets Manager 」の残りのステップを完了します。

Incident Manager インシデントワークフローに PagerDuty サービスを追加する方法については、「」トピックの PagerDuty 「サービスを対応計画に統合する」を参照してください対応計画の作成。

関連情報

PagerDuty と を使用してインシデント対応を自動化する方法 AWS Systems Manager Incident Manager (AWS クラウド 運用と移行ブログ)

「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager のシークレット暗号化と復号」

AWS Systems Manager Incident Manager のトラブルシューティング

AWS Systems Manager Incident Manager の使用中に問題が発生した場合は、以下の情報を使用し、ベストプラクティスに従って解決できます。発生した問題が以下の情報の範囲外である場合、または解決を試みた後にも持続する場合は、AWS Support にお問い合わせください。

トピック

- エラーメッセージ: ValidationException – We were unable to validate the AWS Secrets Manager secret
- その他の問題のトラブルシューティング

エラーメッセージ: `ValidationException – We were unable to validate the AWS Secrets Manager secret`

問題 1: 対応計画を作成した AWS Identity and Access Management (IAM) アイデンティティ (ユーザー、ロール、またはグループ) に `secretsmanager:GetSecretValue` IAM アクセス許可がありません。Secrets Manager のシークレットを検証するには、IAM アイデンティティにこのアクセス許可が必要です。

- 解決策: 対応計画を作成する IAM アイデンティティの IAM ポリシーに、不足している `secretsmanager:GetSecretValue` アクセス許可を追加します。詳細については、「IAM ユーザーガイド」の「IAM ID アクセス許可の追加 (コンソール)」または「IAM ポリシーの追加 (AWS CLI)」を参照してください。

問題 2: シークレットに IAM アイデンティティによる `GetSecretValue` アクションの実行を許可するリソースベースのポリシーがアタッチされていない、またはリソースベースのポリシーがアイデンティティへのアクセス許可を拒否しています。

- 解決策: `secrets:GetSecretValue` に IAM アイデンティティへのアクセス許可を付与する `Allow` ステートメントを作成するか、シークレットのリソースベースのポリシーに追加します。または、IAM アイデンティティを含む `Deny` ステートメントを使用する場合は、アイデンティティがアクションを実行できるようにポリシーを更新してください。詳細については、「AWS

Secrets Manager ユーザーガイド」の「アクセス許可ポリシーを AWS Secrets Manager シークレットにアタッチする」を参照してください。

問題 3: シークレットには、Incident Manager サービスプリンシパル (ssm-incidents.amazonaws.com) へのアクセスを許可するリソースベースのポリシーがアタッチされていません。

- 解決策: シークレットのリソースベースのポリシーを作成または更新し、以下のアクセス許可を含めます。

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

問題 4: シークレットを暗号化するために選択された AWS KMS key がカスタマーマネージドキーではない。または、選択されたカスタマーマネージドキーが Incident Manager サービスプリンシパルに対して IAM アクセス許可 (kms:Decrypt および kms:GenerateDataKey*) を付与していません。あるいは、対応計画を作成した IAM アイデンティティに IAM アクセス許可 (GetSecretValue) がない可能性があります。

- 解決策: トピック「 PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存する」の「Prerequisites」で説明されている要件を満たしていることを確認してください。

問題 5: 一般アクセス REST API キーまたはユーザートークン REST API キーを含むシークレットの ID が無効になっています。

- 解決策: 末尾にスペースを入れずに、Secrets Manager シークレットの ID を正確に入力したことを確認してください。使用するシークレットが保存されているのと同じ AWS リージョン で作業する必要があります。削除したシークレットは使用できません。

問題 6: まれに、Secrets Manager サービスに問題が発生したり、Incident Manager との通信に問題が発生したりすることがあります。

- 解決策: 数分後にもう一度お試しください。AWS Health Dashboard で、いずれかのサービスに影響する可能性のある問題がないか確認してください。

その他の問題のトラブルシューティング

上記の手順を実行しても問題が解決しない場合、追加のヘルプを以下のリソースで参照してください。

- Incident Manager コンソールにアクセスした際の Incident Manager 固有の IAM 問題については、「AWS Systems Manager Incident Manager ID 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。
- AWS Management Console にアクセスするときの一般的な認証および認可の問題については、「IAM ユーザーガイド」の「IAM のトラブルシューティング」を参照してください。

