aws

ユーザーガイド

Amazon DevOps Guru

Amazon DevOps Guru: ユーザーガイド

Table of Contents

Amazon DevOps Guru とは

Amazon DevOps Guru ユーザーガイドへようこそ。

DevOpsGuru は完全マネージド型の運用サービスで、開発者や運用者はアプリケーションのパフォーマンスと可用性を簡単に向上させることができます。 DevOpsGuru を使用すると、運用上の問題の特定に関連する管理タスクをオフロードして、アプリケーションを改善するための推奨事項を迅速に実装できます。 DevOpsGuru が作成する事後対応型のインサイトは、アプリケーションの改善に今すぐ活用できます。また、将来アプリケーションに影響を与える可能性のある運用上の問題を回避するために事前対応型インサイトを作成します。

DevOpsGuru は機械学習を適用して運用データやアプリケーションのメトリクスやイベントを分析し、通常の運用パターンから逸脱した動作を特定します。 DevOpsGuru が運用上の問題やリスクを検出すると、ユーザーに通知されます。 DevOpsGuruは、問題ごとに、現在およびfuture 予測される運用上の問題に対処するためのインテリジェントな推奨事項を提示します。

開始するには、「 DevOpsGuru を使い始めるにはどうすればいいですか?」を参照してください。

DevOpsGuru はどのように機能しますか?

DevOpsGuru ワークフローは、対象範囲と通知を設定するところから始まります。 DevOpsGuru を設定すると、運用データの分析が開始されます。異常な動作が検出されると、問題に関連するレコメンデーション、メトリクスのリスト、ロググループ、およびイベントを含むインサイトが作成されます。インサイトがあるたびに、 DevOps Guru から通知が届きます。有効にすると AWS Systems Manager OpsCenter、 OpsItem が作成されるので、Systems Manager OpsCenter を使用してインサイトを追跡および管理できます。各インサイトには、異常な動作に関連するレコメンデーション、メトリクス、ロググループが含まれます。インサイト内の情報を使用して、異常な動作を理解して対処することができます。

3 つの高レベルのワークフローステップの詳細については、「 DevOps高レベルの Guru ワークフロー」を参照してください。Guru AWS ワークフローが他のサービスとどのように相互作用するかなど、より詳細な DevOps Guru ワークフローについては、を参照してください DevOpsGuru の詳細なワークフロー。

トピック

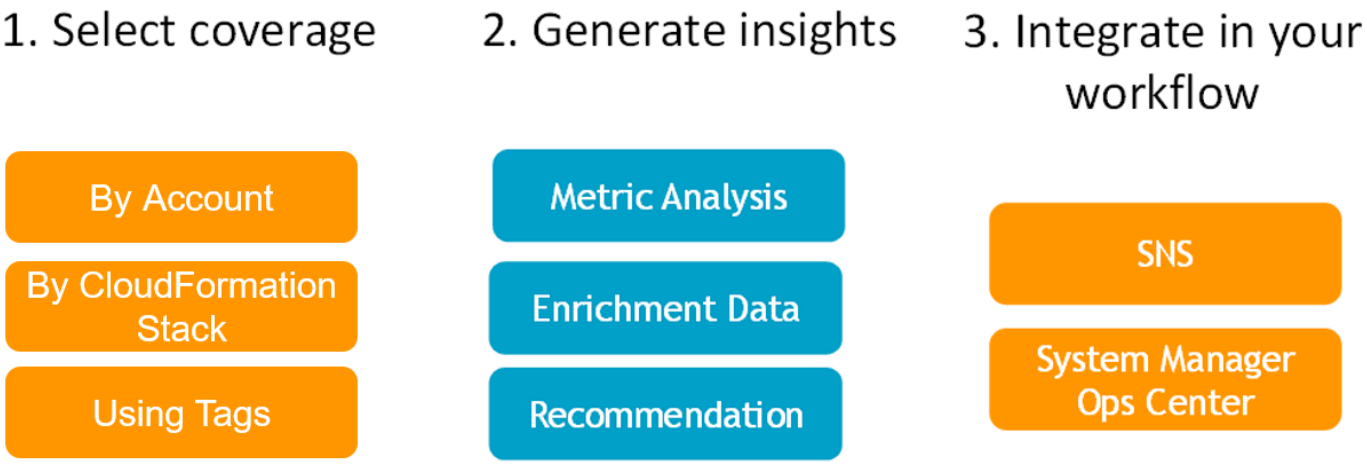
- DevOps高レベルの Guru ワークフロー
- DevOpsGuru の詳細なワークフロー

DevOps高レベルの Guru ワークフロー

Amazon DevOps Guru のワークフローは、大きく 3 つのステップに分けることができます。

1. AWS AWS アカウント内のどのリソースを分析したいかを指定して、 DevOps Guru の適用範囲を指定します。
2. DevOpsGuru は AWS CloudTrail、Amazon CloudWatch のメトリクスやその他の運用データの分析を開始して、修正して運用を改善できる問題を特定します。
3. DevOpsGuru は、重要な DevOps Guru イベントが発生するたびに通知を送信することで、ユーザーがインサイトや重要な情報を把握できるようにします。

OpsItem AWS Systems Manager OpsCenter インサイトの追跡に役立つ情報を作成するように DevOps Guru を設定することもできます。以下の図表に、この高レベルのワークフローを示します。



1. 最初のステップでは、 AWS AWS アカウント内のどのリソースを分析するかを指定してカバレッジを選択します。 DevOpsGuru AWS はアカウント内のすべてのリソースを対象または分析できます。また、 AWS CloudFormation AWS スタックやタグを使用してアカウント内のリソースのサブセットを指定して分析することもできます。指定したリソースがビジネスクリティカルなアプリケーション、ワークロード、およびマイクロサービスを構成していることを確認します。サポートされているサービスとリソースの詳細については、「Amazon DevOps Guru 料金表」を参照してください。
2. 2 番目のステップでは、 DevOps Guru はリソースを分析してインサイトを生成します。これは進行中のプロセスです。 DevOpsGuru コンソールでは、インサイトを表示したり、そこに含まれる

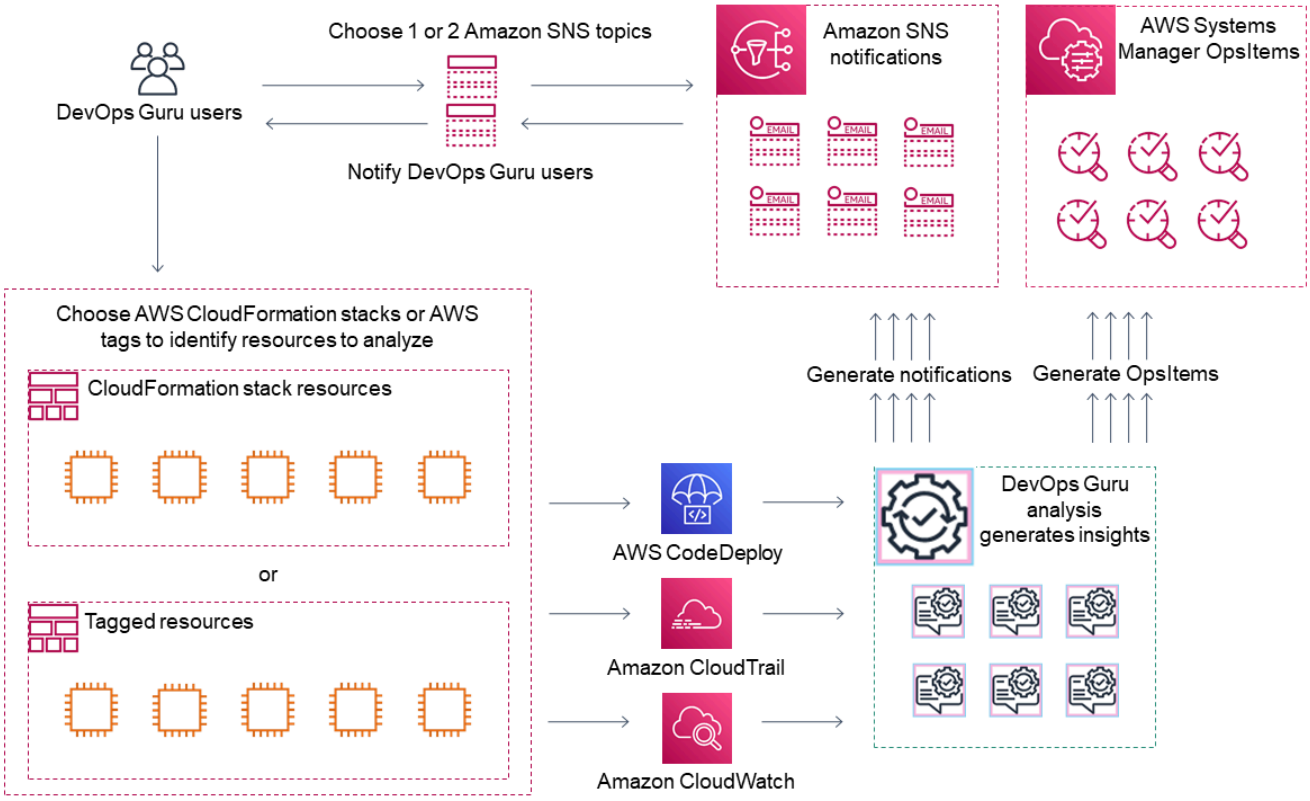
推奨事項や関連情報を確認したりできます。DevOpsGuru は以下のデータを分析して問題を見つけ、インサイトを作成します。

- AWS リソースから出力される個々の Amazon CloudWatch メトリックス。問題が特定されると、 DevOps Guru はそれらのメトリクスをまとめて収集します。
- Amazon CloudWatch ロググループから異常を記録します。ログ異常検出を有効にすると、DevOps Guru は問題が発生したときに関連するログ異常を表示します。
- DevOpsGuru AWS CloudTrail は管理ログからエンリッチメントデータを取得して、収集された指標に関連するイベントを見つけます。イベントは、リソースデプロイイベントと構成の変更です。
- を使用する場合 AWS CodeDeploy、 DevOps Guru はデプロイイベントを分析してインサイトを得るのに役立ちます。 CodeDeploy すべてのタイプのデプロイ (オンプレミスサーバー、Amazon EC2 サーバー、Lambda、または Amazon EC2) のイベントが分析されます。
- DevOpsGuru は特定のパターンを見つけると、特定された問題の軽減または修正に役立つ 1 つ以上の推奨事項を生成します。レコメンデーションは 1 つのインサイトに収集されます。インサイトには、問題に関連するメトリクスとイベントのリストも含まれています。インサイトデータを使用して、特定された問題を理解して対処します。

3. 3 番目のステップでは、 DevOps Guru がインサイト通知をワークフローに統合して、問題の管理と迅速な対処を支援します。
   - AWS アカウントで生成されたインサイトは、 DevOps Guru のセットアップ中に選択された Amazon Simple Notification Service (Amazon SNS) トピックに公開されます。これにより、インサイトが作成されるとすぐに通知されます。詳細については、「DevOps Guru の通知を更新する」を参照してください。
   - DevOpsGuru AWS Systems Manager のセットアップ時に有効にした場合、 OpsItem インサイトごとに対応する情報が作成され、発見された問題の追跡と管理に役立ちます。詳細については、「DevOps Guru での AWS Systems Manager 統合を更新する」を参照してください。

DevOpsGuru の詳細なワークフロー

DevOpsGuru ワークフローは、Amazon、Amazon AWS 簡易通知サービス CloudWatch AWS CloudTrail、などの複数のサービスと統合されています。 AWS Systems Manager次の図は、 AWS 他のサービスとの連携方法を含む詳細なワークフローを示しています。



この図は、 DevOps AWS AWS CloudFormation スタックで定義されたリソースやタグを使ってGuruの適用範囲を指定するシナリオを示しています。 AWS スタックやタグが選択されていない場合、DevOps Guru AWS カバレッジはアカウント内のすべてのリソースを分析します。詳細については、「AWS リソースを使用したアプリケーションの定義」および「DevOpsGuru のカバレッジを決定する」を参照してください。

1. セットアップ時に、インサイトが作成されたときなど、重要な DevOps Guru イベントに関する通知に使用される Amazon SNS トピックを 1 つまたは 2 つ指定します。次に、 AWS CloudFormation 分析したいリソースを定義するスタックを指定できます。また、Systems Manager OpsItem でインサイトごとにを生成できるようにして、インサイトを管理しやすくすることもできます。
2. 設定が完了すると、 DevOps Guru CloudWatch はメトリクス、ロググループ、リソースから生成されるイベント、 AWS CloudTrail メトリクスに関連するデータの分析を開始します。CloudWatch CodeDeploy 運用中にデプロイが含まれる場合、 DevOps Guru はデプロイイベントも分析します。

   DevOpsGuru は、分析されたデータから異常な動作を検出すると、インサイトを作成します。各インサイトには、1 つ以上のレコメンデーション、インサイトの生成に使用されるメトリクスの

リスト、ロググループに関するリスト、およびインサイトの生成に使用されるイベントのリストが含まれます。この情報を使用して、特定された問題に対処します。

3. インサイトが作成されるたびに、 DevOps Guru は DevOps Guru のセットアップ時に指定された 1 つまたは複数の Amazon SNS トピックを使用して通知を送信します。 DevOpsGuruがSystems Manager OpsItem でを生成できるようにした場合 OpsCenter、各インサイトは新しいSystems Manager OpsItem もトリガーします。Systems Manager を使用してインサイトを管理できます OpsItems。

DevOpsGuru を使い始めるにはどうすればいいですか?

次の手順を実行することをお勧めします。

1. DevOpsGuru の詳細については、の情報を読んでください。 DevOps Guru の概念
2. の手順に従って AWS CLI、 AWS アカウント、および管理ユーザーを設定します。Amazon DevOpsGuru のセットアップ
3. の指示に従って DevOps Guru を使用してください。 DevOpsGuru の開始方法

Guru DevOps の料金の発生を止めるにはどうすればいいですか ?

Amazon DevOps Guru を無効化して、 AWS アカウントとリージョンのリソース分析による課金が発生しないようにするには、リソースを分析しないようにカバレッジ設定を更新してください。その場合、「DevOps Guru でのAWS分析カバレッジの更新」のステップに従って、ステップ 4 で [None] (なし) を選択します。 DevOpsGuru AWS がリソースを分析するアカウントとリージョンごとに更新する必要があります。

> **Note**
>
> カバレッジを更新してリソースの分析を停止しても、過去に DevOps Guru が生成した既存のインサイトを確認すると、引き続き少額の料金が発生する可能性があります。この料金は、インサイト情報を取得および表示するために使用される API コールに関連付けられたものです。詳細については、Amazon DevOps Guru の料金表を参照してください。

DevOps Guru の概念

以下の概念は、Amazon DevOps Guru の仕組みを理解する際に重要です。

トピック

異常

異常とは、DevOps Guru によって検出された予期されない、または通常とは異なる関連メトリクスを表します。DevOps Guru は、AWS リソースに関連するメトリクスと運用データを分析する機械学習を使用して異常を生成します。Amazon DevOps Guru をセットアップするとき、分析する AWS リソースを指定します。詳細については、「Amazon DevOpsGuru のセットアップ」を参照してください。

インサイト

インサイトは、DevOps Guru をセットアップするときに指定した AWS リソースの分析時に作成される異常のコレクションです。各インサイトには、運用パフォーマンスを改善するために使用できる観測値、レコメンデーション、および分析データが含まれます。インサイトには 2 つのタイプがあります。

- 事後対応型: 事後対応型インサイトは、異常が発生したときに異常を識別します。これには、現在の問題を理解して対処するのに役立つレコメンデーション、関連するメトリクス、およびイベントを含む異常が含まれています。
- 事前対応型: 事前対応型インサイトでは、異常な動作が発生する前に異常を知ることができます。これには、問題の発生が予測される前に問題に対処するのに役立つレコメンデーションを含む異常が含まれています。

メトリクスと運用イベント

インサイトを構成する異常は、Amazon CloudWatch によって返されるメトリクスおよび AWS リソースによって発行される運用イベントによって生成されます。アプリケーションの問題をよりよく理解するのに役立つ、インサイトを作成するメトリクスと運用イベントを表示できます。

ロググループとログ異常

ログ異常検出を有効にすると、関連するロググループが DevOps Guru コンソールの DevOps Guru インサイトページに表示されます。ロググループを使用すると、リソースのパフォーマンスやアクセス状況に関する重要な診断情報を知ることができます。

ログ異常とは、ロググループで見つかった類似の異常なログイベントのクラスターを表します。DevOps Guru に表示される異常なログイベントの例には、キーワードの異常、フォーマットの異常、HTTP コードの異常などがあります。

ログ異常を使用して、運用上の問題の根本原因を診断できます。また、DevOps Guru はインサイトレコメンデーションのログラインを参照して、推奨ソリューションのコンテキストを詳しく説明します。

> **Note**
>
> DevOps Guru は Amazon CloudWatch と連携して、ログ異常検出を可能にします。ログ異常検出を有効にすると、DevOps Guru は CloudWatch のロググループにタグを追加します。ログ異常検出を無効にすると、DevOps Guru は CloudWatch のロググループからタグを削除します。
>
> さらに、管理者は、CloudWatch のログを閲覧する権限を持つユーザーのみが、異常な CloudWatch のログを閲覧する権限を持っていることを確認する必要があります。IAM ポリシーを使用して、`ListAnomalousLogs` オペレーションへのアクセスを許可または拒否することをお勧めします。詳細については、[DevOps Guru のアイデンティティとアクセス管理] を参照してください。

レコメンデーション

各インサイトは、アプリケーションのパフォーマンス向上に役立つレコメンデーションを提供します。レコメンデーションには、以下が含まれます。

- インサイトを構成する異常に対処するためのレコメンデーションアクションの説明。
- DevOps Guru が異常な動作を検出した分析済みメトリクスのリスト。各メトリクスには、メトリクスに関連付けられたリソースを生成した AWS CloudFormation スタック、リソースの名前、およびリソースに関連付けられている AWS のサービスの名前が含まれます。
- インサイトに関連付けられている異常メトリクスに関連するイベントのリスト。関連する各イベントには、イベントに関連付けられたリソースを生成した AWS CloudFormation スタック、イベン

トを生成したリソースの名前、およびイベントに関連付けられた AWS サービスの名前が含まれます。

- インサイトに関連付けられている異常な動作に関連するロググループのリスト。各ロググループには、サンプルログメッセージ、報告されたログ異常の種類に関する情報、ログ異常が発生した時間、および CloudWatch のログの行を表示するリンクが含まれています。

DevOpsGuru カバレッジ

DevOpsGuru は、さまざまな AWS サービスに対応し、インサイトを作成します。 DevOpsGuru がインサイトを作成するサービスごとに、DevOps分析されたさまざまなメトリクスと生成されたインサイトが表示されます。

事後対応型インサイトのユースケース例:

サービス名	ユースケース	例	メトリクス
AWS Lambda	コールドスタート、リクエストの増加、ダウンストリームのスロットリング、コードデプロイなど、さまざまな根本原因によって発生する Lambda 関数のレイテンシーや時間の異常を検出します。迅速に軽減する方法を推奨します。	コードデプロイ: Amazon API Gateway レイテンシーは、最近の Lambda コードデプロイ後の Lambda レイテンシーの増加による影響を受けます。ダウンストリームスロットリング: オペレーターが DynamoDB の読み取りユニットの容量を減らしたため、再試行回数が増加しました。その結果、スロットリングが発生します。コールドスタート: Lambda 関数はプロビジョニングが不十分なため	所要時間 スロットリング

サービス名	ユースケース	例	メトリクス
		、Lambda はリクエストが実行されるまでの時間が長くなります。	

事前対応型インサイトのユースケース例:

サービス名	ユースケース	メトリクス
Amazon DynamoDB	DynamoDB テーブルの読み込み消費容量は、テーブルの上限に達するリスクがあります。推奨アクション: プロビジョニングキャパシティモードを使用している場合は、自動スケーリングを使用してテーブルのスループットキャパシティを積極的に管理するか、テーブルのリザーブドキャパシティを事前に購入してください。オンデマンド容量モードに切り替えると、読み取りリクエストごとに料金が発生し、使用した分だけ料金が発生します。検出時間: 6 日間	ConsumedReadCapacityUnits

サービスのカバレッジリスト

一部のサービスでは、 DevOpsGuru は事後対応型インサイトを作成します。事後対応型インサイトは、異常な動作を発生時に識別します。これには、現在の問題を理解して対処するのに役立つレコメンデーション、関連するメトリクス、およびイベントを含む異常が含まれています。

一部のサービスでは、 DevOpsGuru はプロアクティブなインサイトを作成します。事前対応型インサイトにより、異常な動作が発生する前に問題を知ることができます。これには、問題の発生が予測される前に問題に対処するのに役立つレコメンデーションを含む異常が含まれています。

DevOpsGuru は、次のような サービスの事後対応型インサイトを作成します。

- Amazon API Gateway
- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2

> **Note**
>
> DevOpsGuru モニタリングは Auto Scaling グループレベルであり、単一のインスタンスレベルではありません。

- Amazon ECS
- Amazon EKS
- AWS Elastic Beanstalk
- Elastic Load Balancing
- Amazon Kinesis
- AWS Lambda
- Amazon OpenSearch Service
- Amazon RDS
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker
- AWS Step Functions
- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon VPC

DevOpsGuru は、次のような サービスのプロアクティブなインサイトを作成します。

- Amazon DynamoDB
- Amazon Kinesis
- AWS Lambda
- Amazon RDS
- Amazon SQS

Amazon DevOpsGuru のセットアップ

このセクションのタスクを完了して、Amazon DevOpsGuru を初めてセットアップします。 AWS アカウントが既にあり、分析する AWS アカウントがわかっていて、インサイト通知に使用する Amazon Simple Notification Service トピックがある場合は、「」にスキップできます DevOpsGuru の開始方法。

オプションで、 の一機能である高速セットアップを使用して DevOpsGuru をセットアップし AWS Systems Manager、そのオプションをすばやく設定できます。高速セットアップを使用して、スタンドアロンアカウントまたは組織の DevOpsGuru を設定できます。Systems Manager で高速セットアップを使用して組織の DevOpsGuru をセットアップするには、次の前提条件を満たす必要があります。

- を持つ組織 AWS Organizations。詳細については、AWS Organizations ユーザーガイドの「AWS Organizations Organizations の用語と概念」を参照してください。
- 2 つ以上の組織単位 (OU)。
- 各 OU の 1 つ以上のターゲット AWS アカウント。
- ターゲットアカウントを管理する権限を持つ 1 つの管理者アカウント。

高速セットアップを使用して DevOpsGuru をセットアップする方法については、 ユーザーガイドの「高速セットアップで DevOpsGuru を設定するAWS Systems Manager 」を参照してください。

高速セットアップなしで DevOpsGuru をセットアップするには、次のステップに従います。

- ステップ 1 – にサインアップする AWS
- ステップ 2 – DevOpsGuru のカバレッジを決定する
- ステップ 3 — Amazon SNS 通知トピックを特定する

ステップ 1 – にサインアップする AWS

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。

2. オンラインの手順に従います。

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

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

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

管理アクセスを持つユーザーを作成する

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

のセキュリティ保護 AWS アカウントのルートユーザー

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

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

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

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

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

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

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

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

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

ステップ 2 – DevOpsGuru のカバレッジを決定する

境界カバレッジによって、Amazon DevOpsGuru によって異常な動作について分析される AWS リソースが決まります。リソースを運用アプリケーションにグループ化することをお勧めします。リソース境界内のすべてのリソースは、1 つ以上のアプリケーションで構成する必要があります。運用ソリューションが 1 つの場合、カバレッジ境界にすべてのリソースを含める必要があります。複数のアプリケーションがある場合は、各ソリューションを構成するリソースを選択し、 AWS CloudFormation スタックまたは AWS タグを使用してそれらをグループ化します。1 つ以上のアプリケーションを定義するかどうかにかかわらず、指定したすべての結合リソースは Guru DevOps によって分析され、カバレッジ境界を構成します。

次のいずれかの方法を使用して、運用ソリューションのリソースを指定します。

- を選択して、 AWS リージョンとアカウントでカバレッジ境界を定義します。このオプションを使用すると、 DevOps Guru はアカウントとリージョン内のすべてのリソースを分析します。これは、アカウントを 1 つのアプリケーションにのみ使用する場合に最適なオプションです。
- AWS CloudFormation スタックを使用して、運用アプリケーションのリソースを定義します。AWS CloudFormation テンプレートは、ユーザーに代わってリソースを定義して生成します。DevOpsGuru を設定するときに、アプリケーションリソースを作成するスタックを指定します。スタックはいつでも更新できます。選択したスタック内のすべてのリソースによって境界カバレッジが定義されます。詳細については、「AWS CloudFormation スタックを使用して DevOps Guru アプリケーション内のリソースを識別する」を参照してください。
- AWS タグを使用してアプリケーションの AWS リソースを指定します。 DevOpsGuru は、選択したタグを含むリソースのみを分析します。それらのリソースが境界を構成します。

  AWS タグは、タグキー とタグ値 で構成されます。1 つのタグキーを指定できます。そのキーで 1 つまたは複数の値を指定できます。アプリケーションのすべてのリソースに対して 1 つの値を使用します。複数のアプリケーションがある場合、すべてのアプリケーションに対して同じキーのタグを使用して、タグの値を使用してリソースをアプリケーションにグループ化します。選択したタグを持つすべてのリソースが DevOpsGuru のカバレッジ境界を構成します。詳細については、「タグを使用した DevOpsGuru アプリケーションのリソースの識別」を参照してください。

境界カバレッジに複数のアプリケーションを構成するリソースが含まれている場合、タグを使用してインサイトをフィルターして、一度に 1 つのアプリケーションでインサイトを表示できます。詳細については、「DevOps Guru インサイトの表示」のステップ 4 を参照してください。

詳細については、「AWS リソースを使用したアプリケーションの定義」を参照してください。サポートされているサービスとリソースの詳細については、「Amazon DevOpsGuru の料金」を参照してください。

ステップ 3 — Amazon SNS 通知トピックを特定する

インサイトの作成時など、重要な DevOpsGuru イベントに関する通知を生成するには、1 つまたは 2 つの Amazon SNS トピックを使用します。これにより、DevOpsGru が検出した問題をできるだけ早く把握できます。 DevOpsGuru の設定時にトピックの準備をします。 DevOpsGuru コンソールを使用して DevOpsGuru を設定するときは、その名前または Amazon リソースネーム (ARN) を使用して通知トピックを指定します。詳細については、DevOps「Guru を有効にする」を参照してください。Amazon SNS コンソールを使用して、各トピックの名前と ARN を表示できます。トピックがな

い場合は、Guru コンソールを使用して DevOpsGuru DevOpsを有効にするときに作成できます。詳細については、Amazon Simple Notification Service デベロッパーガイドの「トピックを作成する」を参照してください。

Amazon SNS トピックに追加されたアクセス許可

Amazon SNS トピックは、 AWS Identity and Access Management (IAM) リソースポリシーを含むリソースです。ここでトピックを指定すると、 DevOpsGuru は次のアクセス許可をリソースポリシーに追加します。

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

これらのアクセス許可は、トピックを使用して DevOpsGuru が通知を発行するために必要です。トピックに対するこれらのアクセス許可を使用しない場合は、それらのアクセス許可を安全に削除できます。トピックはアクセス許可を削除する前と同じように機能し続けます。ただし、これらの追加されたアクセス許可が削除された場合、 DevOpsGuru は トピックを使用して通知を生成できません。