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

Incident Manager のドキュメント履歴

変更	説明	日付
マネージドポリシーの更新 AWSIncidentManagerIncidentAccessServiceRolePolicy	Incident Manager はAWSIncidentManagerIncidentAccessServiceRolePolicy 、検出結果機能をサポートする新しいアクセス許可を に追加しました。これにより、EC2 インスタンスが Auto Scaling グループの一部であるかどうかを確認できます。詳細については、「Incident Manager updates to AWS managed policies」を参照してください。	2024 年 2 月 20 日
その他の HashiCorp Terraform サポート: オンコールローテーション	Terraform は Incident Manager のサポートに を追加しました。Terraform を使用して Incident Manager オンコールリソースをプロビジョニングまたは管理できるようになりました。Incident Manager とのこの統合およびその他のサードパーティ統合については、「Integration with other products and services」を参照してください。	2024 年 2 月 21 日
新機能: 他の からの結果 AWS のサービス	検出結果から、Incident Manager でインシデントが作成されたのとほぼ同じ時間に発生した AWS	2023 年 11 月 15 日

CloudFormation スタックと AWS CodeDeploy デプロイに関連する変更に関する情報が得られます。Incident Manager コンソールでは、これらの変更に関する概要情報を表示でき、多くの場合、変更に関する詳細な情報については、 CloudFormation または CodeDeploy コンソールへのリンクにアクセスできます。検出結果により、インシデントの潜在的な原因の評価にかかる時間を短縮できます。また、対応者がインシデントの原因を調査するために間違ったアカウントやコンソールにアクセスする可能性も低くなります。この機能は、Incident Manager がインシデントに関連する結果 AWS のサービス を識別するために他の のリソースを読み取ることができる新しい マネージドポリシー `AWSIncidentManagerIncidentAccessServiceRolePolicy` も導入します。詳細については、次のトピックを参照してください。

- 結果を使用する
- AWS マネージドポリシー: AWSIncidentManagerIncidentAccessServiceRolePolicy

Incident Manager の統合に関するリストの更新	「Product and service integrations with Incident Manager」トピックが拡張され、Incident Manager と統合してインシデント検出および対応オペレーションで使用できるすべての AWS のサービス とサードパーティツールのリストと説明が追加されました。	2023 年 6 月 9 日

との統合 AWS Trusted Advisor	Trusted Advisor は、レプリケーションセットの設定がリージョンフェイルオーバーとレスポンス AWS リージョンをサポートするために複数のを使用することを確認するようになりました。アラームまたは EventBridge イベントによって CloudWatch作成されたインシデントの場合、Incident Manager はアラームまたはイベントルール AWS リージョン と同じ にインシデントを作成します。そのリージョンで Incident Manager が一時的に使用不能な場合、システムは、レプリケーションセット内にある別のリージョンにインシデントを作成しようとします。Incident Manager が使用不能で、レプリケーションセットに含まれるリージョンが 1 つだけの場合、システムはインシデントレコードの作成に失敗します。このような状況を回避するために、レプリケーションセットが 1 つのリージョンのみに設定されていると、 によって Trusted Advisor レポートされます。Trusted Advisor の詳細な操作方法については、「AWS Support ユーザーガイド」の「AWS Trusted Advisor」を参照してください。	2023 年 4 月 28 日

Microsoft Teams を対応計画のチャットチャネルとして使用	Microsoft Teams および との統合により AWS Chatbot、対応計画でチャットチャネルに Microsoft Teams を使用できるようになりました。この他に、Slack と Amazon Chime のチャットチャネルもサポートされています。インシデント中、Incident Manager は、ステータス通知をチャットチャネルに直接送信し、すべての応答者に情報を提供します。応答者は、Microsoft Teams アプリケーションで相互に通信したり、インシデント関連の AWS CLI コマンドとやり取りしたりすることもできます。詳細については、「Working with chat channels in Incident Manager」を参照してください。	2023 年 4 月 4 日