Amazon DevOpsGuru リソース分析コストの見積もり

Amazon DevOpsGuru が AWS リソースを分析するための月額コストを見積もることができます。指定したリソース範囲のアクティブな各 AWS リソースに対して実行された分析時間に対する料金が発生します。リソースは、メトリクス、イベント、またはログが 1 時間以内に生成された場合にアクティブになります。

DevOps Guru は、選択したリソースをスキャンして月額コスト見積りを作成します。リソース、時間単位の請求対象料金、および推定月額料金を表示できます。コスト見積りでは、デフォルトで、分析されたアクティブなリソースが時間の 100% 使用されていることを前提としています。推定使用量に基づいて分析された各サービスのこのパーセンテージを変更して、更新された月間コスト見積りを作成できます。見積もりは、リソースを分析するためのコストであり、 DevOpsGuru API コールに関連するコストは含まれません。

コスト見積りは一度に 1 つずつ作成できます。コスト見積りの生成にかかる時間は、コスト見積りを作成するときに指定するリソースの数によって異なります。少量のリソースを指定した場合、完了までに 1 ～ 2 時間かかる場合があります。大量のリソースを指定した場合、完了までに最大 4 時間かかる場合があります。実際のコストは分析したアクティブなリソースの使用時間の割合によって異なります。

> **Note**
>
> 1 つのコストの見積りで指定できるのは 1 つの AWS CloudFormation スタックだけです。実際の対象境界については、最大 1,000 スタックを指定できます。

月次リソース分析のコスト見積りを作成するには

1. https://console.aws.amazon.com/devops-guru/ で Amazon DevOpsGuru コンソールを開きます。
2. ナビゲーションペインで、[コスト見積りツール] を選択します。
3. DevOpsGuru を有効にしていない場合は、IAM ロールを作成する必要があります。表示される DevOpsGuru ポップアップウィンドウの IAM ロールの作成 で、同意 を選択して IAM ロールを作成します。これにより、コスト見積り分析を開始するか、 DevOpsGuru の使用を開始するときに、 DevOpsGuru が IAM サービスにリンクされたロールを作成できます。これにより、DevOpsGuru はコスト見積りの作成に必要なアクセス許可を持ちます。既に DevOpsGuru を有効にしている場合、ロールは既に作成されており、このオプションは表示されません。

4. 推定値の作成に使用するリソースを選択します。

   - 1 つのAWS CloudFormationスタックで定義されたリソースを分析するための DevOpsGuru のコストを見積もるには、次の手順を実行します。
     1. CloudFormation 現在のリージョン でスタック を選択します。
     2. CloudFormation 「スタックの選択」で、AWSアカウント内の AWS CloudFormationスタックの名前を選択します。スタックの名前を入力してスタックをすばやく検索することもできます。スタックの操作と表示の詳細については、AWS CloudFormation ユーザーガイドの「スタックの操作」を参照してください。
     3. (オプション) 現在分析していない AWS CloudFormationスタックを使用する場合は、リソース分析を有効にするを選択して、 DevOpsGru がそのリソースの分析を開始できるようにします。このオプションは、 DevOpsGru を有効にしていない場合、またはスタック内のリソースをすでに分析している場合は使用できません。
   - タグを使用してリソースを分析するための DevOpsGuru のコストを見積もるには、次の手順を実行します。
     1. [Tags on AWS resources in the current Region] (現在のリージョンの AWS リソースのタグ) を選択します。
     2. [Tag key] (タグキー) でタグのキーを選択します。
     3. [Tag value] (タグ値) (すべての値) または 1 つの値を選択します。
   - DevOpsGuru がAWSアカウントとリージョンのリソースを分析するためのコストを見積もる場合は、AWS現在のリージョン のアカウント を選択します。
5. [月額コストの見積り] を選択します。
6. (オプション) [Active resource utilization %] (アクティブなリソース使用率 %) 列に AWS サービスの更新パーセンテージ値を入力します。デフォルトのアクティブなリソース使用率 % は 100% です。つまり、 DevOps Guru はリソースの分析コストを 1 時間計算し、30 日以上を合計 720 時間推定することで、AWS サービスの見積もりを生成します。サービスのアクティブ時間が 100% 未満の場合は、推定使用量に基づいてパーセンテージを更新して、より正確な見積りを行うことができます。例えば、サービスのアクティブなリソース使用率を 75% に更新すると、リソース分析の 1 時間のコストが (720 x 0.75) 時間 (540 時間) にわたって外挿されます。

見積りがゼロドルの場合、選択したリソースには DevOpsGuru でサポートされているリソースが含まれていない可能性があります。サポートされているサービスとリソースの詳細については、「Amazon DevOpsGuru の料金」を参照してください。

DevOpsGuru の開始方法

このセクションでは、アプリケーションの運用データとメトリクスを分析してインサイトを生成できるように、Amazon DevOpsGuru の使用を開始する方法について説明します。

トピック

ステップ 1: セットアップを開始する

開始する前に、「Amazon DevOpsGuru のセットアップ」の手順を実行して準備します。

ステップ 2: DevOpsGuru を有効にする

を初めて使用するように Amazon DevOpsGuru を設定するには、Guru DevOpsのセットアップ方法を選択する必要があります。組織全体のアプリケーションをモニタリングするか、現在のアカウントでアプリケーションをモニタリングすることができます。

組織全体のアプリケーションをモニタリングするか、現在のアカウントに対してのみ DevOpsGuru を有効にすることができます。次の手順では、ニーズに基づいて DevOpsGuru を設定するさまざまな方法の概要を説明します。

組織全体のアカウントをモニタリングする

組織全体のアプリケーションをモニタリングする場合は、組織の管理アカウントにログインします。必要に応じて、組織メンバーアカウントを委任管理者としてセットアップします。一度に設定できる委任管理者は 1 人だけですが、後で管理者設定を変更できます。管理アカウントおよび設定した委任管理者アカウントの両方は、組織内のすべてのアカウントのすべてのインサイトにアクセスできます。

コンソールを使用して組織のクロスアカウントサポートを追加するか、 AWS CLI を使用してサポートを追加できます。

DevOpsGuru コンソールでオンボードする

コンソールを使用して、組織全体のアカウントのサポートを追加できます。

コンソールを使用して Guru DevOpsが集約されたインサイトを表示できるようにする

1. https://console.aws.amazon.com/devops-guru/ で Amazon DevOpsGuru コンソールを開きます。
2. セットアップタイプとして [Monitor applications across your organizations] (組織全体のアプリケーションをモニタリングする) を選択します。
3. 委任管理者として使用するアカウントを選択します。[Register delegated administrator] (委任管理者の登録) を選択します。これにより、 DevOpsGru が有効になっているすべてのアカウントの統合ビューにアクセスできます。委任された管理者は、組織全体のすべての DevOpsGuru インサイトとメトリクスをまとめて表示できます。SSM Quick Setup または AWS CloudFormation スタックセットを使用して他のアカウントを有効にすることができます。クイックセットアップの詳細については、「Configure DevOps Guru with Quick Setup」を参照してください。スタックセットでのセットアップの詳細については、AWS CloudFormation ユーザーガイドの「スタックの操作」 および「ステップ 2 – DevOpsGuru のカバレッジを決定する」と「AWS CloudFormation スタックを使用して DevOps Guru アプリケーション内のリソースを識別する」を参照してください。

AWS CLI によるオンボード

AWS CLI を使用して、 DevOpsGru が集約されたインサイトを表示できるようにします。以下のコマンドを実行します。

```
aws iam create-service-linked-role --aws-service-name devops-guru.amazonaws.com --
description "My service-linked role to support DevOps Guru"

aws organizations enable-aws-service-access --service-principal devops-
guru.amazonaws.com

aws organizations register-delegated-administrator --account-id >ACCOUNT_ID< --service-
principal devops-guru.amazonaws.com
```

次の表では、コマンドについて説明します。

コマンド	説明
`create-service-linked-role`	

コマンド	説明
	組織に関する情報を収集する許可を DevOpsGuru に付与します。このステップが成功しない場合は先に進まないでください。
`enable-aws-service-access`	組織を DevOpsGuru にオンボードします。
`register-delegated-administrator`	メンバーアカウントにアクセスしてインサイトを表示します。

現在のアカウントを監視する

現在の AWS アカウントでアプリケーションをモニタリングする場合は、アカウントとリージョン内のどの AWS リソースをカバーまたは分析するかを選択し、インサイトの作成時に通知するために使用する Amazon Simple Notification Service トピックを 1 つまたは 2 つ指定します。これらの設定は、必要に応じて後で更新できます。

DevOpsGuru が現在のアカウントのアプリケーションをモニタリングできるようにする AWS

1. https://console.aws.amazon.com/devops-guru/ で Amazon DevOpsGuru コンソールを開きます。
2. セットアップタイプとして [Monitor applications in the current AWS account] (現在の AWS アカウントのアプリケーションをモニタリングする) を選択します。
3. DevOpsGuru 分析カバレッジ で、次のいずれかを選択します。

   - 現在の AWS アカウントのすべての AWS リソースを分析する ： DevOpsGuru はアカウント内のすべての AWS リソースを分析します。
   - [分析する AWS リソースを後で選択する] : 解析境界を後で選択します。詳細については、「DevOpsGuru のカバレッジを決定する」および「DevOps Guru でのAWS分析カバレッジの更新」を参照してください。

   DevOpsGuru は、サポートする AWS アカウントに関連付けられているすべてのリソースを分析できます。サポートされているサービスとリソースの詳細については、「Amazon DevOpsGuru の料金」を参照してください。

4. 最大 2 つのトピックを追加できます。 DevOpsGuru はトピックを使用して、新しいインサイトの作成など、重要な DevOpsGuru イベントを通知します。トピックを指定しない場合は、ナビゲーションペインで [設定] を選択して後で追加することができます。

   a. [Specify an Amazon SNS topic] (Amazon SNS トピックを指定) で、使用するトピックを選択します。

   b. Amazon SNS トピックを作成するには、次のいずれかを実行します。

      - [メールを使用して新しい SNS トピックを生成] を選択します。次に、[メールアドレスを指定] から、通知を受け取るメールアドレスを入力します。追加のメールアドレスを入力するには、[新しい E メールを追加] を選択します。
      - [既存の SNS トピックを使用] を選択します。次に、 AWS アカウント でトピックを選択から、使用するトピックを選択します。
      - 別のアカウントの既存のトピックを指定するには、[既存の SNS トピック ARN を使用します] を選択します。[Enter an ARN for a topic] (トピックの ARN を入力) にトピック ARN を入力します。ARN はトピックの Amazon リソースネームです。別のアカウントのトピックを指定できます。別のアカウントのトピックを使用する場合は、トピックにリソースポリシーを追加する必要があります。詳細については、「Amazon SNS トピックへの許可」を参照してください。

5. [Enable (有効化)] を選択します。

を初めて使用するように Amazon DevOpsGuru を設定するには、アカウントとリージョンで対象または分析するリソースを選択し AWS 、インサイトの作成時に通知するために使用する Amazon Simple Notification Service トピックを 1 つまたは 2 つ指定する必要があります。これらの設定は、必要に応じて後で更新できます。

ステップ 3: DevOpsGuru リソースカバレッジを指定する

後で DevOpsGuru を有効にしたときに AWS リソースを指定する場合は、分析するリソースを作成する AWS アカウント内の AWS CloudFormation スタックを選択する必要があります。 AWS CloudFormation スタックは、単一のユニットとして管理する AWS リソースのコレクションです。1 つ以上のスタックを使用して、運用アプリケーションの実行に必要なすべてのリソースを含め、それらが DevOpsGuru によって分析されるように指定できます。スタックを指定しない場合、 DevOpsGuru はアカウント内のすべての AWS リソースを分析します。詳細については、AWS CloudFormation ユーザーガイドの「スタックの操作」および「DevOpsGuru のカバレッジを決定す

る」と「AWS CloudFormation スタックを使用して DevOps Guru アプリケーション内のリソースを識別する」を参照してください。

> **Note**
>
> サポートされているサービスとリソースの詳細については、「Amazon DevOpsGuru の料金」を参照してください。

DevOpsGuru リソースカバレッジを指定する

1. https://console.aws.amazon.com/devops-guru/ で Amazon DevOpsGuru コンソールを開きます。
2. ナビゲーションペインで、[設定] を展開します。
3. [分析されたリソース] で [分析されたリソースの編集] を選択します。
4. 以下のカバレッジオプションのいずれかを選択します。

   - DevOpsGuru でアカウントとリージョンでサポートされているすべてのリソースを分析する場合は、すべての AWS アカウントリソースを選択します。このオプションを選択した場合、AWS アカウントはリソース分析カバレッジの境界になります。アカウント内の各スタックのすべてのリソースは、それぞれのアプリケーションにグループ化されます。スタックにない残りのリソースは、そのアプリケーションにグループ化されます。
   - DevOpsGuru で選択したCloudFormation スタック内のリソースを分析する場合はスタックを選択し、次のいずれかのオプションを選択します。
     - [すべてのリソース] — アカウント内のスタックにあるすべてのリソースが分析されます。各スタックのリソースは、そのアプリケーションにグループ化されます。スタックにないアカウント内のリソースは分析されません。
     - スタックの選択 — DevOpsGuru で分析するスタックを選択します。選択した各スタックのリソースは、そのアプリケーションにグループ化されます。スタックの名前を [Find stacks] (スタックの検索) を入力すると、特定のスタックをすばやく特定できます。最大 1,000 個のスタックを選択できます。

     詳細については、「AWS CloudFormation スタックを使用して DevOps Guru アプリケーション内のリソースを識別する」を参照してください。
   - 選択したタグを含むすべてのリソースを DevOpsGuru で分析する場合は、タグ を選択します。[キー] を選択し、次のいずれかのオプションを選択します。

- [すべてのアカウントリソース] — 現在のリージョンとアカウントのすべての AWS リソースを分析します。選択したタグキーを持つリソースは、タグ値ごとにグループ化されます (存在する場合)。このタグキーのないリソースはグループ化され、個別に分析されます。
- 特定のタグ値を選択する – 選択したキーを持つタグを含むすべてのリソースが分析されます。 DevOpsGuru は、タグの値 によってリソースをアプリケーションにグループ化します。

  タグのキーは、プレフィックス `devops-guru-` で始まる必要があります。このプレフィックスでは大文字と小文字は区別されません。例えば、有効なキーは `DevOps-Guru-Production-Applications` です。詳細については、「タグを使用した DevOpsGuru アプリケーションのリソースの識別」を参照してください。

- DevOpsGuru がリソースを分析したくない場合は、なしを選択します。このオプションは DevOpsGuru を無効にして、リソース分析による料金の発生を停止します。

5. [保存] を選択します。

DevOps Guru 分析のための AWS サービスを有効にする

Amazon DevOps Guru では、サポートされるすべての AWS リソースのパフォーマンスを分析できます。異常な動作が検出されると、その動作とその対処方法に関する詳細を含むインサイトが生成されます。サポートされているサービスとリソースの詳細については、「Amazon DevOps Guru の料金」を参照してください。

DevOps Guru は Amazon CloudWatch メトリクスや AWS CloudTrail イベントなどを使用してリソースの分析を行います。サポートされているほとんどのリソースは、DevOps Guru 分析に必要なメトリクスを自動的に生成します。しかし、いくつかの AWS サービスでは、必要なメトリクスを生成するために追加のアクションが必要です。一部のサービスでは、これらのメトリクスを有効にすると、既存の DevOps Guru カバレッジに対する追加の分析が提供されます。その他のサービスでは、これらのメトリクスを有効にするまで分析を行うことができません。詳細については、DevOpsGuru のカバレッジを決定する および DevOps Guru でのAWS分析カバレッジの更新 を参照してください。

DevOps Guru 分析のためのアクションを必要とするサービス

- Amazon Elastic コンテナサービス — リソースの DevOps Guru カバレッジを改善する追加のメトリクスを生成するには、「Amazon ECS での Container Insights のセットアップ」の手順に従います。これを行うと、Amazon CloudWatch の料金が発生する可能性があります。
- Amazon Elastic Kubernetes Service — DevOps Guru が分析するメトリクスを生成するには、「Amazon EKS と Kubernetes での Container Insights のセットアップ」の手順に従います。DevOps Guru では、これらのメトリクスの生成が設定されるまで Amazon EKS リソースの分析が行われません。これを行うと、Amazon CloudWatch の料金が発生する可能性があります。
- Amazon Simple Storage Service — DevOps Guru が分析するメトリクスを生成するには、リクエストメトリクスを有効にする必要があります。バケット内のすべてのオブジェクトに対する CloudWatch メトリクス設定の作成の手順に従います。DevOps Guru では、これらのメトリクスの生成が設定されるまで Amazon S3 リソースの分析が行われません。これを行うと、CloudWatch および Amazon S3 の料金が発生する可能性があります。

詳細については、「Amazon CloudWatch の料金」を参照してください。

DevOps Guru でのインサイトの使用

Amazon DevOps Guruは、運用アプリケーションで異常な動作を検出するとインサイトを生成します。DevOps Guru は、セットアップ時に指定した AWS リソース内のメトリクスやイベントなどを分析します。各インサイトには、問題を軽減するためのレコメンデーションが含まれています。また、異常な動作を識別するために使用されたメトリクスとロググループのリストも含まれています。

インサイトには 2 つのタイプがあります。

- 事後対応型インサイトには、現在発生している問題に対処するためのレコメンデーションがあります。
- 事前対応型インサイトには、DevOps Guru が将来発生すると予測する問題に対処するレコメンデーションがあります。

トピック

DevOps Guru インサイトの表示

インサイトは、AWS Management Console を使用して表示できます。

DevOps Guru のインサイトの表示

1. Amazon DevOps Guru コンソール (https://console.aws.amazon.com/devops-guru/) を開きます。
2. ナビゲーションペインを開き、[Insights] (インサイト) を選択します。
3. [Reactive] (事後対応型) タブには、事後対応型インサイトのリストが表示されます。[Proactive] (事前対応型) タブには、事前対応型インサイトのリストが表示されます。
4. (オプション) 次のフィルターを使用して目的のインサイトを検索します。
   - 目的のインサイトのタイプに応じて [事後対応型] または [事前対応型] タブを選択します。

- [Filter insights] (インサイトのフィルター) を選択して、フィルターを指定するオプションを選択します。ステータス、重要度、リソース、およびタグフィルターの組み合わせを追加できます。特定のタグを持つリソースによって生成されたインサイトだけを表示するには、AWS タグフィルターを使用します。詳細については、「タグを使用した DevOpsGuru アプリケーションのリソースの識別」を参照してください。

> **Note**
>
> DevOps Guru は次のリソースを分析できますが、タグを使用してインサイトをフィルターすることはできません。
>
> - Amazon API Gateway のパスとルート
> - Amazon DynamoDB Streams
> - Amazon EC2 Auto Scaling グループインスタンス
> - AWS Elastic Beanstalk 環境
> - Amazon Redshift ノード

- インサイトの作成時間でフィルターする時間範囲を選択または指定します。
  - [12h] を選択すると、過去 12 時間に作成されたインサイトが表示されます。
  - [1d] を選択すると、過去 1 日に作成されたインサイトが表示されます。
  - [1w] を選択すると、過去 1 週間に作成されたインサイトが表示されます。
  - [1m] を選択すると、過去 1 か月間に作成されたインサイトが表示されます。
  - [Custom] (カスタム) を選択すると、別の時間範囲を指定できます。インサイトのフィルターに使用できる最大時間範囲は 180 日です。

5. インサイトの詳細を表示するには、その名前を選択します。

DevOps Guru コンソールに表示されるインサイト

Amazon DevOps Guru コンソールを使用して、インサイト内の有用な情報を表示し、異常な動作の診断と対処に役立てることができます。DevOps Guru がリソースを分析し、異常な動作を示す Amazon CloudWatch メトリクス、AWS CloudTrail イベント、および異常な動作を示す運用データを検出すると、問題に対処するためのレコメンデーションと関連するメトリクスおよびイベントに関

する情報を含むインサイトが作成されます。インサイトデータと DevOps Guru のベストプラクティスを使用して、DevOps Guru によって検出された運用の問題に対処します。

インサイトを表示するには、「インサイトの表示」のステップに従ってインサイトを見つけて、その名前を選択します。インサイトページには次の詳細が含まれています。

インサイトの概要

このセクションを使用して、インサイトの高レベルの概要を取得します。インサイトのステータス (継続またはクローズ)、影響を受ける AWS CloudFormation スタックの数、インサイトの開始時刻、終了時刻、および最終更新時刻、および関連する運用項目 (存在する場合) を表示できます。

インサイトがスタックレベルでグループ化されている場合、影響を受けるスタックの数を選択して、その名前を表示できます。インサイトを作成した異常な動作は、影響を受けるスタックによって作成されたリソースで発生しています。インサイトがアカウントレベルでグループ化されている場合、数値は 0 であるか、表示されません。

詳細については、「異常行動がインサイトにグループ化される仕組み」を参照してください。

インサイト名

インサイトの名前は、インサイトがスタックレベルでグループされているか、アカウントレベルでグループ化されているかに応じて異なります。

- スタックレベルのインサイト名には、異常な動作が検出されたリソースを含むスタックの名前が含まれます。
- アカウントレベルのインサイト名にはスタック名は含まれません。

詳細については、「異常行動がインサイトにグループ化される仕組み」を参照してください。

集約されたメトリクス

[Aggregated metrics] (集約されたメトリクス) タブを選択して、インサイトに関連するメトリクスを表示します。テーブルの各行は 1 つのメトリクスを表します。メトリクスを発行したリソースを作成した AWS CloudFormation スタック、リソースの名前とタイプを表示できます。すべてのメトリクスが AWS CloudFormation スタックに関連付けられているではありません。名前のないメトリクスもあります。

同時に複数のリソースが異常である場合、タイムラインビューはリソースを集約し、分析を簡単にする目的で、その異常なメトリクスを単一のタイムラインに表示します。タイムラインの赤い

線は、メトリクスが異常な値を発行した時間範囲を示します。ズームインするには、マウスを使用して特定の時間範囲を選択します。虫眼鏡アイコンを使用してズームイン/ズームアウトすることもできます。

タイムラインの赤い線を選択すると、詳細情報が表示されます。表示されるウィンドウで、次の操作を実行できます。

- [View in CloudWatch] (CloudWatch で表示) を選択すると、CloudWatch コンソールでメトリクスが表示されます 詳細については、Amazon CloudWatch ユーザーガイドの「Statistics」と「Dimensions」を参照してください。
- グラフにカーソルを合わせると、異常なメトリクスデータとその発生時間の詳細が表示されます。
- 下向き矢印の付いたボックスを選択すると、グラフの PNG 画像がダウンロードされます。

グラフに表示された異常

[Graphed anomalies] (グラフに表示された異常) タブを選択すると、各インサイトの異常に関する詳細なグラフが表示されます。各異常に対して 1 つのタイルが表示され、関連する指標で検出された異常な動作の詳細が表示されます。リソースレベルおよび統計ごとに異常を調査して確認できます。グラフはメトリクス名でグループ化されています。各タイルで、タイムラインの特定の時間範囲を選択してズームできます。虫眼鏡アイコンを使用してズームインとズームアウトすることや、定義済みの期間を時間、日、週単位 ([1H]、[3H]、[12H]、[1D]、[3D]、[1W]、または [2W]) で選択することもできます。

[View all statistics and dimensions] (すべての統計とディメンションを表示) を選択すると、異常に関する詳細が表示されます。表示されるウィンドウで、次の操作を実行できます。

- [View in CloudWatch] (CloudWatch で表示) を選択すると、CloudWatch コンソールでメトリクスが表示されます
- グラフにカーソルを合わせると、異常なメトリクスデータとその発生時間の詳細が表示されます。
- [Statistics] (統計) または [Dimension] (ディメンション) を選択すると、グラフの表示をカスタマイズできます。詳細については、Amazon CloudWatch ユーザーガイドの「Statistics」と「Dimensions」を参照してください。

ロググループ

ログ異常検出を有効にすると、DevOps Guru は CloudWatch ロググループにタグを付け、インサイトに関連するロググループを表示できるようにします。インサイト詳細ページの ロググループ セクションでは、表の各行が 1 つのロググループを表し、関連するリソースを一覧表示します。

同時に複数の異常なロググループが存在する場合、タイムラインビューはリソースを集約し、分析を簡単にする目的で、単一のタイムラインに表示します。タイムラインの紫色の線は、ロググループにログ異常が発生した時間範囲を示します。

タイムラインの紫色の線を選択すると、キーワードの例外や数値偏差などのログ異常情報のサンプルが表示されます。[ロググループの詳細を表示] を選択すると、ログの異常が表示されます。表示されるウィンドウで、次の操作を実行できます。

- ログの異常と関連イベントのグラフを表示します。
- グラフにカーソルを合わせると、異常なログデータとその発生時間の詳細が表示されます。
- サンプルメッセージ、発生頻度、関連するリコメンデーション、発生時刻とともにログの異常を詳細に表示できます。
- [CloudWatch で詳細を表示] をクリックすると、ログ異常のログ行が表示されます。

関連イベント

[Related events] (関連イベント) で、インサイトに関連する AWS CloudTrail イベントを表意jします。これらのイベントを使用して、異常動作の根本的な原因を理解および診断して異常動作に対処します。

レコメンデーション

[Recommendations] (レコメンデーション) で、根本的な問題の解決に役立つ可能性のある推奨事項を表示できます。DevOps Guru が異常な動作を検出すると、レコメンデーションの作成が試みられます。インサイトにレコメンデーションが含まれないこともあります。

異常行動がインサイトにグループ化される仕組み

インサイトは、スタックレベルまたはアカウントレベルでグループ化されます。AWS CloudFormation スタックに含まれるリソースに対して生成されたインサイトはスタックレベルのインサイトです。それ以外のインサイトはアカウントレベルのインサイトです。

スタックがグループ化される方法は、Amazon DevOps Guru でリソース分析カバレッジをどのように構成したかに応じて異なります。

カバレッジが AWS CloudFormation スタックによって定義されている場合

選択したスタックに含まれるすべてのリソースが分析され、検出されたすべてのインサイトはスタックレベルでグループ化されます。

カバレッジが現在の AWS アカウントとリージョンである場合

アカウントとリージョン内のすべてのリソースが分析され、検出されたインサイトには 3 つのグループ化シナリオがあります。

- スタックの一部ではないリソースの生成されたインサイトは、アカウントレベルでグループ化されます。
- 最初の 10,000 個の解析されたスタックにあるリソースから生成されたインサイトは、スタックレベルでグループ化されます。
- 最初の 10,000 個の解析されたスタックにないリソースから生成されたインサイトは、アカウントレベルでグループ化されます。例えば、10,001 番目の分析スタック内のリソースに対して生成されたインサイトは、アカウントレベルでグループ化されます。

詳細については、「DevOpsGuru のカバレッジを決定する」を参照してください。

インサイトの重要度の概要

インサイトには、3 つの重大度 (高,中, または低) があります。Amazon DevOps Guru が関連する異常を検出し、各異常に重要度を割り当てると、インサイトが作成されます。DevOps Guru は、ドメインの知識と長年の集団体験を使用して、異常の重要度 (高、中、または低) を割り当てます。インサイトの重要度は、インサイトの作成に寄与した最も重要な異常によって決定されます。

- インサイトを生成したすべての異常の重要度が低である場合、インサイトの重大度は低になります。
- インサイトを生成したすべての異常の最も高い重要度が中である場合、インサイトの重大度は中になります。インサイトを生成した一部の異常の重要度は低である可能性があります。
- インサイトを生成したすべての異常の最も高い重要度が高である場合、インサイトの重大度は高になります。インサイトを生成した一部の異常の重要度は低または中である可能性があります。

DevOpsGuru を使用したデータベースのモニタリング

DevOpsGuru は、 でデータベースを運用する上で大きな価値を提供します AWS。機械学習アルゴリズムを活用することで、 DevOpsGuru はデータベースのパフォーマンスの最適化、信頼性の向上、運用オーバーヘッドの削減に役立ちます。ユーザーガイドのこのセクションでは、さまざまなデータベースサービスの特定の DevOpsGuru ユースケースなど、これらの AWS データベース機能の概要を説明します。

DevOpsGuru は、Amazon RDS や などのリレーショナルデータベースに関するインサイトを提供できます Amazon Redshift。また、 Amazon DynamoDB や などの非リレーショナルデータベースや NoSQL データベースに関するインサイトを提供することもできます Amazon ElastiCache。

トピック

- DevOpsGuru を使用したリレーショナルデータベースのモニタリング
- DevOpsGuru を使用した非リレーショナルデータベースのモニタリング

DevOpsGuru を使用したリレーショナルデータベースのモニタリング

DevOpsGuru は 2 つの主要なデータソースからプルして、リレーショナルデータベースのインサイトや異常を探します。Amazon RDS および の場合 Amazon Redshift、 CloudWatch 提供されるメトリクスはすべてのインスタンスタイプについて分析されます。Amazon RDS の場合、Performance Insights データは RDS for PostgreSQL、Aurora PostgreSQL、および Aurora MySQL のエンジンタイプにも取り込まれます。

Amazon RDS でのデータベースオペレーションのモニタリング

このセクションには、 CloudWatch 提供されるメトリクスや Performance Insights からのデータなど、 DevOpsGru for RDS でモニタリングされるユースケースとメトリクスに関する具体的な情報が含まれています。主要な概念、設定、利点を含む DevOpsGuru for RDS の詳細については、「」を参照してくださいthe section called “ DevOpsGuru for RDS での異常の操作”。

提供されるメトリクスのデータ CloudWatch を使用した RDS のモニタリング

DevOpsGuru は、CPU 使用率や読み取り/書き込みオペレーションのレイテンシーなどのデフォルトの CloudWatch メトリクスを取り込むことで、すべてのタイプの RDS インスタンスをモニタリング

できます。これらのメトリクスはデフォルトで提供されるため、RDS インスタンスを DevOpsGuru でモニタリングする場合、インサイトを得るために追加の設定は必要ありません。 DevOpsGuru は、履歴パターンに基づいてこれらのメトリクスのベースラインを自動的に確立し、リアルタイムデータと比較してデータベース内の異常や潜在的な問題を検出します。

次の表は、 CloudWatch Amazon RDS が提供するメトリクスの潜在的な事後対応型インサイトのリストを示しています。

AWS DevOpsGuru によってモニタリングされる リソース	DevOpsGuru が識別するシナリオ	CloudWatch モニタリングされる メトリクス
Amazon RDS (すべてのインスタンスタイプ)	CPU またはメモリが制限に達する	DBLoad、DBLoadCPU
RDS for PostgreSQL	高いレプリケーションスロットラグ	OldestReplicationSlotLag

DevOpsGuru がモニタリングする Amazon RDS インスタンスから CloudWatch 提供される追加のメトリクス :

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- FailedSQLServerAgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

Performance Insights のデータを使用した RDS のモニタリング

Aurora PostgreSQL、Aurora MySQL、RDS for PostgreSQL などの特定のタイプの Amazon RDS インスタンスでは、それらのインスタンスで Performance Insights が有効になっていることを確認することで、 DevOpsGuru モニタリングからより多くの機能を引き出すことができます。

DevOpsGuru は、次のようなさまざまな状況に対応する事後対応型インサイトを提供します。

DevOpsGuru が事後対応型インサイトを生成するために識別するシナリオ
ロックの競合の問題
インデックスがありません
アプリケーションプールの設定ミス
最適ではない JDBC のデフォルト

DevOpsGuru は、以下のシナリオを含むさまざまな状況に対してプロアクティブインサイトを提供します。

AWS DevOpsGuru によってモニタリングされる リソース	DevOpsGuru がプロアクティブインサイトを生成するために識別するシナリオ
Aurora MySQL	InnoDB 履歴リストが大きくなりすぎると、データベースの長いシャットダウン時間などのパフォーマンスが低下する可能性があります。
Aurora MySQL	ディスク上に作成されるテンポラリテーブルの増加によるデータベースのパフォーマンスへの影響
RDS for PostgreSQL、Aurora PostgreSQL	トランザクションでアイドル状態が長すぎる接続。ロックを保持し、他のクエリをブロックし、バキューム (autovacuum を含む) でデッド行がクリーンアップされないことによる潜在的な影響

でのデータベースオペレーションのモニタリング Amazon Redshift

DevOpsGuru は、CPU 使用率やディスク容量の割合など、デフォルトの CloudWatch メトリクスを取り込むことで Amazon Redshift リソースをモニタリングできます。これらのメトリクスはデフォルトで提供されるため、 DevOpsGru が Amazon Redshift リソースを自動的にモニタリングするために追加の設定は必要ありません。 DevOpsGuru は、履歴パターンに基づいてこれらのメトリクスのベースラインを確立し、それらをリアルタイムデータと比較して異常を検出します。

DevOpsGuru が識別するシナリオ	CloudWatch モニタリングされる メトリクス
クラスターワークロード、歪んだデータと未ソートのデータ、リーダーノードタスクなどの要因によって引き起こされる Amazon Redshift インスタンスの CPU 使用率が高いことを検出する	CPUUtilization
クエリ処理、ディストリビューションキーとソートキー、メンテナンスオペレーション、またはトゥームストルブロックの問題により、Amazon Redshift インスタンスのディスク容量が不足している場合を検出します。	PercentageDiskSpaceUsed

DevOpsGuru がモニタリングする Amazon Redshift インスタンスから CloudWatch 提供される追加のメトリクス：

- DatabaseConnections
- HealthStatus
- MaintenanceMode
- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS
- ReadLatency
- WLMQueueLength
- WLMQueueWaitTime
- WLMQueryDuration
- WriteLatency

DevOpsGuru for RDS での異常の操作

DevOpsGuru は、Amazon RDS エンジンなど、サポートされているAWSリソースを検出、分析し、レコメンデーションを提供します。Performance Insights がオンになっている Amazon Aurora および RDS for PostgreSQL データベースインスタンスの場合、RDS の DevOpsGuru は、パフォーマンスの問題の詳細なデータベース固有の分析を提供し、是正措置を推奨します。

トピック

DevOpsGuru for RDS の概要

以下は、 DevOpsGru for RDS の主な利点と機能の概要です。インサイトと異常に関する背景情報については、「 DevOps Guru の概念」を参照してください。

トピック

DevOpsGuru for RDS の利点

Amazon RDS データベースを担当していて、そのデータベースに影響を与えるイベントやリグレッションが発生していることを知らないことがあります。問題を知っても、なぜそれが発生しているのか、どう対処すべきかわからないこともあります。データベース管理者 (DBA) にサポートを依頼したり、サードパーティツールに頼ったりするのではなく、 DevOpsGuru for RDS のレコメンデーションに従うことができます。

DevOpsGuru for RDS の詳細な分析には、次の利点があります。

高速診断

DevOpsGuru for RDS は、データベーステレメトリを継続的にモニタリングおよび分析します。Performance Insights、拡張モニタリング、および Amazon CloudWatch は、データベースインスタンスのテレメトリデータを収集します。RDS の DevOpsGuru は、統計および機械学習技術を使用してこのデータをマイニングし、異常を検出します。Amazon Aurora データベースのテレメトリデータの詳細については、「Amazon Aurora ユーザーガイド」の「Amazon Aurora の Performance Insights を使用した DB 負荷のモニタリング」および「拡張モニタリングを使用した OS のモニタリング」を参照してください。Amazon RDS データベースのテレメトリデータの詳細については、「Amazon RDS ユーザーガイド」の「Amazon リレーショナルデータベースサービスの Performance Insights を使用した DB 負荷のモニタリング」および「拡張モニタリングを使用した OS のモニタリング」を参照してください。

高速解像度

各異常はパフォーマンスの問題を特定し、調査または修正措置の方法を提案します。例えば、RDS の DevOpsGuru では、特定の待機イベントの調査が推奨される場合があります。または、データベース接続数を制限するよう、アプリケーションプールの設定のチューニングをお勧めすることもあります。これらのレコメンデーションに基づいて、マニュアルでトラブルシューティングを実行するよりも迅速にパフォーマンスの問題を解決できます。

事前対応型インサイト

DevOpsGuru for RDS は、リソースのメトリクスを使用して、潜在的に問題のある動作を検出してから、大きな問題になります。例えば、データベースに接続されたセッションがアクティブな作業を行っておらず、データベースリソースがブロックされている可能性があることを検出できます。 DevOpsGuru は、問題が大きくなる前に問題に対処するためのレコメンデーションを提供します。

Amazon エンジニアの深い知識と機械学習

パフォーマンスの問題を検出し、ボトルネックの解決を支援するために、 DevOpsGuru for RDS は機械学習 (ML) と高度な統計分析に依存しています。Amazon データベースエンジニアは、数十万のデータベースを管理している何年もにわたる をカプセル化する DevOpsGuru for RDS の検出結果の開発に貢献しました。この集合的な知識を活用することで、 DevOpsGuru for RDS はベストプラクティスを伝えることができます。

データベースのパフォーマンスチューニングの主な概念

DevOpsGuru for RDS は、いくつかの主要なパフォーマンス概念に精通していることを前提としています。これらの概念の詳細については、Amazon Aurora ユーザーガイドの「Performance Insights

の概要」または Amazon RDS ユーザーガイドの「Performance Insights の概要」を参照してください。

トピック

- メトリクス
- 問題の検出
- DB 負荷
- 待機イベント

メトリクス

メトリクスは、時間順に並んだ一連のデータポイントを表します。メトリクスはモニターリング対象の変数と考え、データポイントは時間の経過と共に変数の値を表します。Amazon RDS には、DB インスタンスが実行されているデータベースとオペレーティングシステム (OS) のメトリクスをリアルタイムで提供します。Amazon RDS DB インスタンスのすべてのシステムメトリクスとプロセス情報を Amazon RDS コンソールに表示できます。 DevOpsGuru for RDS は、これらのメトリクスの一部をモニタリングし、インサイトを提供します。詳細については、「Amazon Aurora クラスターのメトリクスのモニタリング」または「Amazon リレーショナルデータベース サービス インスタンスのメトリクスのモニタリング」を参照してください。

問題の検出

DevOpsGuru for RDS は、データベースとオペレーティングシステム (OS) のメトリクスを使用して、重大なデータベースパフォーマンスの問題が差し迫っているか、進行中かを検出します。DevOpsGuru for RDS の問題検出が機能するには、主に 2 つの方法があります。

- しきい値を使用する
- 異常を使用する

しきい値に関する問題の検知

しきい値は、監視対象のメトリクスが評価される境界値です。しきい値は、通常の動作と潜在的に問題のある動作を区別するメトリクスグラフ上の水平線と考えることができます。 DevOpsGuru for RDS は特定のメトリクスをモニタリングし、指定されたリソースで潜在的に問題と見なされるレベルを分析してしきい値を作成します。次に、RDS の DevOpsGuru は、新しいメトリクス値が一定の期間にわたって指定されたしきい値を超えた場合に DevOps、Guru コンソールにインサイトを作成

します。インサイトには、将来のデータベースのパフォーマンスへの影響を防ぐためのレコメンデーションが含まれています。

例えば、RDS の DevOpsGuru は 15 分間のディスクを使用して一時テーブルの数をモニタリングし、ディスク/秒を使用する一時テーブルのレートが異常に高い場合にインサイトを作成する場合があります。ディスク上の一時テーブルの使用レベルが増加すると、データベースのパフォーマンスに影響を与える可能性があります。この状況が重要になる前に公開することで、 DevOpsGuru for RDS は問題を防止するための是正措置を講じるのに役立ちます。

異常による問題の検出

しきい値はデータベースの問題を検出する簡単で効果的な方法ですが、状況によってはそれだけでは不十分な場合もあります。日次報告ジョブなどの既知のプロセスが原因で、メトリクス値が定期的に急上昇し、潜在的に問題となる可能性のある動作に変わるケースを考えてみましょう。このような急増は予期されることであり、それぞれについてインサイトや通知を作成することは逆効果になり、アラート疲労につながる可能性があります。

ただし、非常にまれなスパイクを検出することは依然として必要です。他のメトリクスよりもずっと高い値であったり、ずっと長く続くメトリクスは、実際のデータベースパフォーマンスの問題を表している可能性があるためです。この懸念に対処するために、RDS の DevOpsGuru は特定のメトリクスをモニタリングして、メトリクスの動作が非常に異常または異常になったことを検出します。DevOpsGuru は、これらの異常をインサイトで報告します。

例えば、RDS の DevOpsGuru は、DB 負荷が高いだけでなく、通常の動作から大きく逸脱した場合にインサイトを作成することがあります。これは、データベースオペレーションの予期しない大幅な速度低下を示していることを示しています。 DevOpsGuru for RDS では、異常な DB 負荷のスパイクのみを認識することで、真に重要な問題に集中できます。

DB 負荷

データベースのチューニングの主な概念は、データベース負荷 (DB 負荷) メトリクスです。DB 負荷は、特定の時点でのデータベースのビジー状態を表します。DB 負荷の増加は、データベースアクティビティの増加を意味します。

データベースセッションは、リレーショナルデータベースとのアプリケーションのダイアログを表します。アクティブなセッションは、データベースリクエストの実行中のセッションです。セッションは、CPU での動作中、またはリソースが使用可能になるのを待っているときにアクティブになります。例えば、アクティブなセッションでは、ページがメモリに読み込まれるのを待機し、ページからデータを読み取る間に CPU を消費することがあります。

Performance Insights の DBLoad メトリクスは、平均アクティブセッション (AAS) で測定されます。AAS を計算するために、Performance Insights は、毎秒アクティブセッションの数をサンプリングします。特定の時間間隔において、AAS は、アクティブセッションの総数をサンプルの総数で割った値です。2 の AAS 値は、任意の時点で平均して 2 つのセッションがリクエストでアクティブであったことを意味します。

DB ロードの類比は、倉庫内のアクティビティです。倉庫には100 人のワーカーがいるとします。注文が 1 件入ると、ワーカー 1 人がその注文を処理し、他の作業員はアイドル状態になります。100 件以上の注文が入ると、100 人の作業者全員が同時に注文を履行します。ある特定の期間にアクティブになっているワーカーの人数を定期的にサンプリングすれば、アクティブなワーカーの平均数を算出することができます。計算では、平均してN人のワーカーが常に注文を処理していることになります。昨日の平均が 50 人、今日の平均が 75 人だった場合、倉庫のアクティビティレベルが上がったことになります。同様に、セッションアクティビティの増加につれて DB 負荷が増加します。

詳細については、Amazon Aurora ユーザーガイドの「データベースロード」および「Amazon RDS ユーザーガイド」の「データベースロード」を参照してください。

待機イベント

待機イベントは、データベースセッションが処理できるように待機しているリソースを示すデータベースインストルメンテーションの一種です。Performance Insights がアクティブなセッションをカウントしてデータベースの負荷を計算すると、アクティブなセッションが待機する原因となっている待機イベントも記録されます。この手法により、Performance Insights は、DB 負荷に寄与している待機イベントを表示できます。

すべてのアクティブなセッションはCPU 上で実行されているか、待っています。例えば、セッションでのメモリの検索、計算の実行、またはプロシージャコードの実行の際に CPU が消費されます。セッションが CPU を消費していない場合、データファイルの読み取り、または口グの書き込みを待機している可能性があります。セッションのリソース待機時間が長くなると、CPU 上で動作する時間は短くなります。

データベースを調整するとき、多くの場合、セッションが待機しているリソースを見つけようとします。例えば、2 つまたは 3 つの待機イベントが DB 負荷の 90% を占める場合があります。これは、平均して、アクティブなセッションが少数のリソースを待機するためにほとんどの時間を費やしていることを意味します。これらの待機の原因を突き止めることができれば、問題を解決しようとすることができます。

倉庫ワーカーの例を考えてみましょう。本の注文が入ります。ワーカーは注文を処理するのが遅れる可能性があります。例えば、別の作業者が現在棚の在庫を補充している場合や、トロリーが利用でき

ない場合があります。または、注文ステータスを入力するシステムが遅い可能性があります。作業者が待っている時間が長くなればなるほど、注文の履行にかかる時間は長くなります。待機は倉庫ワークフローの自然な部分ですが、待機時間が過大になると、生産性が低下します。同様に、セッションの待機が繰り返されたり長時間になると、データベースのパフォーマンスが低下する可能性があります。

Amazon Aurora の待機イベントの詳細については、Amazon Aurora ユーザーガイドの「Aurora PostgreSQL の待機イベントでのチューニング」および「Aurora MySQL の待機イベントでのチューニング」を参照してください。

他の Amazon RDS データベースの待機イベントの詳細については、Amazon RDS ユーザーガイドの「RDS for PostgreSQL の待機イベントによるチューニング」を参照してください。

DevOpsGuru for RDS の主要な概念

インサイトは、運用アプリケーションで異常または問題のある動作を検出すると DevOpsGuru によって生成されます。インサイトには、リソースの異常が含まれます。異常は、 DevOpsGru によって検出された 1 つ以上の関連メトリクスのうち、予期しないものまたは異常なものを表します。

インサイトの重要度は、高、中, または低です。インサイトの重要度は、インサイトの作成に寄与した最も重要な異常によって決定されます。例えば、インサイト AWS-ECS_MemoryUtilization_and_others に重要度の低い異常と重要度の高い異常が含まれている場合、インサイトの全体的な重要度は高くなります。

Amazon RDS DB インスタンスで Performance Insights がオンになっている場合、RDS の DevOpsGuru は、これらのインスタンスの異常に関する詳細な分析と推奨事項を提供します。異常を識別するために、RDS の DevOpsGuru はデータベースメトリクス値のベースラインを開発します。RDS の DevOpsGuru は、現在のメトリクス値を過去のベースラインと比較します。

トピック

- 事前対応型インサイト
- 事後対応型インサイト
- レコメンデーション

事前対応型インサイト

事前対応型インサイトでは、問題のある動作を発生前に知ることができます。これには異常と共に、問題が大きくなる前に問題に対処するのに役立つレコメンデーションと、関連指標が含まれています。

各事前対応型インサイトページには、1 つの異常に関する詳細が表示されます。

事後対応型インサイト

事後対応型インサイトは、異常な動作を発生時に識別します。これには、現在の問題を理解して対処するのに役立つレコメンデーション、関連するメトリクス、およびイベントを含む異常が含まれています。

因果異常

因果異常は、事後対応型インサイト内のトップレベルの異常です。 DevOpsGuru コンソールの異常詳細ページのプライマリメトリクスとして表示されます。データベース負荷 (DB 負荷) は、RDS の DevOpsGuru の因果異常です。例えば、インサイト AWS-ECS_MemoryUtilization_and_others にはいくつかのメトリクス異常があり、そのうちの 1 つはリソース AWS/RDS のデータベースロード (DB ロード) です。

インサイト内では、異常データベース負荷 (DB 負荷) は、複数の Amazon RDS DB インスタンスで発生することがあります。異常の重要度は、DB インスタンスごとに異なる可能性があります。例えば、1 つの DB インスタンスの重要度が高で、他の DB インスタンスの重要度が低である場合があります。コンソールは、最も高い重要度の異常にデフォルト設定されます。

コンテキスト異常

コンテキスト異常は、事後対応型インサイトに関連するデータベースロード (DB ロード)での所見です。 DevOpsGuru コンソールの異常詳細ページの関連メトリクスセクションに表示されます。各コンテキスト異常は、調査が必要な特定の Amazon RDS パフォーマンス上の問題を記述しています。例えば、因果異常には、次のようなコンテキスト異常が含まれることがあります。

- CPU 容量の超過 — CPU 実行キューまたは CPU 使用率が通常を上回っています。
- データベースメモリ不足 — プロセスに十分なメモリがありません。
- データベース接続のスパイク — データベース接続の数が通常を超えています。

レコメンデーション

各インサイトには、少なくとも 1 つの推奨アクションがあります。次の例は、 DevOpsGuru for RDS によって生成されるレコメンデーションです。

- SQL ID *`list_of_ids`* をチューニングして CPU 使用量を減らすか、インスタンスタイプをアップグレードして CPU 容量を増やします。

- 現在のデータベース接続の関連スパイクを確認します。新しいデータベース接続の頻繁な動的割り当てを回避するために、アプリケーションプールの設定を調整することを検討してください。
- メモリ内ソートや大きな結合など、過剰なメモリ操作を実行する SQL ステートメントを探します。
- SQL ID (*list_of_ids*) の高い I/O 使用量を調査します。
- 大量の一時データを作成するステートメント (大規模なソートを実行するステートメントや大きな一時テーブルを使用するステートメントなど) がないかどうかをチェックします。
- アプリケーションをチェックして、データベースワークロードの増加の原因を確認します。
- MySQL のパフォーマンススキーマを有効にすることを検討してください。
- 実行時間の長いトランザクションをチェックし、コミットまたはロールバックで終了します。
- 指定した時間を超えて「トランザクションのアイドル」状態にあるセッションを終了するように、idle_in_transaction_session_timeout パラメーターを設定します。

DevOpsGuru for RDS の仕組み

DevOpsGuru for RDS はメトリクスデータを収集して分析し、ダッシュボードに異常を公開します。

トピック

- データ収集と分析
- 異常の公開

データ収集と分析

DevOpsGuru for RDS は、Amazon RDS Performance Insights から Amazon RDS データベースに関するデータを収集します。この機能は Amazon RDS DB インスタンスをモニタリングし、メトリクスを収集してチャート内のメトリクスを探索できるようにします。最も重要なパフォーマンスメトリクスは ですDBLoad。RDS の DevOpsGuru は、Performance Insights メトリクスを消費し、それらを分析して異常を検出します。Performance Insights の詳細については、Amazon Aurora ユーザーガイドの「Amazon Aurora の Performance Insights を使用した DB 負荷のモニタリング」またはAmazon RDS ユーザーガイドの「Amazon RDS の Performance Insights を使用した DB 負荷のモニタリング」を参照してください。

DevOpsGuru for RDS は、機械学習と高度な統計分析を使用して、Performance Insights から収集したデータを分析します。 DevOpsGuru for RDS でパフォーマンスの問題が見つかった場合は、次のステップに進みます。

異常の公開

DB 負荷が高いなどのデータベースのパフォーマンス上の問題により、データベースのサービス品質が低下する可能性があります。 DevOpsGuru は RDS データベースで問題を検出すると、ダッシュボードにインサイトを公開します。インサイトには、リソース AWS/RDS の異常値が含まれています。

インスタンスで Performance Insights が有効な場合、異常には問題の詳細な分析が含まれます。DevOpsGuru for RDS では、調査または特定の是正措置を実行することもお勧めします。例えば、特定の高負荷 SQL ステートメントの調査、CPU 容量の増加を検討、 idle-in-transaction セッションを閉じることが推奨されます。

サポートされているデータベースエンジン

DevOpsGuru for RDS は、次のデータベースエンジンでサポートされています。

MySQL 対応 Amazon Aurora

> このエンジンの詳細については、Amazon Aurora ユーザーガイドの「Amazon Aurora MySQL の操作」を参照してください。

PostgreSQL 対応 Amazon Aurora

> このエンジンの詳細については、Amazon Aurora ユーザーガイドの「Amazon Aurora PostgreSQL の操作」を参照してください。

Amazon RDS for PostgreSQL 対応

> このエンジンの詳細については、Amazon RDS ユーザーガイドの Amazon RDS for PostgreSQL を参照してください。

DevOpsGuru は異常を報告し、他のデータベースエンジンの基本的な分析を行います。RDS 用 DevOpsGuru は、Amazon Aurora および RDS for PostgreSQL インスタンスについてのみ詳細な分析とレコメンデーションを提供します。

DevOpsGuru for RDS の有効化

DevOpsGuru for RDS を有効にすると、 DevOpsGru が DB インスタンスなどのリソースの異常を分析できるようになります。Amazon RDS では、RDS DB インスタンスまたは DB クラスターの推奨機能を簡単に見つけて有効化できます。これを実現するために、RDS は Amazon EC2、

DevOpsGuru、IAM などの他の のサービスへの API コールを行います。RDS コンソールがこれらの API 呼び出しを行うと、可視化のために AWS CloudTrail ログに記録されます。

DevOpsGuru が Amazon RDS データベースのインサイトを公開できるようにするには、以下のセクションのタスクを完了します。

トピック

- Amazon RDS DB インスタンスの Performance Insights をオンにする
- DevOpsGuru for RDS のアクセスポリシーの設定
- Amazon RDS DB インスタンスを DevOpsGuru カバレッジに追加する

Amazon RDS DB インスタンスの Performance Insights をオンにする

DevOpsGuru for RDS が DB インスタンスの異常を分析するには、Performance Insights が有効になっていることを確認します。DB インスタンスで Performance Insights が有効になっていない場合、RDS の DevOpsGuru は次の場所で通知します。

ダッシュボード

リソースタイプ別にインサイトを表示すると、 Performance Insights がオンになっていないことが RDS タイルで通知されます。リンクを選択して、Amazon RDS コンソールで Performance Insights を有効にします。

インサイト

ページ下部の [レコメンデーション] セクションで [Enable Amazon RDS Performance Insights] (Amazon RDS Performance Insights の有効化) を選択します。

設定

[Service: Amazon RDS] (サービス: Amazon RDS) セクションで、Amazon RDS コンソールで Performance Insights をオンにするためのリンクを選択します。

詳細については、Amazon Aurora ユーザーガイドの「Performance Insights のオンとオフの切り替え」またはAmazon RDS ユーザーガイドの「Performance Insights のオンとオフの切り替え」を参照してください。

DevOpsGuru for RDS のアクセスポリシーの設定

ユーザーが DevOpsGuru for RDS にアクセスするには、次のいずれかのポリシーからのアクセス許可が必要です。

- AWS マネージドポリシー `AmazonRDSFullAccess`
- 以下のアクションを許可するカスタマーマネージドポリシーです。
  - `pi:GetResourceMetrics`
  - `pi:DescribeDimensionKeys`
  - `pi:GetDimensionKeyDetails`

詳細については、Amazon Aurora ユーザーガイドの「Performance Insights アクセスポリシーの設定」またはAmazon RDS ユーザーガイドの「Performance Insights アクセスポリシーの設定」を参照してください。

Amazon RDS DB インスタンスを DevOpsGuru カバレッジに追加する

DevOpsGuru コンソールまたは Amazon RDS コンソールで Amazon RDS データベースをモニタリングするように DevOpsGuru を設定できます。

DevOpsGuru コンソールには、次のオプションがあります。

- アカウントレベルで DevOpsGuru をオンにします。これがデフォルトです。このオプションを選択すると、 DevOpsGuru は Amazon RDS データベースを含む AWS アカウントAWS リージョンおよび でサポートされているすべてのAWSリソースを分析します。
- RDS の DevOpsGuru のAWS CloudFormationスタックを指定します。

  詳細については、「AWS CloudFormation スタックを使用して DevOps Guru アプリケーション内のリソースを識別する」を参照してください。
- Amazon RDS リソースのタグ付け