新機能: オンコールスケジュール	Incident Manager のオンコールスケジュールでは、オペレータの介入が必要なインシデントが発生した場合に通知するユーザーを定義します。オンコールスケジュールは、そのスケジュール用に作成する 1 つまたは複数のローテーションで構成されます。各ローテーションには、最大 30 個の連絡先を含めることができます。オンコールスケジュールを作成したら、エスカレーション計画にエスカレーションとして含めることができます。そのエスカレーション計画に関連するインシデントが発生すると、Incident Manager はスケジュールに従ってオンコールのオペレータに通知します。詳細については、「Working with on-call schedules in Incident Manager」を参照してください。	2023 年 3 月 28 日

フォーマット済みインシデント分析の印刷または PDF 形式での保存	インシデント分析ページに [印刷] ボタンが追加され、印刷用にフォーマット済みの分析を生成できるようになりました。デバイス用に設定されたプリンタ宛先を使用して、インシデント分析を PDF として保存したり、ローカルプリンタやネットワークプリンタに送信したりできます。詳細については、「Print a formatted incident analysis」を参照してください。	2023 年 1 月 17 日
PagerDuty 統合: Incident Manager がインシデントタイムラインイベントを PagerDutyインシデントにコピーするようになりました	対応計画 PagerDuty で との統合を有効にすると、Incident Manager は、その計画から作成されたタイムラインイベントを の対応するインシデントレコードに追加します PagerDuty。 PagerDuty は、インシデントに関するメモとしてタイムラインイベントを最大 2,000 件のメモに追加します。これらの変更事項の詳細については、次のトピックを参照してください。 • PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存する • PagerDuty サービスを対応計画に統合する	2022 年 12 月 15 日

Incident Manager と CloudWatch メトリクスの統合。	インシデント関連のメトリクスを で公開できるようになりました CloudWatch。詳細については、「CloudWatch メトリクス」を参照してください。には、サービス AWSIncidentManager ServiceRolePolicy がユーザーに代わってメトリクスを発行できるようにするための追加のアクセス許可が含まれています。	2022 年 12 月 15 日
インシデントのメモの提供開始とインシデント詳細画面の更新	インシデントのメモを使用して、インシデントに取り組む他のユーザーと共同作業したりやり取りしたりすることができます。また、インシデント詳細画面からランブックやエンゲージメントのステータスを表示できます。詳細については、「Incident Details」を参照してください。	2022 年 11 月 16 日

PagerDuty エスカレーション計画とページングワークフローを Incident Manager 対応計画に統合する	Incident Manager を と統合 PagerDuty し、対応計画に PagerDuty サービスを追加できるようになりました。統合を設定すると、Incident Manager は、Incident Manager で作成された新しいインシデント PagerDuty ごとに、 で対応するインシデントを作成できます。 は、 PagerDuty 環境で定義したページングワークフローとエスカレーションポリシー PagerDuty を使用します。 詳細については、次のトピックを参照してください。 • 「Product and service integrations with Incident Manager」 • PagerDuty アクセス認証情報を AWS Secrets Manager シークレットに保存する • トピックの対応計画に PagerDuty サービスを統合する 対応計画の作成 • トラブルシューティング	2022 年 11 月 16 日

インシデントのメモの提供開始とインシデント詳細画面の更新。	インシデントのメモを使用して、インシデントに取り組む他のユーザーと共同作業したりやり取りしたりすることができます。また、インシデント詳細画面からランブックやエンゲージメントのステータスを表示できます。詳細については、「Incident Details」を参照してください。	2022 年 11 月 16 日
レプリケーションセットのタグ付けサポート	AWS Systems Manager Incident Manager でレプリケーションセットにタグを割り当てられるようになりました。これにより、レプリケーションセットで AWS リージョン 指定された の対応計画、インシデントレコード、連絡先にタグを割り当てるための既存のサポートが追加されます。詳細については、以下のトピックを参照してください。 • 準備ウィザード • 「Tagging Incident Manager resources」	2022 年 11 月 2 日