  タグは、ユーザーが AWS リソースに割り当てるカスタム属性ラベルです。タグを使用して、アプリケーションを構成する AWS リソースを識別します。その後、タグでインサイトをフィルターして、アプリケーションによって作成されたインサイトのみを表示できます。アプリケーション内の Amazon RDS リソースによって生成されたインサイトのみを表示するには、`Devops-guru-rds` のような値を Amazon RDS リソースタグに追加します。詳細については、「タグを使用した DevOpsGuru アプリケーションのリソースの識別」を参照してください。

  > **Note**
  >
  > Amazon RDS リソースにタグを付けるときは、クラスターではなくデータベースインスタンスにタグを付ける必要があります。

Amazon RDS コンソールから DevOpsGuru モニタリングを有効にするには、「RDS コンソールで DevOps Guru を有効にする」を参照してください。Amazon RDS コンソールから DevOpsGuru を有効にするには、タグを使用する必要があります。タグの詳細については、the section called “タグを使用してアプリケーションのリソースを識別する”を参照してください。

Amazon RDS での異常を分析する

DevOpsGuru for RDS がダッシュボードでパフォーマンスの異常を公開するときは、通常、次のステップを実行します。

1. DevOpsGuru ダッシュボードでインサイトを表示します。RDS の DevOpsGuru は、リアクティブインサイトとプロアクティブインサイトの両方を報告します。

   詳細については、「インサイトの表示」を参照してください。
2. AWS/RDS リソースの異常を表示します。

   詳細については、「事後対応型異常を表示する と 事前対応型の異常を表示する」を参照してください。
3. DevOpsGuru for RDS の推奨事項に応答します。

   詳細については、「レコメンデーションへの対応」を参照してください。
4. DB インスタンスの状態を監視して、解決されたパフォーマンスの問題が再発しないことを確認します。

   詳細については、Amazon Aurora ユーザーガイドの「Amazon Aurora DB クラスターのメトリクスのモニタリング」およびAmazon RDS ユーザーガイドの「Amazon RDS インスタンスのメトリクスのモニタリング」を参照してください。

インサイトの表示

DevOpsGuru コンソールのインサイトページにアクセスして、事後対応型および事前対応型のインサイトを検索します。そこから、リストからインサイトを選択すると、メトリクス、レコメンデーション、インサイトに関する詳細情報を含む詳細ページを表示できます。

インサイトを表示するには

1. https://console.aws.amazon.com/devops-guru/ で Amazon DevOpsGuru コンソールを開きます。
2. ナビゲーションペインを開き、[Insights] (インサイト) を選択します。

3. 事後対応型インサイトを表示するには [事後的] タブを選択し、事前対応型インサイトを表示するには [予測的] を選択します。
4. インサイトの名前を選択し、ステータスと重要度で優先順位を付けます。

   詳細なインサイトページが表示されます。

事後対応型異常を表示する

インサイト内で Amazon RDS リソースの異常を確認できます。事後対応型インサイトのページの「集計メトリクス」セクションでは、異常のリストと対応するタイムラインを表示できます。異常に関連するロググループやイベントに関する情報を表示するセクションもあります。事後対応型インサイトの因果異常にはそれぞれ、異常に関する詳細が記載された対応するページがあります。

RDS 事後対応型異常の詳細な分析を表示する

この段階では、異常をドリルダウンして Amazon RDS DB インスタンスの詳細な分析とレコメンデーションを取得します。

詳細分析は、Performance Insights がオンになっている Amazon RDS DB インスタンスでのみ使用できます。

異常の詳細ページにドリルダウンするには

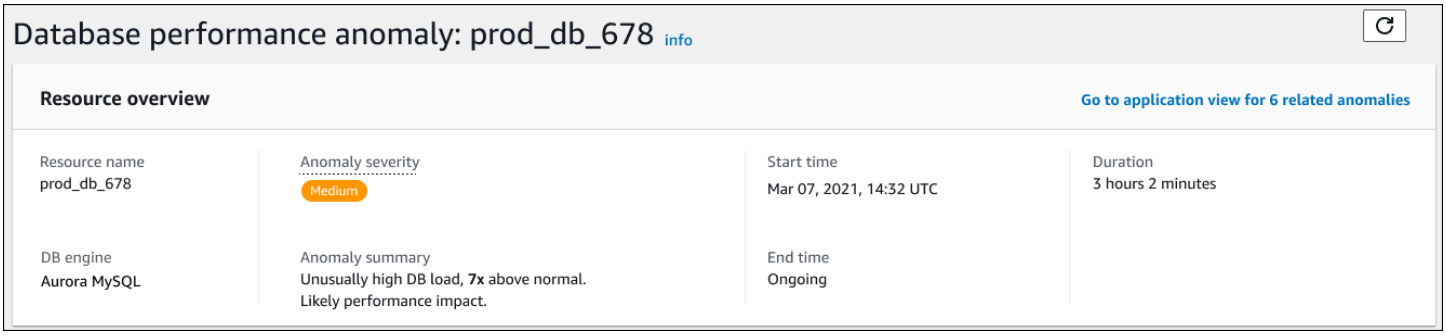
1. インサイトページで、AWS/RDS リソースタイプの集計メトリクスを検索します。
2. [詳細を表示] を選択します。

   異常の詳細ページが表示されます。タイトルは [データベースパフォーマンスの異常] で始まり、名前はリソースを示します。コンソールでは、異常が発生した時期に関係なく、重要性が最も高い異常がデフォルトで設定されます。
3. (オプション) 影響を受けるリソースが複数ある場合は、ページ上部にあるリストから別のリソースを選択します。

以下は、詳細ページのコンポーネントの説明を示しています。

リソースの概要

詳細ページの上部セクションは [Resource overview] (リソースの概要) です。このセクションは、Amazon RDS DB インスタンスで発生するパフォーマンスの異常をまとめたものです。

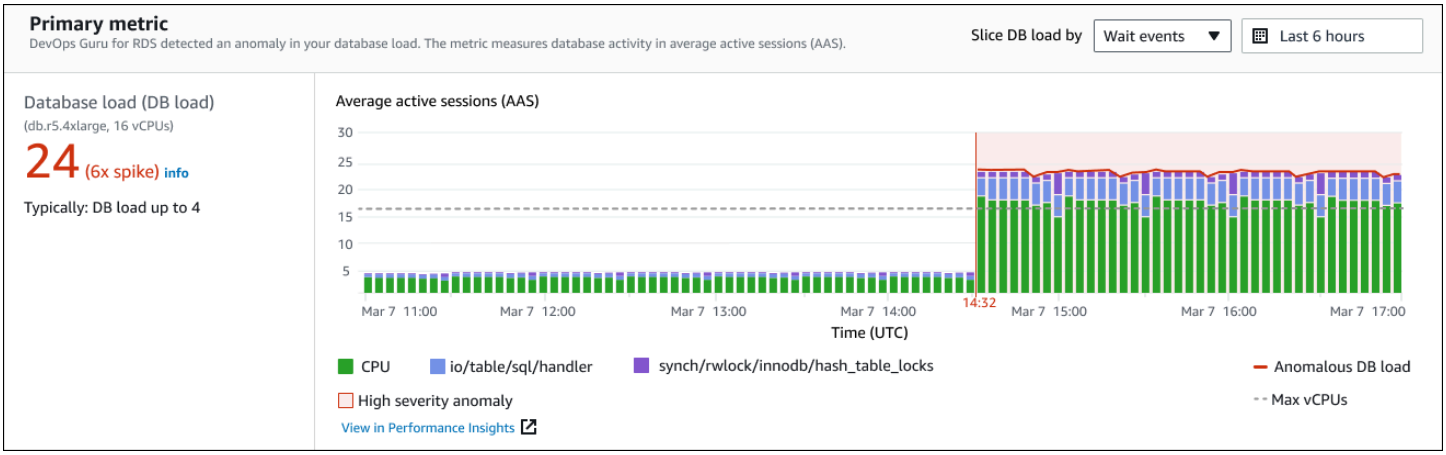


このセクションには、次のフィールドが含まれます。

- Resource name (リソース名) — 異常が発生している DB インスタンスの名前。この例では、リソース名は prod_db_678 です。
- DB engine (DB エンジン) — 異常が発生している DB インスタンスの名前。この例では、エンジンは Aurora MySQL です。
- Anomaly severity (異常の重要性) — インスタンスに対する異常による悪影響の尺度。重要度は、高、中, および低です。
- Anomaly summary (異常の概要) — 問題の簡単な概要。一般的な概要は、Unusually high DB load (異常に高い DB 負荷) です。
- Start time (開始時間) と End time (終了時間) – 異常が開始および終了したとき。終了時間が [Ongoing] (進行中) の場合、異常が引き続き発生しています。
- Duration (期間) — 異常動作の持続時間。この例では、異常は進行中であり、3 時間 2 分間発生しています。

プライマリメトリクス

プライマリメトリクスセクションは、インサイト内の最上位レベルの異常である因果異常の概要が表示されます。因果異常は、DB インスタンスが経験する一般的な問題と考えることができます。



左側のパネルには、問題の詳細が表示されます。この例では、概要には次の情報が含まれます。

- データベース負荷 (DB 負荷) — データベース負荷の問題としての異常の分類。Performance Insights の対応するメトリクスは DBLoad です。このメトリクスは Amazon にも発行されます CloudWatch。
- db.r5.4xlarge — DB インスタンスクラス。vCPUs の数 (この例では 16) は、平均アクティブセッション (AAS) チャートの点線に対応します。
- 24 (6x スパイク) — インサイトで報告された時間間隔中の平均アクティブセッション (AAS) で測定された DB 負荷。したがって、異常期間中の任意の時点で、データベースで平均 24 のセッションがアクティブだったことがわかります。DB 負荷は、このインスタンスの通常の DB 負荷の 6 倍です。
- 一般的に最大 4 の DB 負荷 — 一般的なワークロードにおける AAS 単位で測定された DB 負荷のベースライン。4 の値は、通常の操作中に、データベース上で任意の時点で平均 4 以下のセッションがアクティブであることを意味します。

デフォルトでは、負荷チャートは待機イベントによってスライスされます。つまり、チャート内の各バーについて、最大の色付き領域は、総 DB 負荷に最も寄与している待機イベントを表します。グラフには、課題が開始された時刻 (赤色) が表示されます。バー内で最も多くのスペースを占める待機イベントに注目します。

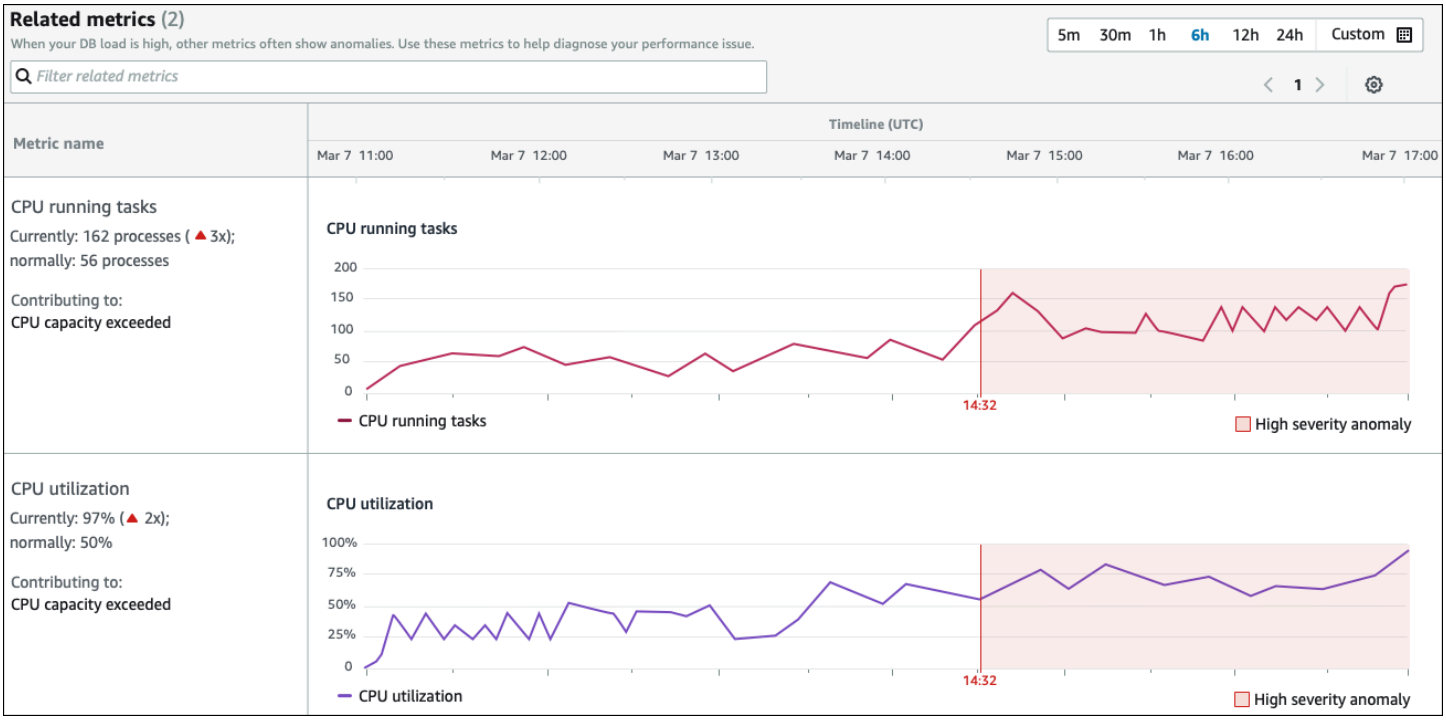
- CPU
- `IO:wait/io/sql/table/handler`

上記の待機イベントは、この Aurora MySQL データベースでは通常よりも多く表示されます。Amazon Aurora の待機イベントを使用してパフォーマンスをチューニングする方法について

は、 Amazon Auroraユーザーガイドの「Aurora MySQL の待機イベントを使用したチューニング」および「Aurora PostgreSQL の待機イベントを使用したチューニング」を参照してください。RDS for PostgreSQL の待機イベントを使用してパフォーマンスを調整する方法については、Amazon RDS ユーザーガイドの「RDS for PostgreSQL の待機イベントを使用したチューニング」を参照してください。

関連メトリクス

[Related metrics] (関連メトリクス) セクションには、因果異常内の特定の検出内容であるコンテキスト異常がリストされます。これらの検出結果は、パフォーマンスの問題に関する追加情報を提供します。



[Related metrics] (関連メトリクス) テーブルには 2 つの列 (メトリクス名およびタイムライン (UTC)) があります。テーブルの個々の行は、特定のメトリクスに対応します。

各行の最初の列には、次の情報が含まれます。

- ## – メトリクスの名前。最初の行は、タスクを実行している CPU としてメトリクスを識別します。
- Currently (現在) — メトリクスの現在の値。最初の行では、現在の値は 162 プロセス (3x) です。
- 通常 – 正常に機能している場合のこのデータベースのこのメトリクスのベースライン。RDS の DevOpsGuru は、1 週間の履歴の 95 パーセンタイル値としてベースラインを計算します。最初の行は、通常 56 のプロセスが CPU で実行されていることを示します。

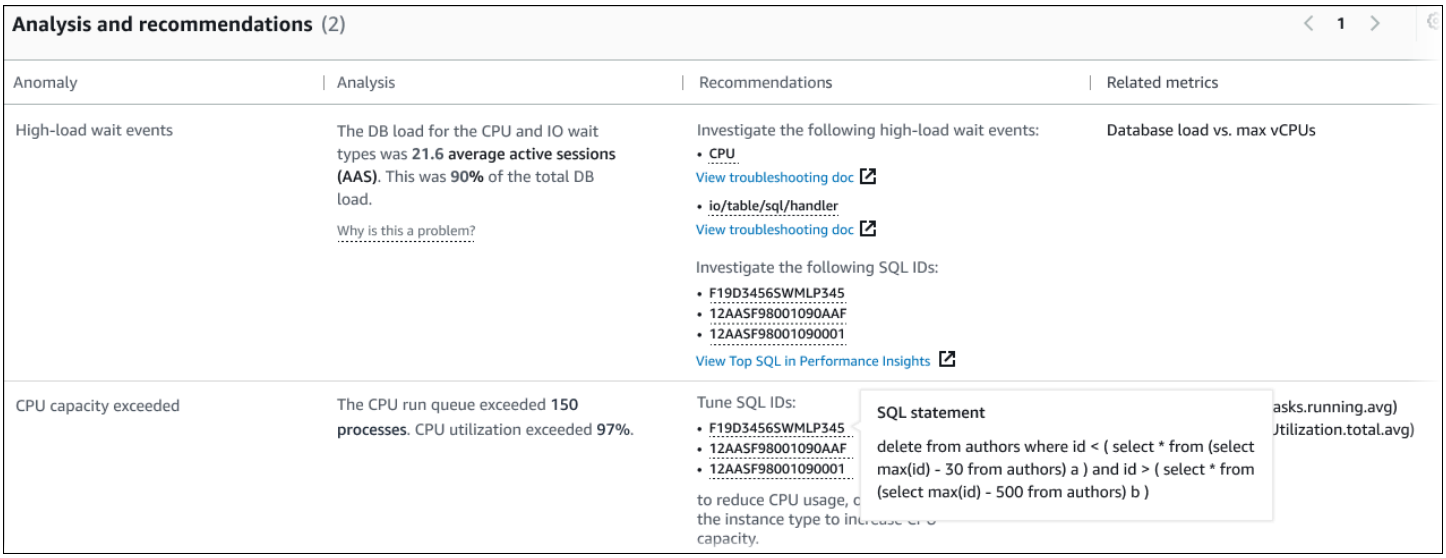
- Contributing to (寄与) — このメトリクスに関連付けられている検出結果。最初の行では、タスクを実行中の CPU メトリクスは、CPU 容量超過異常に関連付けられています。

Timeline (タイムライン) 列には、メトリクスの折れ線グラフが表示されます。影付きの領域は、DevOpsGru for RDS が検出結果を重要度が高いと指定した時間間隔を示します。

分析とレコメンデーション

因果異常が全体的な問題を説明するのに対し、コンテキスト異常は調査を必要とする特定の検出結果を示します。各結果は、関連するメトリクスのセットに対応します。

次の例の [Analysis and recommendations] (分析とレコメンデーション) セクションには、高 DB 負荷異常に 2 つの検出結果があります。



このテーブルには、次の列があります。

- Anomaly (異常) — このコンテキスト異常の全般的な説明。この例では、最初の異常は高負荷待機イベントで、2 番目の異常は CPU 容量超過です。
- Analysis (分析) — 異常の詳細な説明。

  最初の異常では、3 つの待機タイプが DB 負荷の 90% に寄与しています。2 番目の異常では、CPU 実行キューが 150 を超えています。これは、任意の時点で 150 を超えるセッションが CPU 時間を待っていたことを意味します。CPU 使用率は 97% を超えています。つまり、問題が発生している間、CPU は 97% のビジー状態でした。したがって、CPU はほぼ継続的に占有され、平均 150 のセッションが CPU で実行されるのを待機していました。
- Recommendations (レコメンデーション) — 異常に対して提案されたユーザー対応。

最初の異常では、RDS の DevOpsGuru は待機イベント cpuおよび を調査することを推奨していますio/table/sql/handler。これらのイベントに基づいてデータベースのパフォーマンスを調整する方法については、Amazon Aurora ユーザーガイドの「cpu」と「io/table/sql/handler」を参照してください。

2 番目の異常では、RDS の DevOpsGuru では、3 つの SQL ステートメントを調整して CPU 消費を減らすことをお勧めします。リンクにカーソルを合わせると、SQL テキストが表示されます。

- Related metrics (関連メトリクス) — 異常の特定の測定値を示すメトリクス。これらのメトリクスの詳細については、Amazon Aurora ユーザーガイドの「Amazon Aurora のメトリクスのリファレンス」またはAmazon RDS ユーザーガイドの「Amazon RDS のメトリクスのリファレンス」を参照してください。

  最初の異常では、RDS の DevOpsGuru は DB 負荷をインスタンスの最大 CPU と比較することを推奨しています。2 番目の異常では、レコメンデーションは、CPU 実行キュー、CPU 使用率、および SQL 実行率を確認することです。

事前対応型の異常を表示する

インサイト内で Amazon RDS リソースの異常を表示できます。事前対応型インサイトにはそれぞれ 1 つのプロアクティブな異常の詳細が表示されます。事前対応型インサイトページでは、インサイトの概要、異常に関する詳細な指標、将来の問題を防ぐためのレコメンデーションを確認できます。事前対応型異常を確認するには、事前対応型インサイトページにアクセスしてください。

インサイトの概要

インサイト概要セクションには、インサイトが作成された理由の詳細が表示されます。インサイトの重大度、異常の説明、異常が発生した時間枠が表示されます。また、 DevOpsGru によって検出された影響を受けるサービスとアプリケーションの数も一覧表示されます。

メトリクス

[メトリクス] セクションには異常のグラフが表示されます。各グラフには、リソースのベースライン動作によって決まるしきい値と、異常発生時から報告された指標のデータが表示されます。

集約されたリソースに関するレコメンデーション

このセクションでは、報告された問題が大きな問題になる前に軽減するために実行できるアクションを提案します。実行できるアクションは、[推奨されるカスタム変更] 列に表示されます。レコメン

デーションの背後にある理論的根拠は、 DevOps「なぜ Guru がこれを推奨するのですか？」列に表示されます。レコメンデーションへの対応方法の詳細については、the section called “レコメンデーションへの対応” を参照してください。

レコメンデーションへの対応

レコメンデーションは、インサイトの最も重要な部分です。この分析の段階では、ユーザーはパフォーマンスの問題を解決するためのアクションを起こします。通常、次のステップを実行します。

1. 報告されたパフォーマンスの問題が実際の問題を示しているかどうかを判断します。

   場合によっては、問題が予期されていることや問題が良性であることがあります。例えば、テストデータベースに極端な DB 負荷がかかる場合、 DevOpsGuru for RDS は負荷をパフォーマンスの異常として報告します。ただし、テストの結果は予期されているので、この異常を解決する必要はありません。

   問題への対処が必要であると判断した場合は、次のステップに進みます。
2. レコメンデーションを実装するかどうかを決定します。

   レコメンデーションの表では、推奨アクションが列に表示されます。事後対応型インサイトの場合、これは事後対応型異常の詳細ページの [推奨事項] 列です。事前対応型インサイトの場合、これは事前対応型インサイトページの [推奨されるカスタム変更] 列です。

   DevOpsGuru for RDS には、潜在的な問題のあるシナリオをいくつか網羅したレコメンデーションのリストが用意されています。このリストを確認したら、現在の状況に関連性のより高いリコメンデーションを判断し、適用を検討してください。レコメンデーションが状況に合っている場合は、次のステップに進みます。そうでない場合は、残りの手順をスキップし、手動の手法を使用して問題のトラブルシューティングを行います。
3. 推奨されるアクションを実行します。

   DevOpsGuru for RDS では、次のいずれかを実行することをお勧めします。

   - 具体的な是正措置を実行します。

     例えば、RDS の DevOpsGuru では、CPU 容量のアップグレード、アプリケーションプール設定の調整、パフォーマンススキーマの有効化が推奨される場合があります。
   - 問題の原因を調査します。

     通常、RDS の DevOpsGuru では、特定の SQL ステートメントまたは待機イベントを調査することをお勧めします。例えば、レコメンデーションは待機イベント `io/table/sql/handler`

の調査であることがあります。Amazon Aurora ユーザーガイドの「Aurora PostgreSQL の待機イベントのチューニング」または「Aurora MySQL の待機イベントのチューニング」、もしくはAmazon RDS ユーザーガイドの「RDS for PostgreSQL の待機イベントのチューニング」でリストされている待機イベントを検索します。次に、推奨されるアクションを実行します。

> **Important**
>
> 本稼働インスタンスの修正前に、各変更の影響を完全に把握できるように、テストインスタンスでの変更のテストをお勧めします。このようにして、変更の影響を理解します。

DevOpsGuru を使用した非リレーショナルデータベースのモニタリング

DevOpsGuru は、 のベストプラクティスに従ってリソースを設定しておくのに役立つ、非リレーショナルデータベースまたは NoSQL データベースのインサイトを生成できます。例えば、DevOpsGuru は、既存のトラフィックに基づいて将来のニーズを予測することで、キャパシティプランニングを最大限に活用するのに役立ちます。 DevOpsGuru は、設定したよりも少ないリソースを利用しているかどうかを特定し、過去の使用状況に基づいてアプリケーションの可用性を向上させるためのレコメンデーションを提供できます。これにより、不要なコストを削減できます。

キャパシティプランニング以外にも、 DevOpsGuru はスロットリング、トランザクションの競合、条件チェックの失敗、SDK パラメータの改善が必要な分野などの運用上の問題を検出してトラブルシューティングします。通常、データベースは複数の サービスとリソースに接続され、 DevOpsGru はタグ付けまたは AWS CloudFormation 集約に基づいてグループを使用して、分析のためにアプリケーション構造を関連付けることができます。異常には、同じソリューションの影響を受ける複数のリソースが含まれる場合があります。 DevOpsGuru は、さまざまなリソースメトリクス、設定、ログ、およびイベントを関連付けることができます。例えば、 DevOpsGuru は、 Amazon DynamoDB テーブルからデータを読み書きしている可能性のある Lambda 関数からのデータを分析して関連付けることができます。これにより、 DevOpsGuru は複数の関連リソースをモニタリングして異常を検出し、データベースソリューションに役立つインサイトを提供します。

でのデータベースオペレーションのモニタリング Amazon DynamoDB

次の表は、 DevOpsGru が をモニタリングするシナリオとインサイトの例を示しています Amazon DynamoDB。

Amazon DynamoDB ユースケース	例	メトリクス
読み取りおよび書き込みリクエストが多数あるため、 AccountProvisionedReadCapacityUtilization および AccountProvisionedWriteCapacityUtilization の大部分が使用されている場合に検出します。	Amazon DynamoDB 読み込みまたは書き込みリクエストのテーブル消費キャパシティがテーブルレベルの制限に達しています。	AccountProvisionedReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
指定された条件式がデータベースで想定される条件と一致しないために発生した Amazon DynamoDB リクエストで、条件チェックの失敗を検出します。	条件チェックの失敗は、テーブル内の不正なデータ、厳密な条件式、または競合状態によって発生します。	ConditionalCheckFailedRequests

でのデータベースオペレーションのモニタリング Amazon ElastiCache

次の表は、 DevOpsGru が をモニタリングするシナリオとインサイトの例を示しています Amazon ElastiCache。

DevOpsGuru が識別するシナリオ	CloudWatch モニタリングされる メトリクス
Amazon ElastiCache クラスターの需要の変化により、 クラスターが Redis または Memcached のコンピューティング制限に達したときに検出します。	CPUUtilization 、EngineCPUUtilization 、Evictions

CodeGuru Profiler との統合

このセクションでは、Amazon DevOps Guru と Amazon CodeGuru Profiler との統合方法の概要について説明します。CodeGuru Profiler からのリコメンデーションは、DevOps Guru コンソールでインサイトとして表示できます。

Amazon DevOps Guru は、EventBridge 管理ルールを使用して Amazon CodeGuru Profiler と統合されます。CodeGuru Profiler は、EventBridge にイベントを送信します。管理ルールは、デフォルトのイベントバスで送信されるイベントをルーティングします。CodeGuru Profiler からの各インバウンドイベントは、事前対応型の異常レポートです。詳細については、「CodeGuru Profiler による EventBridge の操作」を参照してください。

DevOps Guruは、EventBridge によるインバウンドイベントをサポートしています。イベントは、DevOps Guru が特定したリコメンデーションに変更があったことを示します。CodeGuru Profiler は24時間ごとにハートビートイベントを送信して、イベントの継続性を示します。イベントには、CodeGuru Profiler のリコメンデーションと、コンピュートリソースのメタデータが含まれます。イベントのライフサイクルについては、「Amazon EventBridge イベント」を参照してください。

DevOps Guru をセットアップすると、DevOps Guru は別のサービスからのイベントをルーティングする EventBridge 管理ルールをアカウントに作成します。このルールは DevOps Guru にルーティングされます。インバウンドイベントがあると通知が送信されます。

イベントバスは DevOps Guru などのソースからイベントを受け取り、そのイベントバスに関連付けられたルールにそれらをルーティングします。イベントバスの詳細については、「イベントバス」を参照してください。

一部のパラメータについては、「Amazon EventBridge イベント」を参照してください。

DevOps Guru で CodeGuru Profiler のインサイトを受け取るには、以下が必要です。

- CodeGuru Profiler が有効になっている必要があります。CodeGuru Profiler を有効にする方法については、「CodeGuru Profiler の設定」を参照してください。
- DevOps Guru が有効になっている必要があります。DevOps Guru を有効にする方法については、「DevOps Guru を有効にする」を参照してください。
- CodeGuru Profiler と DevOps Guru の両方で、同じリージョンで同じリソースを監視する必要があります。

AWS リソースを使用したアプリケーションの定義

Amazon DevOps Guru は、カバレッジ境界内にあるリソースをグループ化し、運用上のインサイトのために分析するリソースを指定します。リソースは、AWS CloudFormation スタック内のリソースごと、またはタグ付きのリソースごとにおグループ化されます。DevOps Guru をセットアップするときに、スタックまたはタグを選択します。スタックまたはタグは後で更新することもできます。リソースグループをアプリケーションと考えることをお勧めします。例えば、モニタリングアプリケーションに使用するすべてのリソースが 1 つのスタックで定義されている場合があります。 DevOps Guru が分析するリソースを定義する境界として、データベースアプリケーションで使用するすべてのリソースに同じタグを追加することもできます。コレクション内のすべてのリソースは、この境界内にあります。アカウント内のリソースコレクションに含まれていないリソースは、境界外にあるので分析されません。サポートされているサービスとリソースの詳細については、「Amazon DevOps Guru の料金」を参照してください。

アプリケーションのリソースを含むカバレッジ境界は、3 つの方法で定義できます。

- AWS アカウントとリージョン内のサポートされているすべての AWS リソースを指定します。この場合、アカウントとリージョンがリソースの境界になります。このオプションを使用すると、DevOps Guru はアカウントとリージョン内のすべてのリソースを分析します。1 つのスタックにあるすべてのリソースは 1 つのアプリケーションにグループ化されます。スタックにないリソースは、そのリソースのアプリケーションにグループ化されます。
- AWS CloudFormation スタックを使用してアプリケーションのリソースを指定します。スタックには、AWS CloudFormation を使用して生成されたリソースが含まれます。DevOps Guru で、アカウント内のスタックを選択します。選択した各スタックのリソースは、1 つのアプリケーションにグループ化されます。スタック内のすべてのリソースが DevOps Guru によって分析され、インサイトが取得されます。
- AWS タグを使用してアプリケーションのソースを指定します。1 つの AWS タグには 1 つのキーと 1 つの値 が含まれます。DevOps Guru で、タグを 1 つのタグキーを選択します。オプションとして、キーとついになっている 1 つまたは複数の値を選択します。値を使用して、リソースをアプリケーションにグループ化できます。

詳細については、「DevOps Guru でのAWS分析力バレッジの更新」を参照してください。

トピック

- タグを使用した DevOpsGuru アプリケーションのリソースの識別

- AWS CloudFormation スタックを使用して DevOps Guru アプリケーション内のリソースを識別する

タグを使用した DevOpsGuru アプリケーションのリソースの識別

タグを使用して、Amazon DevOpsGuru が分析するAWSリソースを識別し、選択したタグキーとタグ値でモニタリング用にグループ化するリソースを指定できます。これらの設定は、 DevOpsGru を設定するとき、または分析済みリソースページから分析済みリソースの編集 を選択するときに編集できます。[タグ] を選択したら、「devops-guru-」で始まる特定のタグキーを選択します。アカウント内のすべてのリソースを分析し、タグ値を使用してリソースをグループ化するには、[すべてのアカウントリソース] を選択します。タグ値を使用して DevOpsGuru が分析するリソースを指定するには、特定のタグ値の選択を選択します。

> **Note**
>
> [すべてのアカウントリソース] が選択され、タグ値が存在しない場合、タグキーのないリソースはグループ化され、個別に分析されます。

タグのキーを使用してリソースを識別し、そのキーと一緒に値を使用してリソースをアプリケーションにグループ化します。例えば、リソースにキー devops-guru-applications をタグ付けすると、そのキーを別の値とともに各アプリケーションに対して使用できます。タグのキーと値のペアdevops-guru-applications/database、devops-guru-applications/cicd, および devops-guru-applications/monitoring を使用して、アカウント内の 3 つのアプリケーションを特定できます。各アプリケーションは、同じタグキーと値のペアを含む関連リソースで構成されます。リソースへのタグの追加は、リソースが属する AWS のサービスを使用して行います。詳細については、「AWS リソースに AWS タグを追加する」を参照してください。

アプリケーションのリソースにタグを追加した後、インサイトを生成したリソースのタグでインサイトをフィルターできます。タグを使用してインサイトをフィルターする方法の詳細については、「DevOps Guru インサイトの表示」を参照してください。

サポートされているサービスとリソースの詳細については、「Amazon DevOpsGuru の料金」を参照してください。

トピック

- AWS タグとは

- タグを使用した DevOpsGuru アプリケーションの定義
- DevOpsGuru でのタグの使用
- AWS リソースに AWS タグを追加する

AWS タグとは

タグは、AWS リソースの識別や整理に役立ちます。多くの AWS のサービスではタグ付けがサポートされるため、さまざまなサービスからリソースに同じタグを割り当てて、リソースの関連を示すことができます。例えば、AWS Lambda 関数に割り当てたタグと同じタグを Amazon DynamoDB テーブルリソースに割り当てることができます。タグの使用の詳細については、「タグ付けのベストプラクティス」ホワイトペーパーを参照してください。

各 AWS タグは 2 つの部分で構成されます。

- タグキー (CostCenter、Environment、Project、Secret など)。タグキーでは、大文字と小文字が区別されます。
- タグ値と呼ばれるオプションのフィールド (111122223333、Production、チーム名など)。タグ値を省略すると、空の文字列を使用した場合と同じになります。タグキーと同様に、タグ値でも大文字と小文字が区別されます。

これらは総称的にキーと値のペアと呼ばれます。

タグを使用した DevOpsGuru アプリケーションの定義

タグを使用して Amazon DevOpsGuru アプリケーションを定義するには、アプリケーションを構成するアカウントのAWSリソースにそのタグを追加します。タグには 1 つのキーと 1 つの値が含まれます。DevOpsGuru によって分析される同じキー を持つ各AWSリソースにタグを追加することをお勧めします。リソースをアプリケーションにグループ化するには、タグで別の値を使用します。例えば、キー devops-guru-analysis-boundary を持つタグをカバレッジ境界内のすべての AWS に割り当てることができます。別の値とそのキーをともに使用して、アカウント内のアプリケーションを識別します。これらのアプリケーションには、値 containers、database、および monitoring を使用できます。詳細については、「DevOps Guru でのAWS分析カバレッジの更新」を参照してください。

AWS タグを使用して分析対象のリソースを指定するには、1 つのキーを含むタグを使用できます。タグのキーは任意値とペアにすることができます。該当するキーを含むリソースを運用アプリケーションにグループ化するには、値を使用します。

> **Important**
>
> リソースカバレッジを定義するために使用したタグ内のキーに使用する文字列は、プレフィックス Devops-guru- で始まる必要があります。タグキーは DevOps-Guru-deployment-application または devops-guru-rds-application の可能性があります。キーを作成するとき、キー内の文字の大文字と小文字は任意に選択できます。キーを作成すると、大文字と小文字が区別されます。例えば、 DevOpsGuru は という名前のキーdevops-guru-rdsと という名前のキーを使用しDevOps-Guru-RDS、これらは 2 つの異なるキーとして機能します。アプリケーションで使用できるキーと値のペアは、Devops-Guru-production-application/RDS または Devops-Guru-production-application/containers であることがあります。

DevOpsGuru でのタグの使用

Amazon DevOpsGuru で分析するAWSリソースを識別するAWSタグを指定するか、グループ化するリソースを識別するタグ値を指定します。これらのリソースは、リソースカバレッジの境界です。1 つのキーと値 (複数可) を選択できます。値は必ずしも選択する必要はありません。

タグを選択するには

1. https://console.aws.amazon.com/devops-guru/ で Amazon DevOpsGuru コンソールを開きます。
2. ナビゲーションペインを開き、[設定] を展開します。
3. [Analyzed resources] (分析されたリソース) で [Edit] (編集) を選択します。
4. 選択したタグを含むすべてのリソースを Guru で分析する場合は、「タグ」を選択します。DevOps[キー] を選択し、次のいずれかのオプションを選択します。

   - [すべてのアカウントリソース] — 現在のリージョンとアカウントのすべての AWS リソースを分析します。選択したタグキーを持つリソースは、タグ値ごとにグループ化されます (存在する場合)。このタグキーのないリソースはグループ化され、個別に分析されます。
   - 特定のタグ値を選択する – 選択したキーを持つタグを含むすべてのリソースが分析されます。 DevOpsGuru は、タグの値 によってリソースをアプリケーションにグループ化します。

   タグのキーは、プレフィックス devops-guru- で始まる必要があります。このプレフィックスでは大文字と小文字は区別されません。例えば、有効なキーは DevOps-Guru-Production-Applications です。

5. [保存] を選択します。

AWS リソースに AWS タグを追加する

DevOpsGuru で分析するAWSリソースを識別するAWSタグを指定するときは、リソースが関連付けられているタグを選択します。各リソースが属する AWS サービス、または AWS タグエディタを使用して、リソースにタグを追加できます。

- リソースのサービスを使用してタグを管理するには、コンソール、AWS Command Line Interface、またはリソースが属するサービスの SDK を使用します。例えば、Amazon Kinesis ストリームリソースまたは Amazon CloudFront ディストリビューションリソースにタグを付けることができます。タグ付けできるリソースを含むサービスの例を 2 つ紹介します。DevOpsGuru が分析できるほとんどのリソースはタグをサポートしています。詳細については、「Amazon Kinesis デベロッパーガイド」の「ストリームのタグ付けAmazon Kinesis」および「Amazon CloudFront デベロッパーガイド」の「ディストリビューションのタグ付け」を参照してください。タグを他のタイプのリソースに追加する方法については、該当する AWS のサービスのユーザーガイドまたはデベロッパーガイドを参照してください。

  > **Note**
  >
  > Amazon RDS リソースにタグを付けるときは、クラスターではなくデータベースインスタンスにタグを付ける必要があります。

- AWS タグエディターを使用して、リージョン内のリソースごと、または特定の AWS のサービス内のリソースごとにタグを管理することができます。詳細については、AWS Resource Groups とタグユーザーガイドの「タグエディタ」を参照してください。

リソースにタグを追加するときは、キーのみ、またはキーと値を追加できます。例えば、 DevOps アプリケーションの一部であるすべてのリソースdevops-guru-の キーを使用してタグを作成できます。キー devops-guru- と値 RDS を含むタグを追加し、そのキーと値おペアをアプリケーション内の Amazon RDS リソースにのみ追加できます。これは、アプリケーション内の Amazon RDS リソースのみから生成されたインサイトをコンソールで表示する場合に便利です。

AWS CloudFormation スタックを使用して DevOps Guru アプリケーション内のリソースを識別する

AWS CloudFormation スタックを指定して、DevOps Guru で分析する AWS リソースを指定できます。スタックは、単一のユニットとして管理できる AWS リソースのコレクションです。選択したスタック内のすべてのリソースによって DevOps Guru 境界カバレッジが定義されます。選択したスタックごとに、サポートされているリソースの運用データが異常な動作について分析されます。これらの問題は関連する異常に分類され、インサイトが作成されます。各インサイトには、問題に対処するのに役立つレコメンデーションが含まれています。最大 1,000 個のスタックを指定できます。詳細については、AWS CloudFormation ユーザーガイドの「スタックの操作」と「DevOps Guru での AWS分析カバレッジの更新」を参照してください。

スタックを選択すると、DevOps Guru は即座に追加したリソースの分析を開始します。スタックからリソースを削除すると、そのリソースは分析されなくなります。

DevOps Guru がアカウント内のサポートされているすべてのリソースを分析するように選択した場合 (AWS アカウントとリージョンが DevOps Guru カバレッジ境界である場合)、DevOps Guru は、スタック内のリソースを始めとするアカウント内のサポートされているすべてのリソースについて分析し、インサイトを作成します。スタックにないリソースの異常から作成されたインサイトは、アカウントレベルでグループ化されます。スタックに含まれるリソースの異常から作成されたインサイトは、スタックレベルでグループ化されます。詳細については、「異常行動がインサイトにグループ化される仕組み」を参照してください。

DevOps Guru が分析するスタックを選択する

Amazon DevOps Guru が分析するリソースを含む AWS CloudFormation スタックを選択します。この操作は、AWS Management Console または SDK を使用して行うことができます。

トピック

- DevOps Guru が分析するスタックを選択する (コンソール)
- DevOps Guru が分析するスタックを選択する (DevOps Guru SDK)

DevOps Guru が分析するスタックを選択する (コンソール)

コンソールを使用して AWS CloudFormation コンソールを追加できます。

分析するリソースを含むスタックを選択するには

1. Amazon DevOps Guru コンソール (https://console.aws.amazon.com/devops-guru/) を開きます。
2. ナビゲーションペインを開き、[設定] を選択します。
3. [DevOps Guru analysis coverage] (DevOps Guru 分析カバレッジ) で、[管理] を選択します。
4. 選択したスタック内のリソースを DevOps Guru で分析するには、[CloudFormation stacks] (CloudFormation スタック) を選択して、次のいずれかのオプションを選択します。

   - [すべてのリソース] — アカウント内のスタックにあるすべてのリソースが分析されます。各スタックのリソースは、そのアプリケーションにグループ化されます。スタックにないアカウント内のリソースは分析されません。
   - [Select stacks] (スタックを選択) — DevOps Guru が分析するスタックを選択します。選択した各スタックのリソースは、そのアプリケーションにグループ化されます。スタックの名前を [Find stacks] (スタックの検索) を入力すると、特定のスタックをすばやく特定できます。最大 1,000 個のスタックを選択できます。
5. [保存] を選択します。

DevOps Guru が分析するスタックを選択する (DevOps Guru SDK)

Amazon DevOps Guru SDK を使用して AWS CloudFormation スタックを指定するには、`UpdateResourceCollection` メソッドを使用します。詳細については、Amazon DevOps Guru API リファレンスの「UpdateResourceCollection」を参照してください。

Amazon の使用 EventBridge

Amazon DevOpsGuru は Amazon と統合 EventBridge され、インサイトおよび対応するインサイトの更新に関連する特定のイベントを通知します。 AWS サービスからのイベントは、ほぼリアルタイムで EventBridge に配信されます。どのイベントに興味があるのか、イベントがルールに一致した場合にどのように自動的に実行するアクションをとるのか簡単なルールを指定して書き込みすることができます。自動的に開始できるアクションには、以下の例が含まれます。

- AWS Lambda 関数の呼び出し
- Amazon Elastic Compute Cloud 実行コマンドの呼び出し
- Amazon Kinesis Data Streams へのイベントの中継
- Step Functions ステートマシンのアクティブ化
- Amazon SNS トピックまたは Amazon SQS キューの通知

次の定義済みパターンのいずれかを選択してイベントをフィルタリングしたり、カスタムパターンルールを作成して、サポートされている AWS リソースでアクションを開始したりできます。

- DevOps Guru の新しいインサイトを開く
- DevOps Guru の新しい異常の関連付け
- DevOps Guru Insight 重要度のアップグレード
- DevOps Guru の新しいレコメンデーションが作成されました
- DevOps Guru Insight がクローズされました

DevOpsGuru のイベント

DevOpsGuru からのイベントの例を次に示します。イベントは、ベストエフォートベースで出力されます。イベントパターンの詳細については、「Amazon EventBridgeまたは Amazon EventBridge イベントパターンの開始方法」を参照してください。

DevOpsGuru 新しいインサイトオープンイベント

DevOps Guru が新しいインサイトを開くと、次のイベントが送信されます。

```
{
    "version" : "0",
```

```
    "id" : "08108845-ef90-00b8-1ad6-2ee5570ac6c4",
    "detail-type" : "DevOps Guru New Insight Open",
    "source" : "aws.devops-guru",
    "account" : "123456789012",
    "time" : "2021-11-01T17:06:10Z",
    "region" : "us-east-1",
    "resources" : [ ],
    "detail" : {
      "insightSeverity" : "high",
      "insightDescription" : "ApiGateway 5XXError Anomalous In Stack TestStack",
      "insightType" : "REACTIVE",
      "anomalies" : [
        {
          "startTime" : "1635786000000",
          "id" : "AL41JDFFQPYlZlXD8cpREkAAAAF83HGGgC9TmTr9lbfJ7sCiISlWMeFCbHY_XXXX",
          "sourceDetails" : [
            {
              "dataSource" : "CW_METRICS",
              "dataIdentifiers" : {
                "period" : "60",
                "stat" : "Average",
                "unit" : "None",
                "name" : "5XXError",
                "namespace" : "AWS/ApiGateway",
                "dimensions" : [
                  {
                    "name" : "ApiName",
                    "value" : "Test API Service"
                  },
                  {
                    "name" : "Stage",
                    "value" : "prod"
                  }
                ]
              }
            }
          ]
        }
      ],
      "accountId" : "123456789012",
      "messageType" : "NEW_INSIGHT",
      "insightUrl" : "https://us-east-1.console.aws.amazon.com/devops-guru/#/insight/
reactive/AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "startTime" : "1635786120000",
```

```
      "insightId" : "AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "region" : "us-east-1"
    }
  },
```

重大度の高い新しいインサイトのカスタムサンプルイベントパターン

ルールでは、イベントパターンを使用してイベントを選択し、ターゲットに振り分けます。以下は、DevOps Gru イベントパターンの例です。

```
{
  "source": [
    "aws.devops-guru"
  ],
  "detail-type": [
    "DevOps Guru New Insight Open"
  ],
  "detail": {
    "insightSeverity": [
         "high"
         ]
  }
}
```

DevOps Guru 設定を更新する

次の Amazon DevOps Guru 設定を更新できます。

- DevOps Guru のカバレッジ。アカウント内で分析するリソースを決定します。
- ジョブの通知。重要な DevOps Guru イベントについて通知するために使用する Amazon Simple Notification Service トピックを決定します。
- インサイトを強化する機能。これには、ログの異常検知、暗号化、AWS Systems Manager 統合設定が含まれます。DevOps Guru がログデータを表示するかどうか、追加のセキュリティーキーを使用するかどうか、また新しいインサイトごとに Systems Manager OpsCenter で OpsItem を作成するかどうかを決定します。

トピック

管理アカウント設定を更新する

組織のアカウントに DevOps Guru を設定できます。委任管理者が登録されていない場合は、委任管理者を登録できます。委任管理者の登録の詳細については、「DevOps Guru を有効にする」を参照してください。

DevOps Guru でのAWS分析カバレッジの更新

アカウント内で DevOps Guru で分析するAWSリソースを更新できます。これを行うには、コンソールの [分析されたリソース] で ページに移動し、 [編集] を選択します。詳細については、「分析されたリソースの表示」を参照してください。

DevOps Guru の通知を更新する

重要な Amazon DevOps Guru イベントについて通知するために使用する Amazon Simple Notification Service トピックを設定します。自分の AWS アカウントの既存のトピック名のリストから選択する、DevOps Guru によってアカウントに作成される新しいトピックの名前を入力する、または使用しているリージョンの任意の AWS アカウントの既存のトピックの Amazon リソースネーム (ARN) を入力することができます。自分のアカウントにないトピックの ARN を指定する場合は、IAM ポリシーを追加して、DevOps Guru がそのトピックにアクセスするための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、「Amazon SNS トピックへの許可」を参照してください。最大2つのトピックを追加できます。

DevOps Guru は、次の更新に関する通知を送信します。

- 新しいインサイトの作成。
- インサイトへの新しい異常の追加。
- インサイトの重要度のアップグレード (Low または Medium から High)。
- インサイトのステータスの変更 (進行中から解決済み) 。
- インサイトに関するレコメンデーションの識別。

DevOps Guru アカウントにリソースを追加しようとしたときに、選択した AWS CloudFormation スタックまたはタグキーが無効である場合も、DevOps Guru は通知を送信します。

課題のあらゆる種類の更新について Amazon SNS 通知を受信するか、課題が開かれた、クローズされた、または重要度が変化したときにのみ Amazon SNS 通知を受信するかを選択できます。デフォルトでは、すべての更新に関する通知が届きます。

通知を更新するには、まず通知ページに移動し、Amazon SNS 通知トピックの設定を追加、削除、または更新するかどうかを選択します。

トピック

- DevOps Guru コンソールに表示される通知設定に移動します
- DevOps Guru コンソールに Amazon SNS 通知トピックを追加する
- DevOps Guru コンソールの Amazon SNS 通知トピックを削除する
- Amazon SNS 通知設定を更新する
- Amazon SNS トピックに追加されたアクセス許可

DevOps Guru コンソールに表示される通知設定に移動します

通知を更新するには、まず通知設定セクションに移動する必要があります。

通知設定セクションに移動するには、「通知設定」セクションに移動します。

1. Amazon DevOps Guru コンソール (https://console.aws.amazon.com/devops-guru/) を開きます。
2. ナビゲーションペインで [設定] を選択します。

   設定ページには、設定済みの Amazon SNS トピックに関する情報が記載された [通知] セクションがあります。

DevOps Guru コンソールに Amazon SNS 通知トピックを追加する

Amazon SNS 通知トピックを DevOps Guru コンソールに追加するには

1. the section called “DevOps Guru コンソールに表示される通知設定に移動します”.
2. [Add notification] (通知を追加) をクリックします。
3. Amazon SNS トピックを追加するには、次のいずれかを実行します。

   - [メールを使用して新しい SNS トピックを生成] を選択します。次に、[メールアドレスを指定] から、通知を受け取るメールアドレスを入力します。追加のメールアドレスを入力するには、[新しい E メールを追加] を選択します。
   - [既存の SNS トピックを使用] を選択します。[AWS アカウントのトピックを選択] で、使用するトピックを選択します。
   - 別のアカウントの既存のトピックを指定するには、[既存の SNS トピック ARN を使用します] を選択します。[Enter an ARN for a topic] (トピックの ARN を入力) にトピック ARN を入力します。ARN はトピックの Amazon リソースネームです。別のアカウントのトピックを指定できます。別のアカウントのトピックを使用する場合は、トピックにリソースポリシーを追加する必要があります。詳細については、「Amazon SNS トピックへの許可」を参照してください。
4. [保存] を選択します。

DevOps Guru コンソールの Amazon SNS 通知トピックを削除する

DevOps Guru コンソールから Amazon SNS トピックを削除するには

1. the section called “DevOps Guru コンソールに表示される通知設定に移動します”.
2. [既存のトピックを選択] を選択します。
3. ドロップダウンメニューから、削除するトピックを選択します。
4. [削除] を選択します。
5. [保存] を選択します。

Amazon SNS 通知設定を更新する

DevOps Guru の Amazon SNS 通知トピックには、2種類の通知設定があります。すべての重要度レベルの通知を受信するか、重大度レベルが[高] と[中] の通知のみを受信するかを選択できます。通知を受け取ることも、すべての更新通知を受け取ることも、一部の更新のみ通知を受け取るように選択することもできます。

問題のあらゆる種類の更新について Amazon SNS 通知を受信するように選択すると、DevOps Guru は次の更新に関する通知を送信します。

- 新しいインサイトの作成。
- インサイトへの新しい異常の追加。
- インサイトの重要度のアップグレード (Low または Medium から High)。
- インサイトのステータスの変更 (進行中から解決済み) 。
- インサイトに関するレコメンデーションの識別。

デフォルトでは、重要度レベルが「高」と「中」の通知のみを受け取り、あらゆる種類の更新に関する通知を受け取ります。

Amazon SNS 通知トピックの通知設定を更新するには

1. the section called “DevOps Guru コンソールに表示される通知設定に移動します”.
2. [既存のトピックを選択] を選択します。
3. ドロップダウンメニューから、更新したいトピックを選択します。
4. [すべての重要度レベル] を選択して高、中、および低重要度レベルの通知を受信するか、[高と中のみ] を選択して高および中重要度レベルの通知を受信します。

5. [インサイトのすべての更新について通知する] を選択するか、[インサイトが開かれたときまたは閉じられたとき、または重大度レベルが低または中から高に変更されたときに通知する] を選択します。
6. [保存] を選択します。

Amazon SNS トピックに追加されたアクセス許可

Amazon SNS トピックは、AWS Identity and Access Management (IAM) リソースポリシーに含まれるリソースです。ここでトピックを指定すると、DevOps Guru はリソースポリシーに次のアクセス許可を追加します。

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

DevOps Guru がトピックを使用して通知を公開するには、これらのアクセス許可が必要です。トピックに対するこれらのアクセス許可を使用しない場合は、それらのアクセス許可を安全に削除できます。トピックはアクセス許可を削除する前と同じように機能し続けます。ただし、これらのアクセス許可を削除すると、DevOps Guru はトピックを使用して通知を生成できなくなります。

DevOps Guru 通知をフィルターする

DevOps Guru の通知は、Amazon SNS サブスクリプションフィルタポリシーによって、the section called “Amazon SNS 通知設定を更新する” または Amazon SNS サブスクリプションフィルタポリシーを使用してフィルターできます。

トピック

Amazon SNS サブスクリプションフィルターポリシーを使用して通知をフィルターする

Amazon Simple Notification Service (Amazon SNS) サブスクリプションフィルターポリシーを作成して、Amazon DevOps Guru から受け取る通知の数を減らすことができます。

フィルターポリシーを使用して、受信する通知のタイプを指定します。次のキーワードを使用して Amazon SNS メッセージをフィルターできます。

- `NEW_INSIGHT` — 新しいインサイトが作成されたときに通知を受け取ります。
- `CLOSED_INSIGHT` — 既存のインサイトが閉じられたときに通知を受け取ります。
- `NEW_RECOMMENDATION` — インサイトから新しいレコメンデーションが作成されたときに通知を受け取ります。
- `NEW_ASSOCIATION` — インサイトから新しい異常が検出されたときに通知を受け取ります。
- `CLOSED_ASSOCIATION` — 既存の異常が閉じられたときに通知を受け取ります。
- `SEVERITY_UPGRADED` — インサイトの重要度がアップグレードされたときに通知を受け取ります。

Amazon SNS サブスクリプションフィルターポリシーを作成する方法については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS サブスクリプションフィルターポリシー」を参照してください。フィルターポリシーで、ポリシーの `MessageType` でキーワードの 1 つを指定します。例えば、Amazon SNS トピックがインサイトから新しい異常が検出された場合にのみ通知を配信するフィルターは次のようになります。

```
{
  "MessageType":["NEW_ ASSOCIATION"]
}
```