Incident Manager と Atlassian Jira Service Management の統合	Incident Manager を Jira サービスマネジメントと統合するには、 AWS Service Management Connector for Jira Service Management を使用します。統合を設定すると、Incident Manager で作成された新しいインシデントは、対応するインシデントを Jira に作成します。Incident Manager でインシデントを更新すると、その更新が Jira の対応するインシデントに追加されます。Incident Manager または Jira でインシデントを解決すると、設定に基づいて、対応するインシデントも解決されます。詳細については、「AWS Service Management Connector Administrator Guide」の「Configuring Jira Service Management」を参照してください。	2022 年 10 月 6 日

タグ付けの拡張サポート	Incident Manager は、レプリケーションセットで AWS リージョン 指定された の対応計画、インシデントレコード、連絡先へのタグの割り当てをサポートします。Incident Manager は、対応計画から作成されたインシデントへのタグの自動割り当てもサポートしています。詳細については、「Tagging Incident Manager resources」を参照してください。	2022 年 6 月 28 日
Incident Manager と の統合 ServiceNow	Incident Manager は、AWS のサービス管理コネクタServiceNowを使用して と統合できます ServiceNow。統合を設定すると、Incident Manager で作成された新しいインシデントは、対応するインシデントを に作成します ServiceNow。Incident Manager でインシデントを更新すると、その更新は の対応するインシデントに追加されます ServiceNow。Incident Manager または のいずれかでインシデントを解決すると ServiceNow、設定された設定に基づいて、対応するインシデントも解決されます。詳細については、「 での AWS Systems Manager Incident Manager の統合 ServiceNow」を参照してください。	2022 年 6 月 9 日

連絡先情報のインポート	インシデントが作成されると、Incident Manager は音声通知または SMS 通知を使用して応答者に通知できます。呼び出しまたは SMS 通知が Incident Manager からのものであることを応答者に確認してもらうため、すべての応答者が Incident Manager の仮想カード形式 (.vcf) ファイルをモバイルデバイスのアドレス帳にダウンロードすることをお勧めします。詳細については、「Import contact details to your address book」を参照してください。	2022 年 5 月 18 日

インシデントの作成と修復を強化するための複数の機能強化	Incident Manager は、インシデントの作成と修復を強化するために、以下の機能が強化されました。 • 他の でインシデントを自動的に作成する AWS リージョン: Amazon CloudWatch または Amazon がインシデント EventBridge を作成 AWS リージョン したときに Incident Manager が で利用できない場合、これらのサービスはレプリケーションセットで指定された利用可能なリージョンのいずれかでインシデントを自動的に作成するようになりました。詳細については、「Cross-Region incident management」を参照してください。 • ランブックパラメータにインシデントメタデータ を自動的に入力する: インシデントから AWS リソースに関する情報を収集するように Incident Manager を設定できるようになりました。その後、Incident Manager は収集した情報をランブックパラメータに入力できます。詳細については、「Tutorial: Using Systems Manager Automation runbooks with	2022 年 5 月 17 日

	Incident Manager」を参照してください。 • AWS リソース情報を自動的に収集する: システムがインシデントを作成すると、Incident Manager はインシデントに関連する AWS リソースに関する情報を自動的に収集するようになりました。その後、Incident Manager はこの情報を [関連項目] タブに追加します。	
複数のランブックのサポート	Incident Manager は、インシデント中に、インシデント詳細ページで複数のランブックの実行をサポートするようになりました。	2022 年 1 月 14 日
Incident Manager が新しい で起動 AWS リージョン	Incident Manager は、次の新しいリージョンで利用できるようになりました: us-west-1、sa-east-1、ap-northeast-2、ap-south-1、ca-central-1、eu-west-2、eu-west-3。Incident Manager のリージョンとクォータの詳細については、「AWS 全般のリファレンス リファレンスガイド」を参照してください。	2021 年 11 月 8 日
コンソールエンゲージメントの確認	Incident Manager コンソールから直接エンゲージメントを承認できるようになりました。	2021 年 8 月 5 日

[プロパティ] タブ	Incident Manager はインシデントの詳細ページにプロパティタブを導入し、インシデント、親 OpsItem、および関連するインシデント後分析に関する詳細情報を提供します。	2021 年 8 月 3 日
Incident Manager の起動	Incident Manager は、 が AWS ホストするアプリケーションに影響を与えるインシデントをユーザーが緩和および回復できるように設計されたインシデント管理コンソールです。	2021 年 5 月 10 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。