フィルター処理された Amazon DevOps Guru の Amazon SNS 通知の例

フィルターポリシーを使用して Amazon SNS トピックからの Amazon Simple Notification Service (Amazon SNS) 通知の例を次に示します。MessageType は NEW_ASSOCIATION に設定されているので、インサイトから新しい異常が検出された場合にのみ通知を送信します。


```
{
      "accountId": "123456789012",
      "region": "us-east-1",
      "messageType": "NEW_ASSOCIATION",
      "insightId": "ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-Function duration due to increased number of invocations",
      "insightUrl": "https://us-east-1.console.aws.amazon.com/devops-guru/insight/
reactive/ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightType": "REACTIVE",
      "insightDescription": "At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-Function had\n an increased duration anomaly possibly caused by
 the Lambda function invocation increase. DevOps Guru has detected this is a repeated
 insight. DevOps Guru treats repeated insights as 'Low Severity'.",
      "startTime": 1628767500000,
      "startTimeISO": "2023-03-29T22:00:00Z",
      "anomalies": [
        {
          "id": "AG2n8ljW74BoI1CHu-m_oAgAAAF7Ohu24N4Yro69ZSdUtn_alzPH7VTpaL30JXiF",
          "startTime": 1628767500000,
          "startTimeISO": "2023-03-29T22:00:00Z",
          "openTime": 1680127740000,
          "openTimeISO": "2023-03-29T22:09:00Z",
          "sourceDetails": [
            {
              "dataSource": "CW_METRICS",
              "dataIdentifiers": {
                "namespace": "AWS/SQS",
                "name": "ApproximateAgeOfOldestMessage",
                "stat": "Maximum",
                "unit": "None",
                "period": "60",
                "dimensions": "{\"QueueName\":\"FindingNotificationsDLQ\"}"
              }
            }
          ],
          "associatedResourceArns":[
```

```
            "arn:aws:sns:us-east-1:123456789012:DevOpsGuru-insights-sns"
          ]
        }
      ],
      "resourceCollection":{
      "cloudFormation":{
         "stackNames":[
            "CapstoneNotificationPublisherEcsApplicationInfrastructure"
          ]
        }
      }
}
```

DevOps Guru での AWS Systems Manager 統合を更新する

AWS Systems Manager OpsCenter で新しいインサイトごとに OpsItem を作成できます。OpsCenter は、運用作業項目 (OpsItems) の表示、調査、レビューを行うことのできる一元的なシステムです。インサイトの OpsItems は、各インサイトの作成をトリガーした異常な動作に対処する作業を管理するのに役立ちます。詳細については、AWS Systems Manager ユーザーガイドの「AWS Systems Manager OpsCenter」と「OpsItem の使用」を参照してください。

> **Note**
>
> OpsItem のタグフィールドのキーまたは値を変更すると、DevOps Guru はその OpsItem を更新することができません。例えば、OpsItem のタグを `"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"` から変更すると、DevOps Guru はその OpsItem を更新できません。

Systems Manager の統合を管理するには

1. Amazon DevOps Guru コンソール (https://console.aws.amazon.com/devops-guru/) を開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [AWS Systems Manager integration] (AWS Systems Manager 統合) で、[Enable DevOps Guru to create an AWS OpstItem in OpsCenter for each insight] (DevOps Guru で各インサイトの AWS OpstItem を OpsCenter 作成する) を選択して、新しい各インサイトに OpsItem を作成します。このオプションを選択しない場合、新しいインサイトごとに OpsItem は作成されません。

アカウントで作成された OpsItems に対して請求が発生します 詳細については、AWS Systems Manager 料金を参照してください。

DevOps Guru でのログ異常検出を更新する

ログ異常検出設定を管理するには

1. Amazon DevOps Guru コンソール (https://console.aws.amazon.com/devops-guru/) を開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [ログ異常検出] で、[インサイトに関連するログデータを表示する権限を DevOps Guru に付与してログ異常検出を有効にする] を選択し、DevOps Guru にインサイトに関連するログデータを表示させます。

DevOps Guru の暗号化設定を更新する

暗号化設定を更新して、AWS 所有キーまたは AWS KMS カスタマーマネージドキーを使用できます。既存のカスタマーマネージド AWS KMS キーから新しいカスタマーマネージド AWS KMS キーに切り替えると、DevOps Guru は新しいキーを使用して新しく取り込まれたメタデータの暗号化を自動的に開始します。履歴データは、以前に設定したカカスタマーマネージド AWS KMS キーで暗号化されたままになります。

> **Note**
>
> 許可を取り消すか、前の AWS KMS キーを無効にするか削除すると、DevOps Guru はこのキーで暗号化されたデータにアクセスできなくなり、読み取り操作の実行時に `AccessDeniedException` が表示される可能性があります。

暗号化設定を管理するには

1. Amazon DevOps Guru コンソール (https://console.aws.amazon.com/devops-guru/) を開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [暗号化] セクションで[暗号化の編集] を選択します。

4. データを保護するために使用したい暗号化の種類を選択します。デフォルトの AWS 所有キーを使用して、既存のカスタマーマネージドキーを選択することも、新しいカスタマーマネージド AWS KMS キーを作成して使用することもできます。
5. [保存] を選択します。

暗号化は DevOps Guru のセキュリティの重要な部分です。詳細については、「the section called “データ保護”」を参照してください。

通知の表示

DevOpsGuru にはさまざまなタイプの通知があります。

トピック

このページのセクションでは、各タイプの通知の例を示しています。

新しいインサイト

新しいインサイトの通知には、次の情報が含まれます。


```
{
   "accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-4",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"DevOps Guru has detected this is a repeated insight. DevOps
 Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680148920000,
   "startTimeISO": "2023-03-30T04:02:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime": 1680148800000,
         "startTimeISO": "2023-03-30T04:00:00Z",
```

```
         "openTime": 1680148920000,
         "openTimeISO": "2023-03-30T04:02:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
                  "name":"ApproximateAgeOfOldestMessage",
                  "namespace":"AWS/SQS",
                  "period":"60",
                  "stat":"Maximum",
                  "unit":"None",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        },
   }
}
```

クローズドインサイト

クローズドインサイトの通知には、次の情報が含まれます。

```
{
"accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"CLOSED_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "DynamoDB table writes are under utilized in mock-stack",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription":"DynamoDB table writes are under utilized",
```

```
    "insightSeverity":"medium",
    "startTime": 1670612400000,
    "startTimeISO": "2022-12-09T19:00:00Z",
    "endTime": 1679994000000,
    "endTimeISO": "2023-03-28T09:00:00Z",
    "anomalies":[
       {
          "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
          "startTime": 1665428400000,
          "startTimeISO": "2022-10-10T19:00:00Z",
          "endTime": 1679986800000,
          "endTimeISO": "2023-03-28T07:00:00Z",
          "openTime": 1670612400000,
          "openTimeISO": "2022-12-09T19:00:00Z",
          "closeTime": 1679994000000,
          "closeTimeISO": "2023-03-28T09:00:00Z",
          "description":"Empty receives while messages are available",
          "anomalyResources":[
             {
                "type":"AWS::SQS::Queue",
                "name":"SampleQueue"
             }
          ],
          "sourceDetails":[
             {
                "dataSource":"CW_METRICS",
                "dataIdentifiers":{
                "name":"NumberOfEmptyReceives",
                   "namespace":"AWS/SQS",
                   "period":"60",
                   "stat":"Sum",
                   "unit":"COUNT",
                   "dimensions":"{\"QueueName\":\"SampleQueue\"}"
                }
             }
           ],
         "associatedResourceArn": [
             "arn:aws:sqs:us-east-1:123456789101:SampleQueue"
         ]
       }
    ],
    "resourceCollection":{
         "cloudFormation":{
             "stackNames":[
```

```
                "SampleApplication"
            ]
        }
    }
}
```

新しいアソシエーション

新しいアソシエーションの通知には、次の情報が含まれます。

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_ASSOCIATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-GetOneFunction duration due to increased number of
 invocations",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-GetOneFunction had\nan increased duration anomaly possibly
 caused by the Lambda function invocation increase. DevOps Guru has detected this is a
 repeated insight. DevOps Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680127200000,
   "startTimeISO": "2023-03-29T22:00:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime":1672945500000,
         "startTimeISO": "2023-03-29T22:00:00Z",
         "openTime": 1680127740000,
         "openTimeISO": "2023-03-29T22:09:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
               "namespace":"AWS/SQS",
                  "name":"ApproximateAgeOfOldestMessage",
                  "stat":"Maximum",
                  "unit":"None",
```

```
                  "period":"60",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

新しいリコメンデーション

新しいリコメンデーションの通知には、次の情報が含まれます。

```
{
   "accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"NEW_RECOMMENDATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "Recreation of AWS SDK Service Clients",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription": "Usually for a given service you can create one [AWS SDK
 service client](https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/creating-
clients.html) and reuse that client across your entire service.\n\nWhen instead you
 create a new AWS SDK service client for each call (e.g. for DynamoDB) it\u0027s
 generally a waste of CPU time.",
   "insightSeverity":"medium",
   "startTime": 1680125893576,
   "startTimeISO": "2023-03-29T21:38:13.576Z",
   "recommendations":[
      {
         "name":"Tune Availability Zones of your Lambda Function",
```

```
        "description":"Based on your configurations, we recommend that you set
 SampleFunction to be deployed in at least 3 Availability Zones to maintain Multi
 Availability Zone Redundancy.",
        "reason":"Lambda Function SampleFunction is currently only deployed to 2
 unique Availability zones in a region with 7 total Availability zones.",
        "link":"https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html",
        "relatedAnomalies":[
           {
              "sourceDetails":{
                   "cloudWatchMetrics":null
              },
              "resources":[
                 {
                    "name":"SampleFunction",
                    "type":"AWS::Lambda::Function"
                 }
              ],
              "associatedResourceArns": [
                 "arn:aws:lambda:arn:123456789101:SampleFunction"
              ]
           }
        ]
     }
  ],
  "resourceCollection": {
       "cloudFormation": {
       "stackNames":[
           "SampleApplication"
        ]
     }
  }
}
```

重要度のアップグレード

重要度のアップグレードの通知には、次の情報が含まれます。

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"SEVERITY_UPGRADED",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-11",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
   "insightType":"REACTIVE",
   "insightDescription": "DevOps Guru has detected this is a repeated insight. DevOps
 Guru will treat future occurrences of this insight as 'Low Severity' for the next 7
 days.",
   "insightSeverity":"high",
   "startTime": 1680127320000,
   "startTimeISO": "2023-03-29T22:02:00Z",
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

リソース検証の失敗

AWS CloudFormation スタックとAWSタグを使用して、 DevOpsGru で分析するAWSリソースをフィルタリングして識別できます。 DevOpsGuru がリソースを識別するために無効なスタックまたはタグを選択すると、DevOpsGru はSELECTED_RESOURCE_FILTER_VALIDATION_FAILURE通知を作成します。これは、指定したタグまたはスタック名にリソースが関連付けられていない場合に発生する可能性があります。 DevOpsGuru フィルタリング方法を最大限に活用するには、リソースが関連付けられているスタックとタグを選択します。

```
{
    "accountId":"123456789101",
    "region":"eu-west-1",
    "messageType":"SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE",
    "ResourceFilterType": "Tags",
    "InvalidResourceNames": [
         "Devops-Guru-tag-key-tag-value"
    ],
    "awsInsightSource": "aws.devopsguru"
}
```

DevOps Guru が分析したリソースの表示

DevOps Guru は、ListMonitoredResourcesアクションを使用して分析中のリソース名とそのアプリケーション境界のリストを提供します。この情報は、Amazon CloudWatch、AWS CloudTrail、および DevOps Guru のAWSサービスにリンクされた役割を使用するその他のサービスから収集されます。

ユーザーがAWS Lambdaや Amazon RDS などの他のサービスの API にアクセスする明示的な権限を持っていなくても、ListMonitoredResourcesアクションが許可されている限り、DevOps Guru はそのサービスのリソースリストを提供することに注意してください。

トピック

- DevOps Guru でのAWS分析カバレッジの更新
- 分析されたリソースビューをユーザーから削除します。

DevOps Guru でのAWS分析カバレッジの更新

アカウント内で DevOps Guru で分析するAWSリソースを更新できます。分析対象のリソースが DevOps Guru カバレッジ境界を構成します。境界を指定すると、リソースがアプリケーションにグループ化されます。4 つの境界カバレッジオプションがあります。

- アカウント内のサポートされているすべてのリソースを DevOps Guru で分析します。アカウント内の 1 つのスタックにあるすべてのリソースは 1 つのアプリケーションにグループ化されます。アカウントに複数のスタックがある場合、各スタックのリソースがそれぞれのアプリケーションを構成します。アカウント内の各スタックのすべてのリソースは、それぞれのアプリケーションにグループ化されます。
- リソースを定義する AWS CloudFormation スタックを選択してリソースを指定します。この場合、DevOps Guru は選択したスタックで指定されたすべてのリソースを分析します。選択したスタックによってアカウント内のリソースが定義されていない場合、そのリソースは分析されません。詳細については、AWS CloudFormation ユーザーガイドの「スタックの操作」と「DevOpsGuru のカバレッジを決定する」を参照してください。
- AWSタグを使用してリソースを指定します。DevOps Guru は、アカウントとリージョンのすべてのリソース、または選択したタグを含むすべてのリソースを分析します。リソースは、選択したタグ値に基づいてグループ化されます。詳細については、「タグを使用した DevOpsGuru アプリケーションのリソースの識別」を参照してください。

- リソース分析による料金が発生することを回避するために、リソースを分析しないように指定します。

> **Note**
>
> カバレッジを更新してリソースの分析を停止した場合、過去に DevOps Guru によって生成された既存のインサイトを確認すると、若干の料金が発生することがあります。この料金は、インサイト情報を取得および表示するために使用される API コールに関連付けられたものです。詳細については、「Amazon DevOps Guru の料金」を参照してください。

DevOps Guru は、サポートされているサービスに関連付けられているすべてのリソースをサポートします。サポートされているサービスとリソースの詳細については、「Amazon DevOps Guru の料金」を参照してください。

DevOps Guru 分析カバレッジを管理するには

1. Amazon DevOps Guru コンソール (https://console.aws.amazon.com/devops-guru/) を開きます。
2. ナビゲーションペインで、 [分析されたリソース] を展開します。
3. [Edit] (編集) を選択します。
4. 以下のカバレッジオプションのいずれかを選択します。

   - DevOps Guru で AWS アカウントとリージョンのすべてのリソースを分析する場合、[All account resources] (すべてのアカウントリソース) を選択します。このオプションを選択した場合、AWS アカウントがリソース分析カバレッジ境界になります。アカウント内の各スタックのすべてのリソースは、それぞれのアプリケーションにグループ化されます。スタックにない残りのリソースは、そのアプリケーションにグループ化されます。
   - 選択したスタック内のリソースを DevOps Guru で分析するには、[CloudFormation stacks] (CloudFormation スタック) を選択して、次のいずれかのオプションを選択します。
     - [すべてのリソース] — アカウント内のスタックにあるすべてのリソースが分析されます。各スタックのリソースは、そのアプリケーションにグループ化されます。スタックにないアカウント内のリソースは分析されません。
     - [Select stacks] (スタックを選択) — DevOps Guru が分析するスタックを選択します。選択した各スタックのリソースは、そのアプリケーションにグループ化されます。スタックの名前を [Find stacks] (スタックの検索) を入力すると、特定のスタックをすばやく特定できます。最大 1,000 個のスタックを選択できます。

詳細については、「AWS CloudFormation スタックを使用して DevOps Guru アプリケーション内のリソースを識別する」を参照してください。

- 選択したタグを含むすべてのリソースを DevOps Guru で分析する場合、[タグ] を選択します。[キー] を選択し、次のいずれかのオプションを選択します。
  - [すべてのアカウントリソース] — 現在のリージョンとアカウントのすべての AWS リソースを分析します。選択したタグキーを持つリソースは、タグ値ごとにグループ化されます (存在する場合)。このタグキーのないリソースはグループ化され、個別に分析されます。
  - [特定のタグ値を選択する] — 選択したキーを持つタグを含むすべてのリソースが分析されます。DevOps Guru は、タグの値によってリソースをアプリケーションにグループ化します。

  タグのキーは、プレフィックス `devops-guru-` で始まる必要があります。このプレフィックスでは大文字と小文字は区別されません。例えば、有効なキーは `DevOps-Guru-Production-Applications` です。詳細については、「タグを使用した DevOpsGuru アプリケーションのリソースの識別」を参照してください。
- DevOps Guru でいずれのリソースも分析しない場合は、[None] (なし) を選択します。このオプションを選択すると DevOps Guru が無効になり、リソース分析による料金の発生が停止します。

5. [保存] を選択します。

分析されたリソースビューをユーザーから削除します。

ユーザーが Lambda や Amazon RDS などの別のサービスの API にアクセスする明示的な権限を持っていなくても、`ListMonitoredResources`アクションが許可されている限り、DevOps Guru はそのサービスからのリソースのリストを提供します。この動作を変更するには、AWS IAM ポリシーを更新してこのアクションを拒否できます。

```
{
            "Sid": "DenyListMonitoredResources",
            "Effect": "Deny",
            "Action": [
                "devops-guru:ListMonitoredResources"
            ]
}
```

DevOps Guru のベストプラクティス

以下のベストプラクティスは、Amazon DevOps Guru によって検出された異常な動作を理解、診断、および修正するために役立ちます。ベストプラクティスと「DevOps Guru コンソールに表示されるインサイト」を使用して、DevOps Guru によって検出されたオペレーションの問題に対処できます。

- 最初に、インサイトのタイムラインビューでハイライトされたメトリクスを確認します。これらのメトリクスは、問題の重要な指標であることがあります。
- Amazon CloudWatch を使用して、インサイト内でハイライトされた最初のメトリクスの直前に発生したメトリクスを表示し、動作がいつどのように変更されたかを特定します。これは、問題を診断して解決するために役立ちます。
- Amazon RDS リソースについては、Performance Insights のメトリクスを参照してください。カウンターメトリクスをデータベースの負荷に関連付けることで、パフォーマンスの問題に関する詳細情報を取得できます。詳細については、「Analyzing performance anomalies with DevOps Gurufor Amazon RDS」を参照してください。
- 同じメトリクスの複数のディメンションは、異常になることがあります。問題を深く理解するには、グラフビューのディメンションを確認してください。
- インサイトのイベントセクションで、インサイトが作成された頃に発生したデプロイイベントまたはインフラストラクチャイベントを確認します。インサイトの異常な動作が発生したときに発生したイベントを知ることは、問題の理解と診断に役立ちます。
- 手掛かりのためのインサイトとして、オペレーションシステム内でほぼ同じ時期に発生したチケットを探します。
- インサイトでレコメンデーションを読み、レコメンデーションのリンクにアクセスします。多くの場合、問題の診断と解決に役立つトラブルシューティングのステップが提供されています。
- すでに問題を解決している場合を除き、解決済みのインサイトを無視しないでください。解決されている場合でも、1 日 1 回は新しいインサイトを確認してください。できるだけ多くのインサイトの背後にある根本原因を理解するようにしてください。システムの問題の兆候である可能性のあるパターンを探してください。システムの問題が未解決のままにしておくと、将来的により深刻な問題が発生する可能性があります。問題をその場で修正しておくと、将来における深刻なインシデントを防止するのに役立ちます。

Amazon DevOpsGuru のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、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、およびクラウド内で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 クラウドで AWS サービスを実行するインフラストラクチャを保護する責任 AWS を担います。 AWS また、 は、お客様が安全に使用できるサービスも提供します。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。Amazon DevOpsGuru 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、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」「コンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ — 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、 DevOpsGuru の使用時に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように DevOpsGuru を設定する方法について説明します。また、 DevOpsGru リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

Amazon DevOpsGuru でのデータ保護

責任 AWS 共有モデル、Amazon DevOpsGuru でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての 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記事「AWS 責任共有モデルおよび GDPR」を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、または SDK を使用して DevOpsGuru AWS CLIまたは他の AWS のサービス を使用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。

DevOpsGuru でのデータ暗号化

暗号化は DevOpsGuru セキュリティの重要な部分です。一部の暗号化 (転送中のデータの暗号化など) はデフォルトで提供されるため、特に操作は必要ありません。その他の暗号化 (保管中のデータの暗号化など) については、プロジェクトまたはビルドの作成時に設定できます。

- 転送中のデータの暗号化: 顧客と DevOpsGuru 間、および DevOpsGuru とそのダウンストリームの依存関係間のすべての通信は、TLS を使用して保護され、署名バージョン 4 の署名プロセスを使用して認証されます。すべての DevOpsGuru エンドポイントは、 によって管理される証明書を使用します AWS Private Certificate Authority。詳細については、「署名バージョン 4 の署名プロセス」および「ACM PCA とは」を参照してください。
- 保管中のデータの暗号化: DevOpsGuru によって分析されたすべての AWS リソースについて、Amazon CloudWatch メトリクスとデータ、リソース IDs、および AWS CloudTrail イベントはAmazon S3、Amazon DynamoDB、および Amazon Kinesis を使用して保存されます。 AWS CloudFormation スタックを使用して分析されたリソースを定義する場合、スタックデータも収集されます。 DevOpsGuru は Amazon S3、DynamoDB、Kinesis のデータ保持ポリシーを使用します。Kinesis に保存されたデータは、設定されているポリシーに応じて、最大 1 年間保持できます。Amazon S3 および DynamoDB に保存されたデータは 1 年間保存されます。

  保存されたデータは、Amazon S3、DynamoDB、および Kinesis の data-at-rest 暗号化機能を使用して暗号化されます。

  カスタマーマネージドキー ： DevOpsGuru は、カスタマーマネージドキーを使用して CloudWatch Logs から生成されたログ異常などのカスタマーコンテンツや機密メタデータの暗号化をサポートしています。この機能では、組織のコンプライアンスや規制要件を満たすのに役立つセルフマネージドのセキュリティレイヤーを追加することができます。 DevOpsGuru 設定でカスタマーマネージドキーを有効にする方法については、「」を参照してくださいthe section called “暗号化を更新する”。

  この暗号化層はユーザーが完全に制御できるため、次のようなタスクを実行できます。

  - キーポリシーの策定と維持
  - IAM ポリシーとグラントの策定と維持
  - キーポリシーの有効化と無効化
  - 暗号化素材のローテーション
  - タグの追加
  - キーエイリアスの作成

- 削除のためのキースケジューリング

詳細については、「 AWS Key Management Service デベロッパーガイド」の「カスタマーマネージドキー」を参照してください。

> **Note**
>
> DevOpsGuru は、 AWS 所有キーを使用して保管時の暗号化を自動的に有効にし、機密性の高いメタデータを無料で保護します。ただし、カスタマーマネージドキーの使用には AWS KMS 料金が適用されます。料金の詳細については、「 の AWS Key Management Service 料金」を参照してください。

DevOpsGuru が で許可を使用する方法 AWS KMS

DevOpsGuru では、カスタマーマネージドキーを使用するには許可が必要です。

カスタマーマネージドキーによる暗号化を有効にすると、 DevOpsGuru は に CreateGrant リクエストを送信してユーザーに代わって許可を作成します AWS KMS。の許可 AWS KMS は、Gru DevOps に顧客アカウントの AWS KMS キーへのアクセスを許可するために使用されます。

DevOpsGuru では、以下の内部オペレーションにカスタマーマネージドキーを使用する権限が必要です。

- トラッカーまたはジオフェンスコレクションの作成時に入力された対称カスタマーマネージド KMS キー ID が有効であることを確認する DescribeKey リクエストを AWS KMS に送信します。
- カスタマーマネージドキーで暗号化されたデータキーを生成する AWS KMS には、 に GenerateDataKey リクエストを送信します。
- Decrypt リクエストを AWS KMS に送信して、暗号化されたデータキーを復号し、データの暗号化に使用できます。

任意のタイミングで、許可に対するアクセス権を取り消したり、カスタマーマネージドキーに対するサービスからのアクセス権を削除したりできます。これを行うと、 DevOpsGuru はカスタマーマネージドキーによって暗号化されたデータにアクセスできなくなり、そのデータに依存するオペレーションに影響します。例えば、 DevOpsGru がアクセスできない暗号化された口グの異常情報を取得しようとすると、オペレーションは AccessDeniedException エラーを返します。

DevOpsGuru での暗号化キーのモニタリング

DevOpsGuru リソースで AWS KMS カスタマーマネージドキーを使用する場合、 AWS CloudTrail または CloudWatch ログを使用して、 DevOpsGru が に送信するリクエストを追跡できます AWS KMS。

カスタマーマネージドキーを作成する

対称カスタマーマネージドキーを作成するには、 AWS Management Console または AWS KMS APIsを使用します。

対称型のカスタマーマネージドキーを作成するには、「対称暗号化 KMS キーの作成」を参照してください。

キーポリシー

キーポリシーは、カスタマーマネージドキーへのアクセスを制御します。すべてのカスタマーマネージドキーには、キーポリシーが 1 つだけ必要です。このポリシーには、そのキーを使用できるユーザーとその使用方法を決定するステートメントが含まれています。カスタマーマネージドキーを作成する際に、キーポリシーを指定することができます。詳細については、「 AWS Key Management Service デベロッパーガイド」の「 の認証とアクセスコントロール AWS KMS」を参照してください。

DevOpsGuru リソースでカスタマーマネージドキーを使用するには、キーポリシーで次の API オペレーションを許可する必要があります。

- `kms:CreateGrant` - カスタマーマネージドキーに許可を追加します。指定された AWS KMS キーへのアクセスを制御する権限を付与します。これにより、DevOpsGuru が必要とする許可オペレーションへのアクセスを許可します。権限の使用の詳細については、「 AWS Key Management Service デベロッパーガイド」を参照してください。

これにより、 DevOpsGru は以下を実行できます。

- を呼び出し GenerateDataKey て暗号化されたデータキーを生成し、保存します。データキーはすぐに暗号化に使用されるわけではないためです。
- Decrypt を呼び出すと、保存されている暗号化データキーを使用して暗号化されたデータにアクセスできます。
- サービスの使用停止プリンシパルを設定して、 へのサービスを許可します RetireGrant。

- kms: DescribeKey を使用してカスタマーマネージドキーの詳細を指定し、 DevOpsGuru がキーを検証できるようにします。

次のステートメントには、 DevOpsGru に追加できるポリシーステートメントの例が含まれています。

```
"Statement" : [
  {
    "Sid" : "Allow access to principals authorized to use DevOps Guru",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "devops-guru.Region.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
  },
  {
    "Sid": "Allow access for key administrators",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
     },
    "Action" : [
      "kms:*"
     ],
    "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
  },
  {
    "Sid" : "Allow read-only access to key metadata to the account",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [
```

```
        "kms:Describe*",
        "kms:Get*",
        "kms:List*"
      ],
      "Resource" : "*"
    }
  ]
```

トラフィックのプライバシー

インターフェイス VPC エンドポイントを使用するように DevOpsGuru を設定することで、リソース分析とインサイト生成のセキュリティを向上させることができます。これを行う場合、インターネットゲートウェイ、NAT デバイス、または仮想プライベートゲートウェイは必要ありません。また、を設定する必要はありませんが PrivateLink、推奨されます。詳細については、「DevOpsGuru とインターフェイス VPC エンドポイント (AWS PrivateLink) 」を参照してください。PrivateLink および VPC エンドポイントの詳細については、AWS PrivateLink「」および「 を介した AWS サービスへのアクセス PrivateLink」を参照してください。

Amazon DevOpsGuru の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 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 DevOpsGuru リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- DevOps AWS マネージドポリシーとサービスにリンクされたロールに対する Guru の更新
- Amazon DevOpsGuru と IAM の連携方法
- Amazon DevOpsGuru のアイデンティティベースのポリシー
- DevOpsGuru のサービスにリンクされたロールの使用
- Amazon DevOpsGuru アクセス許可リファレンス

- Amazon SNS トピックへの許可
- – 暗号化された Amazon AWS KMS SNS トピックのアクセス許可 Amazon SNS
- Amazon DevOpsGuru のアイデンティティとアクセスのトラブルシューティング

対象者

AWS Identity and Access Management (IAM) の使用方法は、 DevOpsGru で行う作業によって異なります。

サービスユーザー – DevOpsGuru サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの DevOpsGuru 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。 DevOpsGuru の機能にアクセスできない場合は、「」を参照してくださいAmazon DevOpsGuru のアイデンティティとアクセスのトラブルシューティング。

サービス管理者 – 社内の DevOpsGuru リソースを担当している場合は、通常、Guru DevOpsへのフルアクセスがあります。サービスユーザーがどの DevOpsGuru 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で DevOpsGuru で IAM を使用する方法の詳細については、「」を参照してくださいAmazon DevOpsGuru と IAM の連携方法。

IAM 管理者 – IAM 管理者は、 DevOpsGru 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 DevOpsGuru アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon DevOpsGuru のアイデンティティベースのポリシー。

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アイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID

フェデレーションが設定されています。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高め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「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、『IAM ユーザーガイド』の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリのユーザー、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できるようにすることもできます。IAM Identity Center の詳細については、『AWS IAM Identity Center ユーザーガイド』の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する権限を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、『IAM ユーザーガイド』の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、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アイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(プロキシとしてロールを使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — 一部の 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権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用して 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 のサービスに権限を委任するロールの作成」を参照してください。

- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

- Amazon EC2 で実行され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 ロールを使用して権限を付与する」を参照してください。

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

ポリシーを使用したアクセスの管理

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、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) AWS 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、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 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権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

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。許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの許可の境界」を参照してください。
- サービスコントロールポリシー (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。

DevOps AWS マネージドポリシーとサービスにリンクされたロールに対する Guru の更新

DevOpsGuru の AWS マネージドポリシーとサービスにリンクされたロールの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更に関する自動通知を受け取るには、 DevOpsGuru の RSS フィードにサブスクライブしてください[Amazon DevOps Guru のドキュメント履歴](#)。

変更	説明	日付
[AmazonDevOpsGuruConsoleFullAccess](#) – 既存ポリシーへの更新。	`AmazonDevOpsGuruFullAccess` マネージドポリシーは Amazon SNS サブスクリプションをサポートするようになりました。	2023 年 8 月 9 日
[AmazonDevOpsGuruReadOnlyAccess](#) – 既存ポリシーへの更新。	`AmazonDevOpsGuruReadOnlyAccess` マネージドポリシーで Amazon SNS サブスクリプションリストへの読み取り専用アクセスがサポートされるようになりました。	2023 年 8 月 9 日
[AmazonDevOpsGuruServiceRolePolicy](#) – 既存ポリシーへの更新。	`AWSServiceRoleForDevOpsGuru` サービスにリンクされたロールは、REST API の API Gateway GET アクションへのアクセスをサポートするようになりました。	2023 年 1 月 11 日
[AmazonDevOpsGuruServiceRolePolicy](#) – 既存ポリシーへの更新。	`AWSServiceRoleForDevOpsGuru` サービスにリンクされたロールは、いくつかの Amazon Simple Storage サービスと Service Quotas ア	2022 年 10 月 19 日

変更	説明	日付
	クションをサポートするようになりました。	
AmazonDevOpsGuruFullAccess – 既存ポリシーへの更新	AmazonDevOpsGuruFullAccess マネージドポリシー は、 CloudWatch FilterLogEvents アクションへのアクセスをサポートするようになりました。	2022 年 8 月 30 日
AmazonDevOpsGuruConsoleFullAccess – 既存ポリシーへの更新	AmazonDevOpsGuruConsoleFullAccess マネージドポリシーが FilterLogEvents アクションへのアクセス CloudWatchをサポートするようになりました。	2022 年 8 月 30 日
AmazonDevOpsGuruReadOnlyAccess – 既存ポリシーへの更新	AmazonDevOpsGuruReadOnlyAccess マネージドポリシーは、 アクションへの CloudWatch FilterLogEvents 読み取り専用アクセスをサポートするようになりました。	2022 年 8 月 30 日

変更	説明	日付
AmazonDevOpsGuruServiceRolePolicy – 既存ポリシーへの更新。	AWSServiceRoleForDevOpsGuru サービスにリンクされたロールは、 CloudWatch ログアクション FilterLogEvents 、DescribeLogGroups 、および をサポートするようになりましたDescribeLogStreams 。	2022 年 7 月 12 日
DevOpsGuru のアイデンティティベースのポリシー – 新しい マネージドポリシー。	AmazonDevOpsGuruConsoleFullAccess ポリシーが追加されました。	2021 年 12 月 16 日
AmazonDevOpsGuruServiceRolePolicy – 既存ポリシーへの更新。	AWSServiceRoleForDevOpsGuru サービスにリンクされたロールで Performance Insights DescribeMetricsKeys 、および Amazon RDS DescribeDBInstances アクションがサポートされるようになりました。	2021 年 12 月 1 日
AmazonDevOpsGuruReadOnlyAccess – 既存ポリシーへの更新	AmazonDevOpsGuruReadOnlyAccess マネージドポリシーで Amazon RDS DescribeDBInstances アクションへの読み取り専用アクセスがサポートされるようになりました。	2021 年 12 月 1 日

変更	説明	日付
AmazonDevOpsGuruFullAccess – 既存ポリシーへの更新	AmazonDevOpsGuruFullAccess マネージドポリシーで Amazon RDS DescribeDBInstances アクションへのアクセスがサポートされるようになりました。	2021 年 12 月 1 日
Amazon DevOpsGuru のアイデンティティベースのポリシー — 新しいポリシーが追加されました。	AWSServiceRoleForDevOpsGuru サービスにリンクされたロールで Amazon RDS の DescribeDBInstances アクションおよび Performance Insights の GetResourceMetrics アクションがサポートされるようになりました。 AmazonDevOpsGuruOrganizationsAccess 管理ポリシーは、組織内の DevOpsGuru へのアクセスを提供します。	2021 年 11 月 16 日
AmazonDevOpsGuruServiceRolePolicy – 既存ポリシーへの更新。	AWSServiceRoleForDevOpsGuru サービスにリンクされたロールで AWS Organizations がサポートされるようになりました	2021 年 11 月 4 日

変更	説明	日付
AmazonDevOpsGuruServiceRolePolicy – 既存ポリシーへの更新。	AWSServiceRoleForDevOpsGuru サービスにリンクされたロールに ssm:CreateOpsItem アクションと ssm:AddTagsToResource アクションの新しい条件が含まれるようになりました。	2021 年 10 月 11 日
DevOpsGuru のサービスにリンクされたロールのアクセス許可 – 既存ポリシーへの更新。	AWSServiceRoleForDevOpsGuru サービスにリンクされたロールに ssm:CreateOpsItem アクションと ssm:AddTagsToResource アクションの新しい条件が含まれるようになりました。	2021 年 6 月 14 日
AmazonDevOpsGuruReadOnlyAccess – 既存ポリシーへの更新	AmazonDevOpsGuruReadOnlyAccess マネージドポリシーで、 および DevOpsGuru DescribeFeedback アクションへの AWS Identity and Access Management GetRole読み取り専用アクセスを許可するようになりました。	2021 年 6 月 14 日

変更	説明	日付
AmazonDevOpsGuruReadOnlyAccess – 既存ポリシーへの更新	AmazonDevOpsGuruReadOnlyAccess マネージドポリシーで、 DevOpsGru GetCostEstimation および StartCostEstimation アクションへの読み取り専用アクセスを許可するようになりました。	2021 年 4 月 27 日
AmazonDevOpsGuruServiceRolePolicy – 既存ポリシーへの更新。	AWSServiceRoleForDevOpsGuru ロールは、 および Amazon EC2 Auto Scaling DescribeAutoScalingGroups アクションへのアクセス AWS Systems Manager AddTagsToResource を許可するようになりました。	2021 年 4 月 27 日
DevOpsGuru が変更の追跡を開始しました	DevOpsGuru が AWS マネージドポリシーの変更の追跡を開始しました。	2020 年 12 月 10 日

Amazon DevOpsGuru と IAM の連携方法

IAM を使用して DevOpsGuru へのアクセスを管理する前に、Guru で使用できる IAM DevOps機能について学びます。

Amazon DevOpsGuru で使用できる IAM の機能

IAM 機能	DevOpsGuru のサポート
アイデンティティベースのポリシー	Yes

IAM 機能	DevOpsGuru のサポート
リソースベースのポリシー	No
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	Yes
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	いいえ
サービスリンクロール	はい

DevOpsGuru 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。

DevOpsGuru の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。

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。

DevOpsGuru のアイデンティティベースのポリシーの例

DevOpsGuru アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon DevOpsGuru のアイデンティティベースのポリシー。

DevOpsGuru 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	No

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追加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 ロールとリソースベースのポリシーとの相違点」を参照してください。

DevOpsGuru 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権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

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

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

```
aws
```

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": [
      "aws:action1",
      "aws:action2"
         ]
```

DevOpsGuru アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon DevOpsGuru のアイデンティティベースのポリシー。

DevOpsGuru 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、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

DevOpsGuru リソースタイプとその ARNs」の「Amazon DevOpsGuru で定義されるリソース」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、「Amazon DevOpsGuru で定義されるアクション」を参照してください。

DevOpsGuru アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon DevOpsGuru のアイデンティティベースのポリシー。

DevOpsGuru 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	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。

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。

DevOpsGuru 条件キーのリストを確認するには、「サービス認証リファレンス」の「Amazon DevOpsGuru の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「Amazon DevOpsGuru で定義されるアクション」を参照してください。

DevOpsGuru アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon DevOpsGuru のアイデンティティベースのポリシー。

DevOpsGuru ACLs)

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権限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。

DevOpsGuru 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操作を許可するように ABAC ポリシーを設計します。

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 をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性に基づくアクセスコントロール (ABAC) を使用する」を参照してください。

DevOpsGuru 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 は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

DevOpsGuru 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。

DevOpsGuru のサービスロール

サービスロールのサポート	いいえ

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 のサービスに権限を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 DevOpsGru の機能が破損する可能性があります。 DevOpsGuru 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。

DevOpsGuru のサービスにリンクされたロール

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、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービス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、[Yes] リンクを選択します。

Amazon DevOpsGuru のアイデンティティベースのポリシー

デフォルトでは、ユーザーとロールには DevOpsGuru 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。

各リソースタイプの ARN の形式など、 DevOpsGuru で定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンス」の「Amazon DevOpsGuru 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。 ARNs

トピック

- ポリシーのベストプラクティス
- DevOpsGuru 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
- DevOpsGuru の AWS 管理 (事前定義) ポリシー

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが DevOpsGuru 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 ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権権限とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。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。

DevOpsGuru コンソールの使用

Amazon DevOpsGuru コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の DevOpsGuru リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き DevOpsGuru コンソールを使用できるようにするには、エンティティに DevOpsGuru `AmazonDevOpsGuruReadOnlyAccess`または `AmazonDevOpsGuruFullAccess` AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

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": "*"
        }
    ]
}
```

DevOpsGuru の AWS 管理 (事前定義) ポリシー

AWS は、 によって作成および管理されるスタンドアロン IAM ポリシーを提供することで、多くの一般的なユースケースに対処します AWS。これらの AWS管理ポリシーは、一般的なユースケースに必要なアクセス許可を付与するため、必要なアクセス許可を調査する必要がなくなります。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」 を参照してください。

DevOpsGuru サービスロールを作成および管理するには、 という名前の AWSマネージドポリシーもアタッチする必要がありますIAMFullAccess。

独自のカスタム IAM ポリシーを作成して、 DevOpsGru アクションとリソースのアクセス許可を許可することもできます。こうしたカスタムポリシーは、該当するアクセス許可が必要なユーザーまたはグループにアタッチできます。

アカウントのユーザーにアタッチできる以下の AWS管理ポリシーは、 DevOpsGuru に固有です。

トピック

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

AmazonDevOpsGuruFullAccess – Amazon SNS トピックの作成、Amazon CloudWatch メトリクスへのアクセス、 AWS CloudFormation スタックへのアクセスなどの DevOpsGuru へのフルアクセスを提供します。 Amazon SNS これは、 DevOpsGuru に対するフルコントロールを付与する管理者レベルのユーザーにのみ適用されます。

AmazonDevOpsGuruFullAccess ポリシーには、次のステートメントが含まれます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
```

```
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
```

```
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess` – Amazon SNS トピックの作成、Amazon メトリクスへのアクセス CloudWatch、 AWS CloudFormation スタックへのアクセスなどの DevOpsGuru へのフルアクセスを提供します。 Amazon SNS このポリシーには、パフォーマンスインサイト権限が追加されているため、異常な Amazon RDS Aurora DB インスタンスに関連する詳細な分析をコンソールで表示できます。これは、 DevOpsGuru に対するフルコントロールを付与する管理者レベルのユーザーにのみ適用されます。

AmazonDevOpsGuruConsoleFullAccess ポリシーには、次のステートメントが含まれます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
```

```
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PerformanceInsightsMetricsDataAccess",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
```

```
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruReadOnlyAccess

AmazonDevOpsGuruReadOnlyAccess – DevOpsGuru および他の AWS サービスの関連リソースへの読み取り専用アクセスを許可します。このポリシーは、インサイトを表示する権限を付与するユーザーに適用しますが、 DevOpsGuru の分析力バレッジ境界、Amazon SNS トピック、または Systems Manager OpsCenter 統合を更新しません。

AmazonDevOpsGuruReadOnlyAccess ポリシーには、次のステートメントが含まれます。

```
    {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:DescribeAccountHealth",
                "devops-guru:DescribeAccountOverview",
                "devops-guru:DescribeAnomaly",
                "devops-guru:DescribeEventSourcesConfig",
                "devops-guru:DescribeFeedback",
                "devops-guru:DescribeInsight",
                "devops-guru:DescribeResourceCollectionHealth",
                "devops-guru:DescribeServiceIntegration",
```

```
                "devops-guru:GetCostEstimation",
                "devops-guru:GetResourceCollection",
                "devops-guru:ListAnomaliesForInsight",
                "devops-guru:ListEvents",
                "devops-guru:ListInsights",
                "devops-guru:ListAnomalousLogGroups",
                "devops-guru:ListMonitoredResources",
                "devops-guru:ListNotificationChannels",
                "devops-guru:ListRecommendations",
                "devops-guru:SearchInsights",
                "devops-guru:StartCostEstimation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruOrganizationsAccess – Organizations 管理者が組織内の DevOpsGuru マルチアカウントビューにアクセスできるようにします。このポリシーを、組織内の DevOpsGuru へのフルアクセスを許可する組織の管理者レベルのユーザーに適用します。このポリシーは、組織の管理アカウントと DevOpsGuru の委任管理者アカウントに適用できます。Guru への読み取り専用AmazonDevOpsGuruReadOnlyAccessまたはフルアクセスを提供するには、このポリシーAmazonDevOpsGuruFullAccessに加えて または DevOpsを適用できます。

AmazonDevOpsGuruOrganizationsAccess ポリシーには、次のステートメントが含まれます。

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

```
    "Sid": "AmazonDevOpsGuruOrganizationsAccess",
    "Effect": "Allow",
    "Action": [
     "devops-guru:DescribeOrganizationHealth",
     "devops-guru:DescribeOrganizationResourceCollectionHealth",
     "devops-guru:DescribeOrganizationOverview",
     "devops-guru:ListOrganizationInsights",
     "devops-guru:SearchOrganizationInsights"
    ],
    "Resource": "*"
   },
   {
    "Sid": "OrganizationsDataAccess",
    "Effect": "Allow",
    "Action": [
     "organizations:DescribeAccount",
     "organizations:DescribeOrganization",
     "organizations:ListAWSServiceAccessForOrganization",
     "organizations:ListAccounts",
     "organizations:ListChildren",
     "organizations:ListOrganizationalUnitsForParent",
     "organizations:ListRoots"
    ],
    "Resource": "arn:aws:organizations::*:"
   },
   {
    "Sid": "OrganizationsAdminDataAccess",
    "Effect": "Allow",
    "Action": [
     "organizations:DeregisterDelegatedAdministrator",
     "organizations:RegisterDelegatedAdministrator",
     "organizations:ListDelegatedAdministrators",
     "organizations:EnableAWSServiceAccess",
     "organizations:DisableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "devops-guru.amazonaws.com"
      ]
     }
    }
   }
```

```
 ]
}
```

DevOpsGuru のサービスにリンクされたロールの使用

Amazon DevOpsGuru は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 DevOpsGru 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 DevOpsGuru 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 AWS CloudTrail、Amazon CloudWatch、 AWS CodeDeploy、 AWS X-Ray、および AWS Organizations 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。

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

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、リソースへのアクセス許可を誤って削除することがなくなるため、 DevOpsGru リソースが保護されます。

DevOpsGuru のサービスにリンクされたロールのアクセス許可

DevOpsGuru 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AWSServiceRoleForDevOpsGuru。これは、 DevOpsGru がアカウントで実行する必要があるスコープ付きアクセス許可を持つ AWS マネージドポリシーです。

AWSServiceRoleForDevOpsGuru サービスにリンクされたロールはその引き受け時に、以下のサービスを信頼します。

- devops-guru.amazonaws.com

ロールのアクセス許可ポリシーは、指定されたリソースに対して以下のアクションを実行することを DevOpsGuru AmazonDevOpsGuruServiceRolePolicyに許可します。

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

```
    "Action": [
     "autoscaling:DescribeAutoScalingGroups",
     "cloudtrail:LookupEvents",
     "cloudwatch:GetMetricData",
     "cloudwatch:ListMetrics",
     "cloudwatch:DescribeAnomalyDetectors",
     "cloudwatch:DescribeAlarms",
     "cloudwatch:ListDashboards",
     "cloudwatch:GetDashboard",
     "cloudformation:GetTemplate",
     "cloudformation:ListStacks",
     "cloudformation:ListStackResources",
     "cloudformation:DescribeStacks",
     "cloudformation:ListImports",
     "codedeploy:BatchGetDeployments",
     "codedeploy:GetDeploymentGroup",
     "codedeploy:ListDeployments",
     "config:DescribeConfigurationRecorderStatus",
     "config:GetResourceConfigHistory",
     "events:ListRuleNamesByTarget",
     "xray:GetServiceGraph",
     "organizations:ListRoots",
     "organizations:ListChildren",
     "organizations:ListDelegatedAdministrators",
     "pi:GetResourceMetrics",
     "tag:GetResources",
     "lambda:GetFunction",
     "lambda:GetFunctionConcurrency",
     "lambda:GetAccountSettings",
     "lambda:ListProvisionedConcurrencyConfigs",
     "lambda:ListAliases",
     "lambda:ListEventSourceMappings",
     "lambda:GetPolicy",
     "ec2:DescribeSubnets",
     "application-autoscaling:DescribeScalableTargets",
     "application-autoscaling:DescribeScalingPolicies",
     "sqs:GetQueueAttributes",
     "kinesis:DescribeStream",
     "kinesis:DescribeLimits",
     "dynamodb:DescribeTable",
     "dynamodb:DescribeLimits",
     "dynamodb:DescribeContinuousBackups",
     "dynamodb:DescribeStream",
     "dynamodb:ListStreams",
```

```
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "rds:DescribeOptionGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeAccountAttributes",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "s3:GetBucketNotification",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketWebsite",
    "s3:GetIntelligentTieringConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowPutTargetsOnASpecificRule",
   "Effect": "Allow",
   "Action": [
    "events:PutTargets",
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
  },
  {
   "Sid": "AllowCreateOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateOpsItem"
   ],
   "Resource": "*"
  },
  {
```

```
    "Sid": "AllowAddTagsToOpsItem",
    "Effect": "Allow",
    "Action": [
     "ssm:AddTagsToResource"
    ],
    "Resource": "arn:aws:ssm:*:*:opsitem/*"
   },
   {
    "Sid": "AllowAccessOpsItem",
    "Effect": "Allow",
    "Action": [
     "ssm:GetOpsItem",
     "ssm:UpdateOpsItem"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated": "true"
     }
    }
   },
   {
    "Sid": "AllowCreateManagedRule",
    "Effect": "Allow",
    "Action": "events:PutRule",
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowAccessManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowOtherOperationsOnManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:PutTargets",
```

```
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "devops-guru.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowTagBasedFilterLogEvents",
    "Effect": "Allow",
    "Action": [
     "logs:FilterLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-Guru-Analysis": "true"
     }
    }
   },
   {
    "Sid": "AllowAPIGatewayGetIntegrations",
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": [
     "arn:aws:apigateway:*::/restapis/??????????",
     "arn:aws:apigateway:*::/restapis/*/resources",
     "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
    ]
   }
  ]
}
```

DevOpsGuru のサービスにリンクされたロールの作成

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 でインサイトを作成すると、 DevOpsGuru がサービスにリンクされたロールを作成します。

> **Important**
>
> このサービスにリンクされたロールは、このロールでサポートされている機能を使用する別のサービスでアクションを完了した場合、アカウントに表示されます。例えば、 からリポジトリに DevOpsGuru を追加した場合などです AWS CodeCommit。

DevOpsGuru のサービスにリンクされたロールの編集

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

DevOpsGuru のサービスにリンクされたロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、すべてのリポジトリとの関連付けを解除する必要があります。

> **Note**
>
> リソースを削除しようとしたときに DevOpsGuru サービスがロールを使用している場合、削除が失敗する可能性があります。その場合は、数分待ってからオペレーションを再試行してください。

IAM を使用してサービスリンクロールを手動で削除するには

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

Amazon DevOpsGuru アクセス許可リファレンス

DevOpsGuru ポリシーで AWS全体の条件キーを使用して条件を表現できます。表の詳細については、[IAM ユーザーガイド]の「IAM JSON ポリシー要素のリファレンス」を参照してください。

アクションは、ポリシーの `Action` フィールドで指定します。アクションを指定するには、API オペレーション名 (例えば、`devops-guru:` や `devops-guru:SearchInsights`) の前に `devops-guru:ListAnomalies` プレフィックスを使用します。単一のステートメントに複数のアクションを指定するには、コンマで区切ります (例えば、`"Action": [ "devops-guru:SearchInsights", "devops-guru:ListAnomalies" ]`)。

ワイルドカード文字の使用

ポリシーの `Resource` フィールドでリソース値として Amazon リソースネーム (ARN) を指定します。指定する際は、ワイルドカード文字 (*) を使用することもできます。ワイルドカードを使用して複数のアクションまたはリソースを指定することができます。例えば、 `devops-guru:*`はすべての DevOpsGuru アクションを指定し、 という単語で始まるすべての DevOpsGuru アクションを指定しますdevops-guru:List*`List`。次の例は、`12345` で始まる UUID (Universally Unique IDentifier) を持つすべてのインサイトを示します。

```
arn:aws:devops-guru:us-east-2:123456789012:insight:12345*
```

アイデンティティを使用した認証 をセットアップし、IAM アイデンティティ (アイデンティティベースのポリシー) にアタッチできるアクセス許可ポリシーを作成するときは、以下の表をリファレンスとして使用できます。

DevOpsGuru API オペレーションとアクションに必要なアクセス許可

`AddNotificationChannel`

アクション: `devops-guru:AddNotificationChannel`

DevOpsGuru から通知チャネルを追加するために必要です。通知チャネルは、 DevOpsGru がオペレーションの改善方法に関する情報を含むインサイトを生成するときに通知するために使用されます。

リソース: *

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

DevOpsGuru から通知チャネルを削除するために必要です。通知チャネルは、 DevOpsGru がオペレーションの改善方法に関する情報を含むインサイトを生成するときに通知するために使用されます。

リソース: *

`ListNotificationChannels`

アクション: `devops-guru:ListNotificationChannels`

DevOpsGuru 用に設定された通知チャネルのリストを返すために必要です。各通知チャネルは、オペレーションを改善する方法に関する情報を含むインサイトを DevOpsGuru が生成したときに通知するために使用されます。サポートされている通知タイプは、Amazon Simple Notification Service です。

リソース: *

`UpdateResourceCollectionFilter`

アクション: `devops-guru:UpdateResourceCollectionFilter`

DevOpsGuru によって分析されるアカウント内の AWS リソースを指定するために使用する AWS CloudFormation スタックのリストを更新するために必要です。分析では、レコメンデーション、運用メトリクス、および運用イベントを含むインサイトが生成されます。これらのインサイトを使用して、オペレーションのパフォーマンスを向上させることができます。この方法では、 を使用するために必要な IAM ロールも作成されます CodeGuru OpsAdvisor。

リソース: *

`GetResourceCollectionFilter`

アクション: `devops-guru:GetResourceCollectionFilter`

DevOpsGuru によって分析されるアカウント内のリソースを指定 AWS するために使用する AWS CloudFormation スタックのリストを返すために必要です。分析では、レコメンデーション、運用メトリクス、および運用イベントを含むインサイトが生成されます。これらのインサイトを使用して、オペレーションのパフォーマンスを向上させることができます。

リソース: *

`ListInsights`

アクション: `devops-guru:ListInsights`

AWS アカウント内のインサイトのリストを返すために必要です。返すインサイトは、開始時刻、ステータス (ongoing または any)、およびタイプ (reactive または predictive) で指定できます。

リソース: *

DescribeInsight

アクション: devops-guru:DescribeInsight

ID を使用して指定したインサイトに関する詳細を返すために必要です。

リソース: *

SearchInsights

アクション: devops-guru:SearchInsights

AWS アカウント内のインサイトのリストを返すために必要です。返すインサイトは、開始時間、フィルター、およびタイプ (reactiveまたはpredictive) で指定できます。

リソース: *

ListAnomalies

アクション: devops-guru:ListAnomalies

ID を使用して指定したインサイトに属する異常のリストを返すために必要です。

リソース: *

DescribeAnomaly

アクション: devops-guru:DescribeAnomaly

ID を使用して指定した異常に関する詳細を返すために必要です。

リソース: *

ListEvents

アクション: devops-guru:ListEvents

DevOpsGuru によって評価されるリソースによって生成されたイベントのリストを返すために必要です。返すイベントは、フィルターを使用して指定できます。

リソース: *

ListRecommendations

アクション: devops-guru:ListRecommendations

指定されたインサイトのレコメンデーションのリストを返すために必要です。各レコメンデーションには、メトリクスのリスト、およびレコメンデーションに関連するイベントのリストが含まれます。

リソース: *

DescribeAccountHealth

アクション: devops-guru:DescribeAccountHealth

オープンな事後対応型インサイトの数、オープンな予測インサイトの数、アカウントで分析されたメトリクスの数を返すために必要です AWS 。これらの数値を使用して、 AWS アカウント内のオペレーションの状態を測定します。

リソース: *

DescribeAccountOverview

アクション: devops-guru:DescribeAccountOverview

時間範囲内で作成されたオープンな事後対応型インサイトの数、時間範囲内で作成されたオープンな予測インサイトの数、および時間範囲内でクローズされたすべての事後対応型インサイトの平均回復時間 (MTTR) を返すために必要です。

リソース: *

DescribeResourceCollectionHealthOverview

アクション: devops-guru:DescribeResourceCollectionHealthOverview

DevOpsGuru で指定された各 AWS CloudFormation スタックのすべてのインサイトについて、オープン予測インサイト、オープンリアクティブインサイト、および平均復旧時間 (MTTR) を返すために必要です。

リソース: *

DescribeIntegratedService

アクション: devops-guru:DescribeIntegratedService

DevOpsGuru と統合できるサービスの統合ステータスを返すために必要です。 DevOpsGuru と統合できる 1 つのサービスは です。これは AWS Systems Manager、生成されたインサイト OpsItem ごとに を作成するために使用できます。

リソース: *

`UpdateIntegratedServiceConfig`

アクション: `devops-guru:UpdateIntegratedServiceConfig`

DevOpsGuru と統合できるサービスとの統合を有効または無効にするために必要です。DevOpsGuru と統合できる 1 つのサービスは Systems Manager で、生成されたインサイト OpsItem ごとに を作成するために使用できます。

リソース: *

Amazon SNS トピックへの許可

このトピックの情報は、別の AWS アカウントが所有する Amazon SNS トピックに通知を配信するように Amazon DevOpsGuru を設定する場合にのみ使用します。 Amazon SNS

DevOpsGuru が別のアカウントが所有する Amazon SNS トピックに通知を配信するには、通知を送信する許可を DevOpsGuru に付与するポリシーを Amazon SNS トピックにアタッチする必要があります。 DevOpsGuru で使用するのと同じアカウントが所有する Amazon SNS トピックに通知を配信するように DevOpsGuru を設定すると、Guru DevOpsはトピックにポリシーを追加します。

別のアカウントの Amazon SNS トピックのアクセス許可を設定するポリシーをアタッチしたら、DevOpsGuru に Amazon SNS トピックを追加できます。Amazon SNS ポリシーを通知チャネルで更新して、セキュリティをさらに強化することもできます。

> **Note**
>
> DevOpsGuru は現在、同じリージョンでのクロスアカウントアクセスのみをサポートしています。

トピック

- 他のアカウントで Amazon SNS トピックにアクセス許可を設定する
- 他のアカウントから Amazon SNS トピックを追加する
- 通知チャネルで Amazon SNS ポリシーを更新する (推奨)

他のアカウントで Amazon SNS トピックにアクセス許可を設定する

既存の IAM ロールに許可を追加する

IAM ロールでログインした後で他のアカウントから Amazon SNS トピックを使用するには、使用する Amazon SNS トピックにポリシーをアタッチする必要があります。IAM ロールの使用中に別のアカウントから Amazon SNS トピックにポリシーをアタッチするには、IAM ロールの一部としてそのアカウントリソースに対する以下のアクセス権限が必要です。

- sns:CreateTopic
- sns:GetTopicAttributes
- sns:SetTopicAttributes
- sns:Publish

使用する Amazon SNS トピックに以下のポリシーをアタッチします。Resource キーの場合、*topic-owner-account-id*はトピック所有者のアカウント ID、 *topic-sender-account-id*は DevOpsGuru をセットアップしたユーザーのアカウント ID、 *devops-guru-role*は関連する個々のユーザーの IAM ロールです。region-*id* (例: us-west-2) および に適切な値を置き換える必要があります*my-topic-name*。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
```

```
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:role/devops-guru-role"]
            }
        }
    ]
}
```

IAM ユーザーとしてアクセス許可を追加する

他のアカウントから IAM ユーザーとして Amazon SNS トピックを使用する場合は、使用する Amazon SNS トピックに次のポリシーをアタッチします。Resource キーの場合、 *topic-owner-account-id*はトピック所有者のアカウント ID、 *topic-sender-account-id*は DevOpsGuru をセットアップしたユーザーのアカウント ID、 *devops-guru-user-name*は関連する個々の IAM ユーザーです。region-*id* (例: us-west-2) と に適切な値を置き換える必要があります*my-topic-name*。

> **Note**
>
> 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。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。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
```

```
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:user/devops-guru-user-
name"]
            }
        }
    ]
}
```

他のアカウントから Amazon SNS トピックを追加する

別のアカウントで Amazon SNS トピックのアクセス許可を設定したら、その Amazon SNS トピックを DevOpsGuru 通知設定に追加できます。Amazon SNS トピックは、 AWS CLI または DevOpsGuru コンソールを使用して追加できます。

- コンソールを使用するときに、別のアカウントのトピックを使用するには、[SNS トピック ARN を使用して既存のトピックを指定する] オプションを選択する必要があります。
- AWS CLI オペレーション を使用する場合はadd-notification-channel、`NotificationChannelConfig` オブジェクト`TopicArn`内で を指定する必要があります。

コンソールを使用して他のアカウントから Amazon SNS トピックを追加する

1. https://console.aws.amazon.com/devops-guru/ で Amazon DevOpsGuru コンソールを開きます。
2. ナビゲーションペインを開き、[設定] を選択します。
3. [通知] セクションに移動し、[編集] を選択します。
4. [SNS トピックを追加] を選択します。
5. 「SNS トピック ARN を使用して既存のトピックを指定する」 を選択します。
6. 使用する Amazon SNS トピックの ARN を入力します。このトピックにポリシーをアタッチすることで、このトピックのアクセス権限をすでに設定しているはずです。
7. (オプション) [通知設定] を選択して、通知頻度の設定を編集します。

8. [保存] を選択します。

通知設定に Amazon SNS トピックを追加すると、 DevOpsGuru はそのトピックを使用して、新しいインサイトの作成時など、重要なイベントを通知します。

通知チャネルで Amazon SNS ポリシーを更新する (推奨)

トピックを追加したら、トピックを含む DevOpsGuru 通知チャネルにのみアクセス許可を指定して、ポリシーのセキュリティを強化することをお勧めします。

通知チャネルで Amazon SNS トピックポリシーを更新する (推奨)

1. 通知の送信元のアカウントで `list-notification-channels` DevOpsGuru AWS CLI コマンドを実行します。

```
aws devops-guru list-notification-channels
```

2. `list-notification-channels` レスポンスで、Amazon SNS トピックの ARN を含むチャネル ID をメモします。チャネル ID は guid です。

   例えば、次のレスポンスでは、ARN `arn:aws:sns:`*region-id*`:`*111122223333*`:`*topic-name* を持つトピックのチャネル ID は *e89be5f7-989d-4c4c-b1fe-e7145037e531* です。

```
{
  "Channels": [
    {
      "Id": "e89be5f7-989d-4c4c-b1fe-e7145037e531",
      "Config": {
      "Sns": {
          "TopicArn": "arn:aws:sns:region-id:111122223333:topic-name"
        },
      "Filters": {
          "MessageTypes": ["CLOSED_INSIGHT", "NEW_INSIGHT", "SEVERITY_UPGRADED"],
          "Severities": ["HIGH", "MEDIUM"]
        }
      }
    }
  ]
}
```

3. the section called “他のアカウントで Amazon SNS トピックにアクセス許可を設定する” のトピックオーナー ID を使用して別のアカウントで作成したポリシーに移動します。ポリシーの Condition ステートメントで、SourceArn を指定する行を追加します。ARN には、リージョン ID (例: us-east-1) 、トピックの送信者の AWS アカウント番号、メモしたチャネル ID が含まれます。

   更新した Condition ステートメントは次のようになります。

```
"Condition" : {
  "StringEquals" : {
    "AWS:SourceArn": "arn:aws:devops-guru:us-
east-1:111122223333:channel/e89be5f7-989d-4c4c-b1fe-e7145037e531",
    "AWS:SourceAccount": "111122223333"
   }
 }
```

AddNotificationChannel が SNS トピックを追加できない場合は、IAM ポリシーに次の権限があることを確認してください。

```
{
     "Version": "2012-10-17",
     "Statement": [{
           "Sid": "DevOpsGuruTopicPermissions",
           "Effect": "Allow",
           "Action": [
                 "sns:CreateTopic",
                 "sns:GetTopicAttributes",
                 "sns:SetTopicAttributes",
                 "sns:Publish"
           ],
           "Resource": "arn:aws:sns:region-id:account-id:my-topic-name"
     }]
}
```

– 暗号化された Amazon AWS KMS SNS トピックのアクセス許可 Amazon SNS

指定した Amazon SNS トピックは、 AWS Key Management Serviceによって暗号化されている可能性があります。 DevOpsGuru が暗号化されたトピックを使用できるようにするには、まず を作成

し、 AWS KMS key 次に次のステートメントを KMS キーのポリシーに追加する必要があります。詳細については、「AWS KMS を使用して Amazon SNS に発行されたメッセージの暗号化」、「 ユーザーガイド」の「キー識別子 (KeyId) 」、および「Amazon Simple Notification Service デベロッパーガイド」の「データ暗号化」を参照してください。 AWS KMS

```
{
  "Version": "2012-10-17",
  "Id": "your-kms-key-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> DevOpsGuru は現在、1 つのアカウント内で使用するために暗号化されたトピックをサポートしています。現時点では、暗号化されたトピックを複数のアカウントで使用することはサポートされていません。

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

以下の情報は、 DevOpsGru と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

- DevOpsGuru でアクションを実行する権限がない
- ユーザーにプログラムによるアクセス権を付与したい

- iam を実行する権限がありません。PassRole
- AWS アカウント外のユーザーに DevOpsGuru リソースへのアクセスを許可したい

DevOpsGuru でアクションを実行する権限がない

から、アクションを実行する権限がないと AWS Management Console 通知された場合は、管理者に連絡してサポートを依頼する必要があります。

以下のエラー例は、ユーザー `mateojackson` がコンソールを使用して架空の *`my-example-widget`* リソースに関する詳細情報を表示しようとしているが、架空の `aws:GetWidget` 許可がないという場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

この場合、Mateo は、`aws:GetWidget` アクションを使用して *`my-example-widget`* リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

ユーザーにプログラムによるアクセス権を付与したい

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

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
		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」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。

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 DevOpsGuru にロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、 という IAM `marymajor` ユーザーがコンソールを使用して DevOpsGuru でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

AWS アカウント外のユーザーに DevOpsGuru 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:

- DevOpsGuru がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいAmazon DevOpsGuru と IAM の連携方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。

- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「外部で認証されたユーザー (ID フェデレーション) へのアクセス権限」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

DevOpsGuru のログ記録とモニタリング

モニタリングは、 DevOpsGuru およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。AWS には、 DevOpsGru を監視し、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツールが用意されています。

- Amazon CloudWatch は、 AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングします。メトリクスを収集および追跡し、カスタマイズされたダッシュボードを作成し、指定されたメトリックが指定したしきい値に達したときに通知またはアクションを実行するアラームを設定できます。例えば、 で Amazon EC2 インスタンスの CPU 使用率やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。 AWSを呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。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。

トピック

- Amazon による DevOpsGuru のモニタリング CloudWatch
- を使用した Amazon DevOpsGuru API コールのログ記録 AWS CloudTrail

Amazon による DevOpsGuru のモニタリング CloudWatch

を使用して DevOpsGuru をモニタリングできます。これにより CloudWatch、raw データを収集し、読み取り可能なほぼリアルタイムのメトリクスに加工します。これらの統計は 15 か月間保持されるため、履歴情報にアクセスし、ウェブアプリケーションまたはサービスの動作をより的確に把握できます。また、特定のしきい値を監視するアラームを設定し、これらのしきい値に達したときに

通知を送信したりアクションを実行したりできます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。

DevOpsGuru では、インサイトのメトリクスと DevOpsGuru 使用状況のメトリクスを追跡できます。運用ソリューションで異常な動作が発生しているかどうかを判断するために、多数の作成済み Insights を監視することをお勧めします。または、コストを追跡するために DevOpsGuru の使用状況をモニタリングすることもできます。

DevOpsGuru サービスは、 AWS/DevOps-Guru名前空間で次のメトリクスを報告します。

トピック

- インサイトのメトリクス
- DevOpsGuru 使用状況メトリクス

インサイトのメトリクス

CloudWatch を使用してメトリクスを追跡し、アカウント AWS で作成されたインサイトの数を表示できます。Type ディメンションで追跡するインサイト (proactive または reactive) を指定できます。すべてのインサイトを追跡する場合は、ディメンションを指定しないでおきます。

メトリクス

メトリクス	説明
Insight	AWS アカウントで作成されたインサイトの数。 有効なディメンション: Type 有効な統計: Sample count、Sum 単位: カウント

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

ディメンション

ディメンション	説明
Type	これがインサイトのタイプです。すべてのインサイトを追跡する場合は、Insights メトリクスのディメンションを指定しないでおきます。有効な値は proactive 、reactive です。

DevOpsGuru 使用状況メトリクス

CloudWatch を使用して Amazon DevOpsGuru の使用状況を追跡できます。

メトリクス

メトリクス	説明
CallCount	次のいずれかの DevOpsGuru メソッドによって行われた呼び出しの数。 • ListInsights • ListAnomaliesForInsight • ListRecommendations • ListEvents • SearchInsights • DescribeInsight • DescribeAnomaly 有効なディメンション:Service 、Class、Type、Resource 有効な統計: Sample count、Sum 単位: カウント

DevOpsGuru 使用状況メトリクスでは、次のディメンションがサポートされています。

ディメンション

ディメンション	説明
`Service`	リソースが含まれる AWS のサービスの名前。例えば、DevOpsGru の場合、この値は ですDevOps-Guru 。
`Class`	これは、追跡されるリソースのクラスです。 DevOpsGuru はこのディメンションを値 で使用しますNone。
`Type`	これは、追跡されるリソースのタイプです。 DevOpsGuru はこのディメンションを値 で使用しますAPI。
`Resource`	これは DevOpsGuru オペレーションの名前です。有効な値は、`ListInsights` 、`ListAnomaliesForInsight` 、`ListRecommendations` 、`ListEvents` 、`SearchInsights` 、`DescribeInsight` 、`DescribeAnomaly` です。

を使用した Amazon DevOpsGuru API コールのログ記録 AWS CloudTrail

Amazon DevOpsGuru は と統合されています。これは AWS CloudTrail、Guru. CloudTrail captures API DevOpsコールでユーザー、ロール、または DevOps AWS のサービスによって実行されたアクションを記録するサービスです。キャプチャされた呼び出しには、 DevOpsGuru コンソールからの呼び出しと、Guru API DevOps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、 DevOpsGru の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、 DevOpsGru 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。

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

DevOpsの Guru 情報 CloudTrail

CloudTrail AWS アカウントを作成すると、 がアカウントで有効になります。DevOpsGuru でアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他の AWS サービスイベントとともにイベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「イベント履歴で CloudTrail イベントを表示する」を参照してください。

DevOpsGuru のイベントなど、 AWS アカウント内のイベントの継続的な記録については、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで作成した証跡がすべての AWS リージョンに適用されます。証跡は、AWS パーティション内のすべてのリージョンからのイベントをログに記録し、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 ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」
- CloudTrail がサポートするサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

DevOpsGuru は、すべてのアクションをイベントとして CloudTrail ログファイルに記録することをサポートしています。詳細については、DevOps「Guru API リファレンス」の「アクション」を参照してください。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。ID 情報は次の判断に役立ちます。

- リクエストが、ルートとユーザー認証情報のどちらを使用して送信されたか。
- リクエストが、ロールとフェデレーションユーザーの一時的なセキュリティ認証情報のどちらを使用して送信されたか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail userIdentity 要素」を参照してください。

DevOpsGuru ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意の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、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 UpdateResourceCollectionアクションを示す CloudTrail ログエントリを示しています。


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAEXAMPLE:TestSession",
    "arn": "arn:aws:sts::123456789012:assumed-role/TestRole/TestSession",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/TestRole",
        "accountId": "123456789012",
        "userName": "sample-user-name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-12-03T15:29:51Z"
      }
    }
  },
  "eventTime": "2020-12-01T16:14:31Z",
  "eventSource": "devops-guru.amazonaws.com",
  "eventName": "UpdateResourceCollection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "sample-ip-address",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.901
 Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
  "requestParameters": {
```

```
    "Action": "REMOVE",
    "ResourceCollection": {
      "CloudFormation": {
        "StackNames": [
          "*"
        ]
      }
    }
  },
  "responseElements": null,
  "requestID": " cb8c167e-EXAMPLE ",
  "eventID": " e3c6f4ce-EXAMPLE ",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

DevOpsGuru とインターフェイス VPC エンドポイント (AWS PrivateLink)

Amazon DevOpsGuru APIsエンドポイントを使用できます。VPC エンドポイントを使用する場合、API コールは VPC 内に含まれ、インターネットにアクセスしないため、セキュリティが向上します。詳細については、「Amazon DevOpsGuru API リファレンス」の「アクション」を参照してください。

インターフェイス VPC エンドポイント を作成して、VPC と DevOpsGuru の間にプライベート接続を確立します。インターフェイスエンドポイントは、インターネットゲートウェイAWS PrivateLink、NAT デバイス、VPN 接続、AWS Direct Connect 接続のいずれも必要とせずに、DevOpsGru APIs にプライベートにアクセスできるテクノロジーである を利用しています。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 DevOpsGuru APIs。VPC と DevOpsGuru 間のトラフィックは Amazon ネットワークを離れません。

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。

DevOpsGuru VPC エンドポイントに関する考慮事項

DevOpsGuru 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「インターフェイスエンドポイントのプロパティと制限」を確認してください。

DevOpsGuru 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。

DevOpsGuru 用のインターフェイス VPC エンドポイントの作成

Guru サービスの VPC エンドポイントは、Amazon VPC DevOpsコンソールまたは AWS Command Line Interface () を使用して作成できますAWS CLI。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。

次のサービス名を使用して DevOpsGuru の VPC エンドポイントを作成します。

- com.amazonaws.*region*.devops-guru

エンドポイントのプライベート DNS を有効にすると、 など、リージョンのデフォルトの DNS 名を使用して DevOpsGuru に API リクエストを行うことができますdevops-guru.us-east-1.amazonaws.com。

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。

DevOpsGuru 用の VPC エンドポイントポリシーの作成

Guru へのアクセスを制御するエンドポイントポリシーを VPC DevOpsエンドポイントにアタッチできます。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: DevOpsGuru アクションの VPC エンドポイントポリシー

DevOpsGuru のエンドポイントポリシーの例を次に示します。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 DevOpsGuru アクションへのアクセスを許可します。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "devops-guru:AddNotificationChannel",
            "devops-guru:ListInsights",
            "devops-guru:ListRecommendations"
         ],
         "Resource":"*"
      }
   ]
}
```

DevOpsGuru のインフラストラクチャセキュリティ

マネージドサービスである Amazon DevOpsGuru 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 DevOpsGuru 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。

Amazon DevOpsGuru の耐障害性

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、物理的に分離された複数のアベイラビリティーゾーンを提供します。DevOpsGuru は複数のアベイラビリティーゾーンで動作し、アーティファクトデータとメタデータを Amazon S3 と Amazon DynamoDB に保存します。暗号化されたデータは複数の施設、および各施設の複数のデバイスで冗長的に保存されるので高い可用性と耐久性が提供されます。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

Amazon DevOps Guru のクォータと制限

次の表に Amazon DevOps Guru の現在のクォータを示します。このクォータは、各 AWS アカウントのサポートされる各 AWS リージョンのものです。

通知

一度に指定できる Amazon Simple Notification Service トピックの最大数	2

AWS CloudFormation スタック

指定できる AWS CloudFormation スタックの最大数	1000

DevOps Guru のリソース監視の制限

リソースの説明	制限	引き上げ可能
Amazon Simple Queue Service (Amazon SQS) キューのモニタリングに関するデフォルトの制限	100*	はい**

* 2023 年 6 月 29 日以降に作成された新しい DevOps Guru アカウント、および同じ日にアクティブで Amazon SQS キューが 100 未満である既存のアカウントが対象です。

**この制限の変更をリクエストするには、AWS Supporthttps://aws.amazon.com/contact-usまでお問い合わせください。Amazon SQS キューのモニタリング制限を 100、500、1,000、5,000、または 10,000 のいずれかにリクエストできます。

API の作成、デプロイ、管理のための DevOps Guru の割り当て

以下の固定クォータは、AWS CLI、API Gateway コンソール、または API Gateway REST API とその SDK を使用して、DevOps Guru で API の作成、デプロイ、および管理に適用されます。

すべての DevOps Guru API のリストについては、「Amazon DevOps Guru アクション」を参照してください。

デフォルトのクォータ	引き上げ可能	
アカウントあたり1 秒ごとに 20 リクエスト	はい	

Amazon DevOps Guru のドキュメント履歴

次の表は、DevOps Guru の今回のリリースの内容をまとめたものです。

- API バージョン: 最新
- 文書の最終更新: 2023 年 8 月 9 日

変更	説明	日付
マネージドポリシーの更新	Amazon SNS サブスクリプションとサブスクリプションリストアクセスが `AmazonDevOpsGuruConsoleFullAccess` ポリシーに追加されました。サブスクリプションリストへのアクセスも `AmazonDevOpsGuruReadOnlyAccess` ポリシーに追加されました。詳細については、「Amazon DevOps Guru のアイデンティティベースのポリシー」を参照してください。	2023 年 8 月 9 日
顧客が管理する暗号化キー	DevOps Guru では、AWS KMS を使用したカスタマーマネージドキーによる暗号化に対応できるようになりました。詳細については、「DevOps Guru におけるデータ保護」を参照してください。	2023 年 7 月 5 日
DevOps Guru for RDS は RDS PostgreSQL をサポートします	DevOps Guru for RDS は、PostgreSQL データベースにおけるパフォーマンスのボ	2023 年 3 月 30 日

	トルネックやその他のインサイトを検出できます。詳細については、「DevOps Guru for RDS の利点」を参照してください。	
DevOps Guru for RDS は事前対応型インサイトをサポートします	DevOps Guru for RDS は、Aurora データベースの問題が発生すると予測される前に、問題の対処に役立つレコメンデーションとともに事前対応型インサイトを発行します。詳細については、「DevOps Guru for RDS での異常への対処」を参照してください。	2023 年 2 月 28 日
[分析されたリソース]	DevOps Guru コンソールの新しいページには、DevOps Guru によって分析されたアカウント内のリソースが一覧表示されます。詳細については、「DevOps Guru が分析したリソースの表示」を参照してください。	2022 年 10 月 20 日
新しい通知構成設定	すべての通知を受信するか、特定の重要度やイベントの通知のみを受信するかを選択できるようになりました。詳細については、「Amazon SNS 通知設定の更新」を参照してください。	2022 年 9 月 30 日

マネージドポリシーへのログ異常分析の追加	AWS DevOps Guru のマネージドポリシーが IAM コンソールで更新され、CloudWatch アクションへのアクセスがサポートされるようになりましたFilterLogEvents 。詳細については、「AWS マネージドポリシーとサービスにリンクされたロールに対する DevOps Guru の更新」を参照してください。	2022 年 8 月 30 日
ログ異常分析が追加されました	DevOps Guru コンソールでは、インサイトに関連するロググループに関する詳細情報を表示できます。CloudWatch のログとストリームを記述できる、拡張されたサービスにリンクされたロールもあります。詳細については、「DevOps Guru コンソールでのインサイトを理解する」と「AWS マネージドポリシーとサービスにリンクされたロールに関する DevOps Guru の更新」を参照してください。	2022 年 7 月 12 日

CodeGuru Profiler 統合	DevOps Guru は、EventBridge マネージドルールを使用して Amazon CodeGuru Profiler と統合されるようになりました。CodeGuru Profiler からの各インバウンドイベントは、事前対応型の異常レポートです。詳細については、「CodeGuru Profiler との統合」を参照してください。	2022 年 3 月 7 日
サービスにリンクされたロールとマネージドポリシーの更新	IAM コンソールで利用可能な拡張ポリシー。この変更により DevOps Guru で Amazon Relational Database Service (Amazon RDS) との拡張統合がサポートされるようになりました。詳細については、「サービスにリンクされたロールの使用」と「DevOps Guru 用の AWS 管理 (定義済み) ポリシー」を参照してください。	2021 年 12 月 21 日
新しいマネージドポリシーが追加されました	`AmazonDevOpsGuruConsoleFullAccess` ポリシーが追加されました。詳細については、「Amazon DevOps Guru のアイデンティティベースのポリシー」を参照してください。	2021 年 12 月 6 日

AWS タグでアプリケーションを定義するためのサポート	AWS タグを使用して、DevOps Guru で分析するリソースの識別、アプリケーション内のリソースの識別、およびコンソールのインサイトのフィルターを行うことができるようになりました。詳細については、「Use tags to identify resources in your applications」を参照してください。	2021 年 12 月 1 日
サービスにリンクされたロールとマネージドポリシーの更新	IAM コンソールで利用可能な拡張ポリシー。この変更により DevOps Guru で Amazon Relational Database Service (Amazon RDS) との拡張統合がサポートされるようになりました。詳細については、「サービスにリンクされたロールの使用」と「DevOps Guru 用の AWS 管理 (定義済み) ポリシー」を参照してください。	2021 年 12 月 1 日
Amazon RDS のサポート	DevOps Guru は、アプリケーションの Amazon Relational Database Service (Amazon RDS) リソースに関する包括的な分析とインサイトを提供するようになりました。詳細については、「Working with anomalies in DevOps Guru for Amazon RDS」を参照してください。	2021 年 12 月 1 日

Amazon EventBridge との統合	DevOps Guru が EventBridge と統合され、DevOps Guru のインサイトに関連する特定のイベントを通知できるようになりました。詳細については、「Working with EventBridge」を参照してください。	2021 年 11 月 18 日
AWS マネージドポリシーを追加	新たに AWS マネージドポリシーを追加しました。`AmazonDevOpsGuruOrganizationsAccess` ポリシーは組織内の DevOps Guru へのアクセスを提供します。詳細については、「アイデンティティベースのポリシー」を参照してください。	2021 年 11 月 16 日
サービスにリンクされたロールポリシーの更新	IAM コンソールで利用可能な拡張ポリシー。この変更により、DevOps Guru がマルチアカウントビューをサポートするようになりました。詳細については、「サービスにリンクされたロールの使用」を参照してください。	2021 年 11 月 4 日
クロスアカウントのサポート	組織の複数のアカウントにわたるインサイトとメトリクスを表示できるようになりました。詳細については、「Amazon DevOps Guru とは」を参照してください。	2021 年 11 月 4 日
一般提供リリース	Amazon DevOps Guru の一般提供 (GA) が開始されました。	2021 年 5 月 4 日

新しいトピック	リソースを分析するための DevOps Guru の月額コストを生成できるようになりました。詳細については、「Amazon DevOps Guru のリソース分析コストの見積もり」を参照してください。	2021 年 4 月 27 日
VPC エンドポイントのサポート	VPC エンドポイントを使用して、リソース分析およびインサイト生成のセキュリティを強化できるようになりました。詳細については、「DevOps Guru とインターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。	2021 年 4 月 15 日
新しいトピック	Amazon CloudWatch で DevOps Guru を監視する方法に関する新しいトピックが追加されました。詳細については、「Amazon CloudWatch を使用した DevOps Guru のモニタリング」を参照してください。	2020 年 12 月 11 日
プレビューリリース	これは Amazon DevOps Guru ユーザーガイドのプレビューリリースです。	2020 年 12 月 1 日

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。

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。